Release Notes for Cisco IOS Release 15.1S

First Published: November 24, 2010
Last Updated: August 28, 2013
Release: Cisco IOS Release 15.1(3)S6
Part Number: OL-23821-03 Rev. IP

Introduction

These release notes support Cisco IOS Release 15.1S up to and including Cisco IOS Release 15.1(3)S6. These release notes are updated as needed to describe new features, caveats, and related documents.

The latest release of Cisco IOS Release 15.1S supports the Cisco 7200 series and Cisco 7300 series routers in addition to the Cisco 7600 series routers. Cisco IOS Release 15.1(3)S is the fourth release from the new 15S release model, so it is a long lived release that will have six maintenance releases. It includes many solution-oriented features and features from all the previous Cisco IOS software releases.

The modular Cisco 7200 series routers and Cisco 7301 router support a wide range of density, performance, and service requirements. The Cisco 7200 series routers and Cisco 7301 router offer a wide range of connectivity options and numerous features including serviceability and manageability. The Cisco 7200 series routers and Cisco 7301 router provide:

- Broadband aggregation: Up to 16,000 PPP sessions per chassis
- Multiprotocol Label Switching (MPLS) for provider-edge deployments
- Modular design: 3RU footprint with broad range of flexible, modular interfaces (from DS0 to OC-3)
- Flexibility: Support for Fast Ethernet, Gigabit Ethernet, and Packet over SONET

The latest release of Cisco IOS software for the Cisco 7600 series routers introduces new features and provides continued operational benefits for service providers. The Cisco 7600 series routers offer advanced wireless and wireline services and transport capabilities enabling Fix Mobile Convergence. Over 100 new features have been added in 15.1S, including the following:

- Optimized Transport and High Availability enhancements, including support for: MPLS-TP for Ethernet Access Circuits (enabling end-end solutions including Cisco's new Carrier Packet Transport and Cisco Prime Network Management), Access Circuit Redundancy (ACR) for ATM/IMA and Circuit Emulation, ATM Routed Bridge Encapsulation over PVCs, EVC Port Channel per Flow Load Balancing, Hot Standby PW Support for ATM and TDM Access Circuits, MST on LAG, REP Edge No-Neighbor, IP Tunnels L3VPN over mGRE MPLS MTU support, ISIS

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

IPv4 Loop-Free Alternate Fast Reroute, MST/MST-AG BPDU PW on LAG NNI, Multiple BPDU PW support for R-L2GP, OSPFv2 Loop Free Alternate Fast ReRoute, ICCP Multi-chassis VLAN Redundancy, Circuit Emulation Service over UDP, VPLS Inter-AS Option B, and many BFD enhancements.

- Multicast specific features including support for: Multicast Label Distribution Protocol-Based Multicast VPN (mLDP MVPN), mLDP MVPN Extranet, mLDP MVPN Filtering and High Availability, Multicast VLAN Registration (MVR), and MVPN Data MDT mapping options.
- Advanced IPv6 features including support for: IPv6 Rapid Deployment (6rd), BGP IPv6 PIC Edge and Core for IP/MPLS, EIGRP IPv6 VRF-Lite, DHCPv6 Relay for MPLS VPN, DHCPv6 Server VRF awareness, and IPv6 Route Health Injection (IPv6 RHI) on ACE30.
- OAM enhancements including support for: MPLS-TP OAM, IEEE 802.1ab LLDP (Link Layer Discovery Protocol), IP SLAs Metro-Ethernet 3.0 with ITU-T Y.1731, ITU-T Y.1731 Performance Monitoring, IPoDWDM Virtual Transponder, IPoDWDM Performance Monitoring, Metric Enhancements for RRI, and many new MIBs.
- Inline Video Monitoring enhancements: including support for: MPLS and PPPoE encapsulation, switchport interfaces, RFC4445 MDI monitoring for RTP encapsulated flows, RTP metric reporting, service availability reporting, and monitoring of SDI / HD-SDI flows common in video contribution networks.
- QoS enhancements including: Service Groups for Subinterfaces and Access Subinterfaces, Bandwidth Profile (Weight Assignment) sharing across Layer 3 and Layer 4 on Ethernet Services Plus (ES+) line cards, Layer 2 Access Control Lists (ACL) on EVCs, Layer 3/4 Access Control Lists (ACL) on Service Instance, Port-Level shaping concurrent with 4-Level Hierarchical QoS on ES+ line cards, Egress QoS scheduling for Port-Channel Interfaces, Layer 2 and Layer 3 QoS ACL Classification for EVC on ES+ line cards, and Layer 3 QoS support on CEoP SPAs.
- Synchronization features including: IEEE 1588v2 Feature Enhancements on the Metronome SPA, SSM support on SPA-1XCHOC12/DS0 and SPA-1XOC48POS/RPR, 1588v2 PTP Best Master Clock Algorithm (BMCA), and MIB Support for 1588v2 and SynchE.

System Requirements

This document describes the system requirements for Cisco IOS 15.1S releases and includes the following sections:

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains specific Cisco IOS features.

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit [3DES] data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Feature-to-image mapping is available through Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to 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 by feature set (software image). You can compare Cisco IOS software releases side-by-side to display both the features unique to each software release and the features that the releases have in common.

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:

www.cisco.com/go/cfn

For help with Cisco Feature Navigator, see the help information at the following URL:

http://www.cisco.com/web/applicat/CFNTOOLS/Help_Docs/help/cfn_support.html

Determining the Software Images (Feature Sets) That Support a Specific Feature

To determine which software images (feature sets) in a Cisco IOS release support a specific feature, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Research Features**.

Step 2 Select your software type or leave the field as “All”.

Step 3 To find a feature, you can search by either Feature or Technology (select the appropriate button). If you select Search by Feature, you can further filter your search by using the Filter By text box.

Step 4 Choose a feature from the Available Features text box, and click the **Add** button to add the feature to the Selected Features text box.

Note To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

Repeat this step to add features. A maximum of 20 features can be chosen for a single search.

Step 5 Click **Continue** when you are finished choosing features.

Step 6 In the Release/Platform Tree area, select either your release (from the Train-Release list) or your platform (from the Platform list).

Step 7 The "Search Result" table will list all the software images (feature sets) that support the features that you chose.

Note You can download your results into an Excel spreadsheet by clicking on the Download Excel button.

Determining the Features Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set), go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Research Software**.

Step 2 Select your software type from the drop-down list and chose the **Release** button in the "Search By" area.

Step 3 From the Major Release drop-down list, chose the appropriate major release.

Step 4 From the Release drop-down list, choose the appropriate maintenance release.

Step 5 From the Platform drop-down list, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down list, choose the appropriate feature set. The Image Details area will provide details on the specific image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.

Note To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

Memory Recommendations

To determine memory recommendations for software images (feature sets) in your Cisco IOS release, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Research Software**.

Step 2 Select your software type from the drop-down list and choose the **Release** button in the "Search By" area.

Step 3 From the Major Release drop-down list, choose the appropriate major release.

Step 4 From the Release drop-down list, choose the appropriate maintenance release.

Step 5 From the Platform drop-down list, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down list, choose the appropriate feature set.

Step 7 The Image Details area will provide details on the specific image including the DRAM and flash memory recommendations for each image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.

Supported Hardware

Cisco IOS Release 15.1S supports the following platforms, including the following models and supervisor engines:

- Cisco 7200 Network Processing Engine (NPE-G2) (introduced in Cisco IOS Release 15.1(3)S)
- Cisco 7200 series routers (Cisco 7200, Cisco 7201) (introduced in Cisco IOS Release 15.1(3)S)
- Cisco 7301 router (introduced in Cisco IOS Release 15.1(3)S)
- Cisco 7600 series routers (Cisco 7603-S, Cisco 7604, Cisco 7606, Cisco 7606-S, Cisco 7609, Cisco 7609-S, and Cisco 7613)
- RSP720-10GE
- Supervisor Engine 32, Supervisor Engine 720, Route Switch Processor 720

Guide to Supported Hardware for Cisco 7600 Series Routers

For extensive information about all supported hardware for Cisco 7600 series routers, see the *Guide to Supported Hardware for Cisco 7600 Series Routers with Cisco IOS Release 15S*:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

Determining the Software Version

To determine the version of Cisco IOS software that is running on your Cisco router, log in to the router and enter the **show version** EXEC command:

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) 7600 Software (s72033-ipservices_wan-mz), Version 12.2(33)SRD, EARLY DEPLOYMENT
RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about choosing a new Cisco IOS software release, see *How to Choose a Cisco IOS Software Release* at the following location:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml

For information about upgrading the Cisco 7200 series routers, see the document at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_install_and_upgrade.html

For information about upgrading the Cisco 7300 series routers, see the document at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps352/tsd_products_support_install_and_upgrade.html

For information about upgrading the Cisco 7600 series routers, see the document at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_install_and_upgrade.html

For Cisco IOS upgrade ordering instructions, see the document at the following location:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

To choose a new Cisco IOS software release based on information about defects that affect that software, use the Bug Toolkit at the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Limitations and Restrictions

This chapter describes limitations and restrictions in Cisco IOS 15.1S releases.

Limitations and Restrictions in Cisco IOS Release 15.1(3)S

This section describes limitations and restrictions in Cisco IOS Release 15.1(3)S.

- The Cisco IOS CEF **ip load-sharing per-packet**, **ip cef accounting per-prefix**, and **ip cef accounting non-recursive** commands are not supported on the Cisco 7600 series routers.
- VAM2+ and VSA HW and encryption are not supported on this release.
- SNA Switch protocol is not supported on this release.
- CUBE and voice port adapters are not supported.
- Only NPE-G2 and NPE-G1 with over 512MB of memory are supported on this release.
- NBAR is not supported on this release.

Limitations and Restrictions in Cisco IOS Release 15.1(2)S

There are no new limitations and restrictions in Cisco IOS Release 15.1(2)S.

Limitations and Restrictions in Cisco IOS Release 15.1(1)S

There are no new limitations and restrictions in Cisco IOS Release 15.1(1)S.

Features and Important Notes for Cisco IOS Release 15.1(3)S

These release notes describe the following topics:

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.1(3)S and contains the following subsections:

New Hardware Features in Cisco IOS Release 15.1(3)S6

There are no new hardware features introduced in Cisco IOS Release 15.1(3)S6.

New Software Features in Cisco IOS Release 15.1(3)S6

There are no new software features introduced in Cisco IOS Release 15.1(3)S6.

New Hardware Features in Cisco IOS Release 15.1(3)S5a

There are no new hardware features introduced in Cisco IOS Release 15.1(3)S5a.

New Software Features in Cisco IOS Release 15.1(3)S5a

There are no new software features introduced in Cisco IOS Release 15.1(3)S5a.

New Hardware Features in Cisco IOS Release 15.1(3)S5

There are no new hardware features introduced in Cisco IOS Release 15.1(3)S5.

New Software Features in Cisco IOS Release 15.1(3)S5

There are no new software features introduced in Cisco IOS Release 15.1(3)S5.

New Hardware Features in Cisco IOS Release 15.1(3)S4

There are no new hardware features introduced in Cisco IOS Release 15.1(3)S4.

New Software Features in Cisco IOS Release 15.1(3)S4

There are no new software features introduced in Cisco IOS Release 15.1(3)S4.

New Hardware Features in Cisco IOS Release 15.1(3)S3

There are no new hardware features introduced in Cisco IOS Release 15.1(3)S3.

New Software Features in Cisco IOS Release 15.1(3)S3

There are no new software features introduced in Cisco IOS Release 15.1(3)S3.

New Hardware Features in Cisco IOS Release 15.1(3)S2

There are no new hardware features introduced in Cisco IOS Release 15.1(3)S2.

New Software Features in Cisco IOS Release 15.1(3)S2

This section describes new and changed features in Cisco IOS Release 15.1(3)S2. Some features may be new to Cisco IOS Release 15.1(3)S2 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)S2. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

BFD—BFD Hardware Offload Support

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wpxref23529

New Hardware Features in Cisco IOS Release 15.1(3)S1

This section describes new and changed features in Cisco IOS Release 15.1(3)S1. Some features may be new to Cisco IOS Release 15.1(3)S1 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)S1. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

VPN Services Port Adapter (VSPA) and Services SPA Carrier (SSC-600)

For detailed information about this feature, see the *Overview of the IPSec VPN SPA* and *Configuring Enhanced IPSec Features Using the IPSec VPN SPA* chapters at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipspasw.html

New Software Features in Cisco IOS Release 15.1(3)S1

This section describes new and changed features in Cisco IOS Release 15.1(3)S1. Some features may be new to Cisco IOS Release 15.1(3)S1 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)S1. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

ES+ Copper SFP Auto Negotiation

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap2.html

BGP IPv6 PIC Edge and Core for IP/MPLS

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/BGP.html

New Hardware Features in Cisco IOS Release 15.1(3)S

This section describes new and changed features in Cisco IOS Release 15.1(3)S. Some features may be new to Cisco IOS Release 15.1(3)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in

Cisco IOS Release 15.1(3)S. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

SFP GLC-SX-MMD and GLC-LH-SMD for 1GE SPA and Supervisor Ports

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

VPN Services Port Adapter and Services SPA Carrier

For detailed information about this feature, see the documents at the following URLs:

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 Cisco IOS Release 15.1(3)S

This section describes new and changed features in Cisco IOS Release 15.1(3)S. Some features may be new to Cisco IOS Release 15.1(3)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)S. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

1588 PTP Best Master Clock Algorithm a.k.a. PTP Redundancy

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76oveth.html

Autostate—Firewall Capability

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/security/fwsm/fwsm41/configuration/guide/switch_f.html#Enabling_Autostate_Messaging_for_Rapid_Link_Failure_Detection

BFD Multihop

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html

Bidirectional MPLS-TP LSP

For detailed information about this feature, see the document at the following URL:

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

Capabilities Manager

For detailed information about this feature, see the document at the following URL:

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

CISCO-ENTITY-FRU-CONTROL-MIB

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/7600mib3.html

CISCO-ERR-DISABLE-MIB

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/7600mib3.html

CISCO-SWITCH-ENGINE-MIB

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/7600mib3.html

Deny ACL QoS Classification on ES+

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html

Egress L3/L4 ACL on Service Instance on Port-Channel With Per Flow Load Balancing

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

EIGRP Wide Metrics

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-1s/eigrp-15-1s-book.html

HA Support for MLDP

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_lsm/configuration/15-1s/imc-lsm-15-1s-book.html

ICCP Multi-chassis VLAN Redundancy

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

IEEE 802.1ab Link Layer Discovery Protocol

For detailed information about this feature, see the document at the following URL:

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

Inline Video Monitoring Support for Availability Reporting

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html#wp1517497

Inline Video Monitoring Support for Uncompressed Video

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html#wp1517497

Inline Video Monitoring Support of MDI Metrics for RTP Encapsulated Flows

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html#wp1517497

IPoDWDM Performance Management

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap10.html

IP Tunneling—IPv6 Rapid Deployment

For detailed information about this feature, see the document at the following URL:

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

IPv6 Route Health Injection on ACE-30

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/supcfg.html

ISIS IPv4 Loop Free Alternate Fast ReRoute for VPLS Core

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios/iproute_isis/configuration/guide/irs_ipv4_lfafrr.html

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/isis_lfa_ipfrr.html

L2TPv3—Layer-2 Tunneling Protocol Version 3

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

L2VPN: PW Status for Static PWs

For detailed information about this feature, see the document at the following URL:

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

mLDP Filtering

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_lsm/configuration/15-1s/imc_mldp_filter.html

MPLS-TP: MS-PW with Static and Dynamic PW Support

For detailed information about this feature, see the document at the following URL:

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

MPLS-TP OAM: Continuity Check via BFD

For detailed information about this feature, see the document at the following URL:

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

MPLS-TP OAM: Fault Management

For detailed information about this feature, see the document at the following URL:

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

MPLS-TP OAM: GACH

For detailed information about this feature, see the document at the following URL:

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

MPLS-TP OAM: Ping/Trace

For detailed information about this feature, see the document at the following URL:

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

MPLS-TP Path Protection

For detailed information about this feature, see the document at the following URL:

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

MPLS-TP: PW Redundancy for Static PWs

For detailed information about this feature, see the document at the following URL:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_transport_profile.html

MPLS-TP Support for Ethernet Access Circuits

For detailed information about this feature, see the document at the following URL:
http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap6.html

Multicast VLAN Registration

For detailed information about this feature, see the document at the following URL:
http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/snooigmp.html

Multiple BPDU PW Support for R-L2GP

For detailed information about this feature, see the document at the following URL:
http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldcfg.html

OSPFv2 Loop Free Alternate Fast Reroute

For detailed information about this feature, see the document at the following URL:
http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-1s/iro-lfa-frr.html

OSPFv3 Address Families

For detailed information about this feature, see the document at the following URL:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf.html

OSPFv3 External Path Preference Option (RFC 5340 from RFC 2328 16.4.1)

For detailed information about this feature, see the document at the following URL:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf.html

OSPFv3 Max-Metric Router-Lsa

For detailed information about this feature, see the document at the following URL:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf.html

OTN-IF MIB

For detailed information about this feature, see the document at the following URL:
http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/7600mib3.html

PIMv6: Anycast RP Solution

For detailed information about this feature, see the document at the following URL:

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

Reverse Route Injection Enhancements

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_rev_rte_inject.html

Stateful MLPPP MR-APS

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfstm1.html

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_mlppp_mr_aps.html

Support for MTU under EVC-Xconnect

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-1s/mp-any-transport.html

TFTP IPv6 Support

For detailed information about this feature, see the document at the following URL:

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

TrustSec SGT Handling: L2 SGT Imposition and Forwarding

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_cts/configuration/15-1s/sec-cts-15-1s-book.html

WCCP: VRF Support

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/wccp.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-2sy/iap-wccp.html

Xconnect as a Client of BFD

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/15_1s/mp_15_1s_book.html

MIBs

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

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

If the Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access the Cisco MIB Locator, 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

Important Notes

The following sections contain important notes about Cisco IOS Release 15.1S.

- Cisco IOS Behavior Changes, page 18
- Deferrals, page 24
- Field Notices and Bulletins, page 24

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 standalone document. When behavior changes are introduced, existing documentation is updated with the changes described in these sections:

- Cisco IOS Release 15.1(3)S5, page 18
- Cisco IOS Release 15.1(3)S4, page 19
- Cisco IOS Release 15.1(3)S3, page 20
- Cisco IOS Release 15.1(3)S2, page 21
- Cisco IOS Release 15.1(3)S1, page 22

Cisco IOS Release 15.1(3)S5

The following behavior changes were introduced in Cisco IOS Release 15.1(3)S5:

- BGP Processing of the Removal of Private AS Numbers from AS Path

  Old Behavior: When the **neighbor remove-private-as** command is configured and a route-map without a continue clause is configured, the processing order is:

  1. neighbor remove-private-as processing
  2. set as-path prepend or set as-path prepend last-as

However, if the route-map contains a continue clause, the processing order is reversed.

New Behavior: When the **neighbor remove-private-as** command is configured and a route-map is configured (whether it has a continue clause or not), the processing order is always:

1. neighbor remove-private-as processing
2. set as-path prepend or set as-path prepend last-as

- Old Behavior: No reporting was available for Wanphy alarms.

  New Behavior: Alarm reporting can be enabled for Wanphy alarms.

  Additional Information:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap10.html#wp1468974

Cisco IOS Release 15.1(3)S4

The following behavior changes were introduced in Cisco IOS Release 15.1(3)S4:

- The maximum value for cleanup-delay time that is configured using the **mpls traffic-eng reoptimize timers delay cleanup-delay time** command to delay the removal of old LSPs after tunnel reoptimization, is changed to 300 seconds.

  Old Behavior: The maximum value for cleanup-delay time that is configured using the **mpls traffic-eng reoptimize timers delay cleanup-delay time** command, is 60 seconds.

  New Behavior: The maximum value for cleanup-delay time that is configured using the **mpls traffic-eng reoptimize timers delay cleanup-delay time** command, is 300 seconds.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/mpls/command/mp-m4.html#GUID-B64630A1-3CD7-42DE-8E86-6CD47AC8981A

- Change to how IPv6 paths are advertised

  Old behavior: An IPv6 path is advertised without a label when the label has not been negotiated.

  New behavior: IPv6 paths are not advertised if the label has not been negotiated.

- The warning messages indicating that support for ISG (IP or PPPoE) sessions on ES+ line cards and SIP-400 is being deprecated are displayed on configuring or unconfiguring broadband (both IP and PPPoE) on Cisco 7600.

  Old behavior: No warning messages. System accepts the configuration.

  New behavior: Warning message indicating that support for ISG (IP or PPPoE) sessions on ES+ line cards and SIP-400 is being deprecated. The configuration is still accepted.

  Additional Information:

  - IP and PPPoE Session Support:

    http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1554342

  - IP Subscriber Awareness over Ethernet:

    http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/ipsuboe.html

- Taps on the same stream with different port range are accepted for RP based LI.

  Old Behavior: Taps on the same stream with different port range were rejected.

  New Behavior: Taps on the same stream with different port range are accepted.

Additional Information:

http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SR/configuration/lawful_intercept/76LIch2.html

Cisco IOS Release 15.1(3)S3

The following behavior changes were introduced in Cisco IOS Release 15.1(3)S3:

- Configure “radius-server attribute 44 include-in-access-req all” instead of “radius-server attribute 44 include-in-access-req” if per vrf level attribute inclusion is not required.

  Old behavior: **radius-server attribute 44 include-in-access-req** command applies attribute 44 for all the sessions.

  New behavior: The command is modified to include the configuration of non-vrf sessions.

  Additional information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/security/m1/sec-cr-r1.html#GUID-0C067786-2A4D-4D26-A429-0E7AA331E4CD

- The status of the **snmp trap link-status** command on an ATM subinterface changes when the device is reloaded.

  Old Behavior: The **snmp-server enable traps atm subif** command enables Simple Network Management Protocol (SNMP) link trap generation on all the ATM subinterfaces. When the device is reloaded SNMP trap generation is enabled on all ATM suninterfaces.

  New Behavior: To enable SNMP link trap generation on an ATM subinterface, first configure the **snmp-server enable traps atm subif** command in global configuration mode and then configure the **snmp trap link-status** command on the ATM subinterface on which SNMP link trap generation is to be enabled.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s4.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s5.html

- Change in BGP next-hop for redistributed recursive static routes.

  Old Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next hop to be itself. The local next-hop (equal to next-hop-self) is kept.

  New Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next-hop to be the recursive next-hop of the static route.

- ASR1K BDI interface supports mtu size change.

  Old Behavior: The default maximum transmission unit (MTU) size is 1500 bytes, and is not configurable.

  New Behavior: For a BDI, the maximum transmission unit (MTU) size can be configured between 1500 and 9216 bytes.

  Additional Information:
  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/bdi.html

- PfR syslog levels are added to minimize number of messages.

  Old Behavior: There are too many PfR syslog messages.

  New Behavior: PfR syslog levels are added to minimize the number of messages displayed, and a syslog notice is added to display when 30 percent of the traffic classes are out-of-policy.

Additional Information:
http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-1mt/pfr-15-1mt-book.html

- A new command **crypto engine hw-FIPS-mode** is introduced for WS-IPSEC-3 IPsec VSPA that reloads the router if there is an FIPS test failure.

  Old Behavior: If WS-IPSEC-3 IPsec VSPA fails FIPS test, it stops passing the traffic.

  New behavior: A new command **crypto engine hw-FIPS-mode** is introduced. If you configure the **crypto engine hw-FIPS-mode** command on a Cisco 7600 series router and the FIPS self test fails for any of the WS-IPSEC-3 IPsec VSPA, the router reloads continuously till the router passes the FIPS self test.

  Additional Information:
  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwvpn.html

- New CLI command added to enable/disable BFDv6 and BFDv4 session offloading.

  Old behavior: No CLI command.

  New behavior: The command **platform bfd disable-offload** added. You can now specifically control offloading of IPv4 and IPv6 BFD sessions.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html

Cisco IOS Release 15.1(3)S2

The following behavior changes were introduced in Cisco IOS Release 15.1(3)S2:

- BGP scan time range is changed.

  Old Behavior: The **bgp scan-time** command has a scanner-interval range of 15-60 seconds. The b**gp scan-time** command cannot be configured (it remains at the default value of 60 seconds) if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).

  New Behavior: The **bgp scan-time** command has a scanner-interval range of 5-60 seconds. The **bgp scan-time** command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).

- Increase in autonomous system number or community prepending in BGP Inbound Optimization using PfR.

  Old Behavior: In both the “BGP Autonomous System Number Prepend” and “BGP Autonomous System Number Community Prepend” methods of controlling inside prefixes using PfR, the number is increased one by one up to the maximum of six ASes in unreachable, loss, and delay OOP cases.

  New Behavior: In both the “BGP Autonomous System Number Prepend” and “BGP Autonomous System Number Community Prepend” methods of controlling inside prefixes using PfR, the new behavior increases the AS number or community to the maximum of six immediately, for unreachable and loss OOP cases.

  In the delay OOP case, the behavior is the same as the old behavior.

  Additional Information: See the “PfR Entrance Link Selection” section under Information About in:

  http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-2mt/pfr-bgp-inbound.html

- Increased maximum number of traffic classes (prefixes) to be learned in a PfR learn list.

  Old Behavior: Using the Cisco IOS CLI, **count** (PfR) command, the maximum number of traffic classes to be learned in a PfR learn list is 100, with a default of 50.

New Behavior: Using the Cisco IOS CLI, **count** (PfR) command, the maximum number of traffic classes to be learned in a PfR learn list is 1000, with a default of 1000.

Additional Information:
http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/command/pfr-cr-book.html

- Documentation changes to support the hiding of the Optimized Edge Routing (OER) CLI.

  Old Behavior: OER border router functionality is supported on the Catalyst 6500 switch.

  New Behavior: OER is no longer supported on the Catalyst 6500 switch, and the OER CLI is hidden.

  Additional Information: See the Cisco IOS Optimized Edge Routing Command Reference:

  http://www.cisco.com/en/US/docs/ios-xml/ios/oer/command/oer-cr-book.html

- The Enhanced IPv6 Neighbor Discovery Cache Management feature was written to address these changes.

  Old Behavior: Information about the enhanced IPv6 Neighbor Discovery cache management feature did not exist in documentation.

  New Behavior: The "Implementing IPv6 Addressing and Basic Connectivity" has this feature.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-addrg-bsc-con.html

- Netflow and microflow configuration support

  Old behavior: You cannot configure netflow and microflow policy on an interface together.

  New behavior: You can configure per-interface NetFlow and QoS micro-policing on an interface. However, do not configure different flow mask types on an interface. Only a single flow mask type should be configured for per-interface NetFlow and microflow policy.

  Impact on customer: Configuration of netflow and microflow policy on a interface is possible.

  Additional Information:
  http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/nde.html#wp1131072

- Switched Virtual Interface (SVI) based Ethernet over MPLS (EoMPLS) now works with Transport Profiles (TP).

  Old Behavior: SVI based EoMPLS did not work for packets over TP.

  New Behavior: SVI based EoMPLS now works for packets over TP.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-1s/mp-any-transport.html

Cisco IOS Release 15.1(3)S1

The following behavior changes were introduced in Cisco IOS Release 15.1(3)S1:

- Policing options are changed for IPv6 HBH packets on SIP-400, SIP-200 and Enhanced Flexwan line cards in Cisco 7600 series routers.

  Old Behavior: Setting the police rate to 0 turns off the policer.

  New Behavior: Setting the police rate to 0 drops all the IPv6 HBH packets. The new **test platform police ipv6 disable** command turns off the policer.

  Additional Information:
  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgsip.html#wp1462909

http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexqos.html#wp1402772

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html#wp1056002

- New AAA attribute for idle timeout direction can be configured in the service profile for ISG sessions.

  Old Behavior: The idle timeout direction is outbound by default.

  New Behavior: The idle timeout direction can be configured in the AAA service profile; if not configured, the default is outbound.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/isg/configuration/xe-3s/isg-sess-maint-pol.html#GUID-EF4EF99E-C76E-467E-BB73-4014A6D68A00

- Idle timeout direction for ISG IP sessions and traffic classes can be configured.

  Old Behavior: The idle timeout direction for IP sessions is inbound. For traffic classes, the timer is applied in the direction of the traffic class. If the idle timer is configured in both the inbound and outbound traffic class, it is applied in the outbound direction.

  New Behavior: The idle timeout direction can be configured in a service policy map using new keywords in the timeout idle command.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/isg/command/isg_m1.html#GUID-F6AA55BC-A3A8-4B85-B2DE-E3D53994A5E1

- IPv6 downstream traffic from an ISG interface can be configured to pass through without a subscriber session.

  Old Behavior: Downstream traffic towards a subscriber is dropped if a subscriber session is not present.

  New Behavior: The **passthru downstream ipv6** command allows IPv6 traffic to pass through without a subscriber session.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/isg/command/isg_m1.html

- BGP scan time range is changed.

  Old Behavior: The **bgp scan-time** command has a scanner-interval range of 15-60 seconds. The **bgp scan-time** command cannot be configured (it remains at the default value of 60 seconds) if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).

  New Behavior: The **bgp scan-time** command has a scanner-interval range of 5-60 seconds. The **bgp scan-time** command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).

- Policing options are changed for IPv6 HBH packets on ES+ line cards in Cisco 7600 series routers.

  Old Behavior: Setting the police rate to 0 turns off the policer.

  New Behavior: Setting the police rate to 0 drops all the IPv6 HBH packets. The new **test platform police ipv6 disable** command turns off the policer.

  Additional Information: http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html#wp1492073

  http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html#wp1056002

- CLI is introduced to ignore S1 SONET overhead byte set to 0xF.

Old Behavior: A packet received with an S1 SONET overhead byte set to 0xF causes the router to switch the clock source to internal.

New Behavior: The **atm sonet ignore s1** command has been introduced, which when set directs the router to ignore an S1 overhead byte set to 0xF, which in turn ensures that the clock does not change.

Additional information: http://www.cisco.com/en/US/docs/ios-xml/ios/atm/command/atm-a1.html

- IPv6 downstream traffic from an ISG interface can be configured to pass through without a subscriber session.

  Old Behavior: Downstream traffic towards a subscriber is dropped if a subscriber session is not present.

  New Behavior: The **passthru downstream ipv6** command allows IPv6 traffic to pass through without a subscriber session.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/isg/command/isg_m1.html

- Server and user-agent SIP headers have only token characters.

  Old Behavior: Outgoing SIP messages have nontoken characters in server and user-agent SIP headers.

  New Behavior: Server and user-agent SIP headers have only token characters.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_sip/configuration/15-2mt/voi-sip-param-mod.html

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Features and Important Notes for Cisco IOS Release 15.1(2)S

These release notes describe the following topics:

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.1(2)S and contains the following subsections:

New Hardware Features in Cisco IOS Release 15.1(2)S

This section describes new and changed features in Cisco IOS Release 15.1(2)S. Some features may be new to Cisco IOS Release 15.1(2)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(2)S. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

GLC-SX-MMD and GLC-LH-SMD for 1GE SPA and Supervisor Ports

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

XFP10GLR-192SR-L and XFP10GER-192IR-L 10GE XFP MAC on All ES 10GE, ES+ 10GE, ES+T 10GE, and 10GE SPAs

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

http://www.cisco.com/en/US/docs/routers/7600/Hardware/Module_and_Line_Card_Installation_Guides/ES40_Line_Card_Installation_Guide/es40_chap2.html

New Software Features in Cisco IOS Release 15.1(2)S

This section describes new and changed features in Cisco IOS Release 15.1(2)S. Some features may be new to Cisco IOS Release 15.1(2)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(2)S. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature

does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

BFD—BFD Hardware Offload Support

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

BFD—Client Grouping for IPv4 Static Routes (IP Core Dev)

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html

BFD—RIPv2 Support

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/iproute_rip/configuration/guide/irr_bfd_ripv2.html

BFD Scale Improvement on the ES+ Line Card for the Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

BGP—Consistency Checker

For detailed information about this feature, see the document at the following URL:

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

BGP IPv6 Client for Single Hop BFD

For detailed information about this feature, see the document at the following URL:

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

BGP IPv6 PIC Edge and Core for IP/MPLS

For detailed information about this feature, see the document at the following URL:

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

Callhome Message Using Dedicated Interface

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1607509

CFM Extension for 1+1 Hot-Standby Support

For detailed information about this feature, see the document at the following URL:

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

Circuit Emulation Service over UDP

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwcep.html

Cisco IOS Shell

For detailed information about this feature, see the document at the following URL:

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

CoPP on Nonaccess Subinterfaces

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

DHCPv6 Relay—MPLS VPN Support

For detailed information about this feature, see the document at the following URL:

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

DHCPv6 Server PD VRF Aware

For detailed information about this feature, see the document at the following URL:

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

Egress QoS Scheduling for Port-Channel Interfaces

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html

EIGRP/SAF HMAC-SHA-256 Authentication

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/iproute_eigrp/configuration/guide/ire_cfg_eigrp.html

Embedded Event Manager 3.2

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_3.2.html

IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731)

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1s/Configuring_IP_SLAs_Metro-Ethernet_3.0_ITU_T_Y.1731_Operations.html

IP Source Guard for Service Instance

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

IP Tunnels L3VPN over mGRE MPLS MTU Support

For detailed information about this feature, see the document at the following URL:

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

ISIS IPv4 Loop-Free Alternate Fast Reroute

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/iproute_isis/configuration/guide/irs_ipv4_lfafrr.html

L2 and L3 QoS ACL Classification for EVC on ES+

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html

L3QoS Support on CEoP SPAs

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book.html

MFI Work for IP FRR

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-1s/mp-any-transport.html

MIB Support for 1588v2 and SynchE

The IEEE Standard PTPv2 1588-2008 defines a protocol that enables precise synchronization of clocks in measurement and control systems implemented with packet-based networks. This MIB supports the Precision Timing Protocol version 2 (PTPv2) feature of Cisco System devices.

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

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

MST/MST-AG BPDU PW on LAG NNI

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldcfg.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap6.html

OSPF Support for NSSA RFC 3101

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_cfg.html

REP MIB

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

RTP Metrics Support for Cisco 7600 Inline Video Monitoring

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html#wp1517497

SPAN on EVC Service Instance

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

SSHv2 Enhancements

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_shell_v2.html

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_shell_v2.html

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_secure_shell_v2.html

SSO Support for REP FH

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1607509

Support PPPoE Encapsulation for Cisco 7600 Inline Video Monitoring

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html#wp1517497

Support Switch-Port Interfaces for Cisco 7600 Inline Video Monitoring

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html#wp1517497

SyncE Timing Services MIB

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_synce.html

Virtual Transponder on Cisco the 7600 IPoDWDM Line Card

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap10.html

Y.1731 Performance Monitoring

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_y1731-perfmon.html

MIBs

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

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

If the Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access the Cisco MIB Locator, 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

Important Notes

The following sections contain important notes about Cisco IOS Release 15.1S.

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 standalone document. When behavior changes are introduced, existing documentation is updated with the changes described in these sections:

- Cisco IOS Release 15.1(2)S2, page 31
- Cisco IOS Release 15.1(2)S1, page 32

Cisco IOS Release 15.1(2)S2

The following behavior changes were introduced in Cisco IOS Release 15.1(2)S2:

- Change is made to **neighbor prefix-length-size** command.

  Old Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, if that neighbor has a peer policy or route map that is removed, the **neighbor prefix-length-size** command setting is also removed.

  New Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, the value of that command overrides the value set for the peer-group. If the command is locally configured for the peer, it will not be inherited from the peer-group.

- Change is made in **show bgp ipv4 unicast summary** command.

  Old Behavior: The **show bgp ipv4 unicast summary** command displays an incorrect number of dynamically created neighbors per address family if a peer-group has been removed from the configuration.

  New Behavior: The **show bgp ipv4 unicast summary** command displays the correct number of dynamically created neighbors, even if a peer-group has been removed. The output displays the number of dynamically created neighbors per address family, and at the end of output, displays the total number of dynamically created neighbors on the router.

- State of MLP bundles is not synced to standby after SPA OIR.

  Old Behavior: Prior to RLS10/SRE4 release, the SPA-1xCHOC12/DS0 SPA boots up with the old controller status. If it was not admin down, it will start with no admin down and interfaces comes up as soon as the spa boots up.

  New Behavior: Effective from Cisco IOS Release 15.1(3)S and 12.2(33)SRE5, the SPA-1xCHOC12/DS0 boots up with admin down status and the original SPA status is restored after one second of the SPA bootup. Wait for a second after the log message "SPA_OIR-6-ONLINECARD: SPA (SPA-1XCHOC12/DS0) online in subslot" is displayed to configure the SPA.

  Additional Information

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwser.html

- BFD for pseudowire VCCV does not support UDP with MPLS-TP.

  Old Behavior: Bidirectional Forwarding Detection (BFD) for Pseudowire Virtual Circuit Connectivity Verification (VCCV) does not support User Datagram Protocol (UDP).

  New Behavior: When BFD for Pseudowire VCCV is used, Cisco IOS incorrectly advertises support for User Datagram Protocol (UDP) encapsulation, even if you specify the **vccv bfd template name raw-bfd** command. Only PW-ACH (raw) encapsulation is supported. This could cause

interoperability issues if the peer attempts to use UDP encapsulation. Cisco IOS-IOS connectivity is not affected. Further, the **udp** keyword for the **vccv bfd template** command has no effect. Only raw BFD is used.

Cisco IOS Release 15.1(2)S1

The following behavior changes were introduced in Cisco IOS Release 15.1(2)S1:

- Input service policies are not implemented for PPPoE client traffic.

  Old Behavior: Input service policies attached to a main interface or a subinterface are not implemented for PPPoE client traffic. Only input service policies attached to a dialer interface are implemented.

  New Behavior: Input service policies attached to a main interface or a subinterface are implemented for PPPoE client traffic but only if an input service policy is not configured for a dialer interface. If an input service policy is configured for a dialer interface, the old behavior is retained. Only the quality of service (QoS) counters for packet classification are supported. Counters for packet dropping, packet marking, and policing actions are not supported and are ignored.

- 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.

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

- Routing protocols purge routes when an interface goes down.

  Old Behavior: Routing protocols do not purge routes when an interface goes down. This is the default behavior.

  New Behavior: Routing protocols purge routes when an interface goes down. This is the default behavior.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html#wp1013065

- Bidirectional Forwarding Detection (BFD) changes to the CLI. New client name is in CLI output of the **show bfd neighbors detail** and **show bfd neighbors client** commands.

  Old Behavior: The client name “xconnect” appears in the **show bfd neighbors** command output.

  New Behavior: The “xconnect” client name is replaced with “AToM” in the **show bfd neighbors** command output.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_book.html

- Disable ISG on ES+ lowQ line card.

  Old Behavior: No restrictions were present in the ES+ Configuration guide.

  New Behavior: Updated the documentation with “ES+ low queue cards do not support ISG (IP session and PPPoE session)” note.

Additional Information:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1554396

- LAG support is extended on access port channel subinterface

  Old Behavior: We can add only two members to the port-channel access type subinterface.

  New Behavior: We can add multiple members to the port-channel access type subinterface if the ISG is not configured.

  Additional Information:
  http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1554373

- Policies with service fragment classes are allowed on all Ethernet main interface types. Policies with fragment classes are allowed on all Ethernet subinterfaces and port-channel subinterfaces.

  Old Behavior: You cannot use mod3/mod4 policies with service fragments and/or fragment classes on Ethernet interface types other than Gigabit Ethernet and port-channel.

  New Behavior: You can use mod3/mod4 policies with service fragments and/or fragment classes on all Ethernet interface types.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_policies_agg.html

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Features and Important Notes for Cisco IOS Release 15.1(1)S

These release notes describe the following topics:

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.1(1)S and contains the following subsections:

New Hardware Features in Cisco IOS Release 15.1(1)S

There are no new hardware features in Cisco IOS Release 15.1(1)S.

New Software Features in Cisco IOS Release 15.1(1)S

This section describes new and changed features in Cisco IOS Release 15.1(1)S. Some features may be new to Cisco IOS Release 15.1S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(1)S. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

1588-V2 Feature Enhancements on Metronome SPA

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgeth.html

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76oveth.html

Access Redundancy Circuit for ATM Local Switching

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_l2_lcl_swng.html

ACR Support for CEM

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_l2_lcl_swng.html

ACR Support for IMA

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_acr_supp_ima.html

ATM Routed Bridge Encapsulation

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios/bbdsl/configuration/guide/bba_atm_rbe.html

http://www.cisco.com/en/US/tech/tk39/tk48/technologies_configuration_example09186a008009455f.shtml

Bandwidth Profiles (Weight Assignments) Shared Across L3 and L4 on ES+

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html

BFD over SVI on Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/bfdsvi.html

BGP: RT Constrained Route Distribution

For detailed information about this feature, see the document at the following URL:

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

Configuration History MIB Enhancements

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

Custom Ethertype for the EVC Port Channel

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldcfg.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

DHCP Snooping with Option 82 on the EVC Port Channel

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

E3 and Channelization Support for SPA-2CHT3-CE-ATM

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgcep.html

EIGRP IPv6 VRF-Lite

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/iproute_eigrp/configuration/guide/ire_cfg_eigrp.html

EVC Port Channel per Flow Load Balancing

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

Hot Standby PW Support for ATM and TDM Access Circuits

For detailed information about this feature, see the documents at the following URLs:

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

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwsip.html#wp1062432

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap6.html

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/pfc3mpls.html

IEEE 802.1ag-2007 Compliant CFM MIB

For detailed information about this feature, see the documents at the following URLs:

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

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

L2 Access Control List on EVC

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_l2acl-evc.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldcfg.html

L2VPN VPLS Inter-AS Option B

For detailed information about this feature, see the document at the following URL:

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

L3/L4 ACL on Service Instance

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/bald_qos.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldcfg.html

Label Switched Multicast Multicast Label Distribution Protocol-Based Multicast VPN Support

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book.html

Legacy QoS Command Deprecation: Removed Commands

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/legacy_qos_cli_deprecation.html

Link State Tracking

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldcfg.html#wp1710611

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_sw_config.html

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book.html

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/54sg/configuration/guide/channel.html

Minimum Bandwidth Guarantee Plus Multiple Policies

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/port_level_shaping.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html

MST on LAG

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldcfg.html

MVPN—Data MDT Enhancements

Multicast distribution tree (MDT) groups were selected at random when the traffic passed the threshold and there was a limit of 255 MDTs before they were reused. The MVPN—Data MDT Enhancements feature provides the ability to deterministically map the groups from inside the VPN routing and forwarding (S,G) entry to particular data MDT groups, through an access control list (ACL).

The user can now map a set of VPN routing and forwarding (S,G) to a data MDT group in one of the following ways:

- 1:1 mapping (1 permit in ACL)
- Many to 1 mapping (many permits in ACL)
- Many to many mapping (multiple permits in ACL and a nonzero mask data MDT)

Because the total number of configurable data MDTs is 1024, the user can use this maximum number of mappings in any of the described combinations.

Per Subscriber Session Call Admission Control

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html

Port Level Shaping Concurrent with 4HQoS on ES+

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/port_level_shaping.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html

REP Edge No-Neighbor

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldcfg.html#wp1782690

RSVP for Flexible Bandwidth Interface

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_rsvp.html

RSVP over DMVPN

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_rsvp.html

RSVP Support for Ingress Call Admission Control

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_rsvp.html

RSVP-VRF Lite Admission Control

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_rsvp_vrf_lite.html

SDH Support for SPA-1XCHSTM4/OC12

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfstm1.html

Service Groups for Subinterfaces and Access Subinterfaces

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/service_groups.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html

SSM Support on SPA-1XCHOC12/DS0 and SPA-1XOC48POS/RPR

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwpos.html

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwser.html

SSO Support Port Mode Cell Relay on the Cisco 7600

In Cisco IOS Release 15.1(1)S, the Cisco 7600 series routers support stateful switchover (SSO) mode for ATM Cell Relay over MPLS in port mode.

Support MPLS Encapsulation for Cisco 7600 Inline Video Monitoring

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html

Unidirectional Link Detection on ES20 Ports Having EVCs

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldcfg.html

MIBs

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

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

If the Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access the Cisco MIB Locator, 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

Important Notes

The following sections contain important notes about Cisco IOS Release 15.1S.

- Cisco IOS Behavior Changes, page 41
- Deferrals, page 43
- Field Notices and Bulletins, page 43

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 standalone document. When behavior changes are introduced, existing documentation is updated with the changes described in these sections:

- Cisco IOS Release 15.1(1)S2, page 41
- Cisco IOS Release 15.1(1)S1, page 41

Cisco IOS Release 15.1(1)S2

The following behavior changes were introduced in Cisco IOS Release 15.1(1)S2:

- ISG can be configured to not update subscriber sessions with data from reauthentication profiles.

  Old Behavior: Intelligent Services Gateway (ISG) applies data from the reauthentication profile to subscriber sessions.

  New Behavior: The **re-authentication do-not-apply** command prevents ISG from applying data from the reauthentication profile to subscriber sessions.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/isg/command/reference/isg_m1.html

- Routing protocols purge routes when an interface goes down.

  Old Behavior: Routing protocols do not purge routes when an interface goes down. This is the default behavior.

  New Behavior: Routing protocols purge routes when an interface goes down. This is the default behavior.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html#wp1013065

- Disable ISG on ES+ lowQ line card.

  Old Behavior: No restrictions was present in the ES+ configuration guide.

  New Behavior: The documentation was updated with the following note: “ES+ low queue cards do not support ISG (IP session and PPPoE session).”

  Additional Information:
  http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1554396

Cisco IOS Release 15.1(1)S1

The following behavior changes were introduced in Cisco IOS Release 15.1(1)S1:

- The **no** form of the **ip nhrp map multicast dyn** command clears all dynamic entries in the multicast table.

  Old Behavior: Dynamic entries in the multicast table are not cleared even though the hold time has expired and the **ip nhrp map multicast dyn** command is disabled, which disables the automatic addition of routers to the multicast mappings by NHRP.

  New Behavior: All dynamic entries in the multicast table are now cleared when the hold time has expired and the **ip nhrp map multicast dyn** command is disabled.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_nhrp.html

- BGP address families are no longer stuck in NoNeg or idle state after reload.

  Old Behavior: After a reload of a router, some or all of the Border Gateway Protocol (BGP) address families do not come up because the router is receiving messages from a neighbor that the address family identifier (AFI) or subsequent address family identifiers (SAFI) is not supported, and the router does not retry those AFIs. The output of the **show ip bgp all** command summary shows the address family in NoNeg or idle state, and it will never leave that state. Typical output looks like:

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
x.x.x.x	4	1	0	0	1	0	0	never	(NoNeg)

  New Behavior: When the router receives a message that the AFI or SAFI is not supported, the router does not drop the rejected AFIs or SAFIs from subsequent OPEN messages. Instead, the router retries the AFI/SAFI within the existing OPEN message retry timing sequence, but with an exponential backoff (stopping at 10 minutes) applied to decisions about whether to include a particular AFI/SAFI in an OPEN message. The timing of OPEN messages is not changed. Successful negotiation of the AFI results in a reset of the backoff sequence for future attempts. Also, when a BGP connection collision occurs with a session in the ESTABLISHED state, BGP sends a CEASE notification on the newly opened connection, and a keepalive message on the old connection. The new connection is closed. If the old session was stale, the keepalive causes it to be closed. The neighbor will retry its OPEN message after receiving the CEASE message and waiting a few seconds.

- 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.

- The maximum transmission unit (MTU) and Time-to-Live (TTL) rate limiters are enabled by default.

  Old Behavior: The MTU and TTL rate limiters were not enabled by default.

  New Behavior: The MTU and TTL rate limiters are enabled by default. The default values are 970 and 97, respectively.

  Additional Information:

  http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SR/configuration/guide/dos.html#wp1163490

- Rate limit SIP200_MP-4-PAUSE message to avoid console flooding

  Old Behavior: In a scaled scenario, SIP200_MP-4-PAUSE messages take on substantial logging space and in the process other important logs might get missed.

  New Behavior: SIP200_MP-4-PAUSE message to avoid console flooding.

  Rate limit SIP200_MP-4-PAUSE ensures that one pause message is logged per unique occurrence across the SIP200 reloads and the subsequent occurrences are only statistically accounted.

  Additional Information:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76tblsip.html

- Disable NP crashinfo for all Network Processor exceptions.

  Old Behavior: A fix is required to reduce the Network Processor (NP) reload time.

  New Behavior: Network Processor crashinfo is disabled for all Network Processor exceptions by default.

  This fix disables crashinfo generation for all SIP400 Network Processor exceptions. This helps in improving the Network Processor reload time.

  Additional Information:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwsip.html

- The lease time for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client is changed.

  Old Behavior: DHCP server was sending infinite lease time to manual binding clients.

  New Behavior: The DHCP server sends a finite lease (the value configured using the **lease** command in DHCP pool configuration mode) to the clients for which manual bindings are configured.

- Two new keywords, **protocol** and **pbr**, were added to the **mode route** command.

  Old Behavior: Destination-only traffic classes cannot be controlled when more than one protocol is operating at the border routers.

  New Behavior: Destination-only traffic classes can be controlled when more than one protocol is operating at the border routers using dynamic policy-based routing (PBR).

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/command/pfr-cr-book.html

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Caveats for Cisco IOS Release 15.1(3)S

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section consists of the following subsections:

Open Caveats—Cisco IOS Release 15.1(3)S6

Cisco IOS Release 15.1(3)S6 is a rebuild release for Cisco IOS Release 15.1(3)S.

- CSCtn00145

  Symptom: Standby sup reloads on issuing the **no ip route** command.

  Conditions: This symptom is observed when static route statements present on the active and is missing on the stand-by. Perform these steps to recreate the issue:

  1. Configure a static route with an interface dependency (eg: ip static route 1.1.1.0 255.255.255.0 eth 0/0).
  2. Shutdown the Hardware Module/SPA corresponding to that interface. When the hardware module/SPA corresponding to that interface is shutdown, the static route entry is hidden from the configuration.

3. Reload the stand-by. When stand-by comes up, it performs a bulk sync to the running configuration of master. However the static routes which are HIDDEN, won't be present in the running configuration of master and hence will not be created in stand-by.
4. Bring up the hardware module/SPA. As this is still treated as OIR, the HIDDEN flag will be removed from the static routes and other related configurations will now be part of running configurations in the master. However these static routes are not present in stand-by as these information is lost due to reload and there will not be a disclosure of routes in standby and standby will be missing these static routes.
5. User executes no ip route. The route will be removed from master but as standby doesn't have these routes, it will result in a PRC failure leading to a standby reload.
6. Stand-by comes up after the reload. Now, it will have the entire configuration along with static routes in sync as the unhidden static routes are now part of the running configurations that are synced to standby

Workaround: Reloading the standby (most likely in a maintenance window) is the only way to sync missing ip route statements.

Resolved Caveats—Cisco IOS Release 15.1(3)S6

Resolved Caveats—Cisco IOS Release 15.1(3)S6

Cisco IOS Release 15.1(3)S6 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S5a but may be open in previous Cisco IOS releases.

- CSCsl38246

  Symptom: When console logging is turned on, a flood of the messages shown below:

  ```
  %MWAM-DFC3-0-CORRECTABLE_ECC_ERR: A correctable ECC error has occurred,
  A_BUS_L2_ERRORS: 0x0, A_BUS_MEMIO_ERRORS: 0xFF, A_SCD_BUS_ERR_STATUS: 0x80DC0000
  ```

  This can potentially lead to watchdog invocation and a subsequent crash.

  Conditions: A single-bit correctable error is detected on a CPU read from DRAM. As long as the errors remain correctable, and the performance of the processor does not deteriorate, the module is usable.

  Workaround: Since this is a parity error you can prevent the issue from happening in the future by resetting the module. If the issue still persists after resetting the module then we may be facing a hardware issue.

- CSCtj24692

  Symptom: NVRAM configuration file gets corrupted when a chassis is power cycled without a graceful shutdown.

  Conditions: This symptom is observed when you power cycle an ASR chassis without graceful shutdown.

  Workaround: Shutdown chassis using **reload** command and make sure RP gets to rommon mode before power cycling the chassis.

- CSCtj61284

  Symptom: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

  Conditions: The symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet (via a VRF-enabled interface).

Workaround: There is no workaround.

- CSCtl18571

  Symptom: On a Cisco 7600 series router with etherchannels configured, the **show etherchannel load-balance module** *x* command shows VLAN included even though the excluded VLAN has been configured globally using the **port-channel load-balance** *algorithm* **exclude vlan** command.

  Conditions: This symptom occurs when the system is operating in pfc3c or pfc3cxl mode with CFC and DFC card without per module load-balance.

  Workaround: This is an issue with the **show** command. The algorithm itself is not affected. The load-balancing algorithm is applied correctly as configured globally.

- CSCtq26296

  Symptom: Cisco router crashes with DLFI configurations.

  Conditions: The symptom is observed while doing a shut/no shut.

  Workaround: There is no workaround.

- CSCtr88785

  Symptom: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.

  Conditions: This symptom is observed on a Cisco 3845 running the c3845-advipservicesk9-mz.151-4.M1 image with a PKI certificate server configuration.

  Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCts02627

  Symptom: The **show mac-address-table** command displays invalid/incomplete port list for entries learned on VPLS Bridge Domain.

  It is observed that port-channel “Po1” is displayed as “Po”, and the Virtual Circuit IDs are missing in the port list of the mac-address-table entries. This is a display issue.

  Conditions: This symptom is observed only with mac-address-table entries that are learned on VPLS Bridge Domain VLAN.

  Workaround: There is no workaround.

- CSCts13720

  Symptom: When static pseduowires are configured with VCCV BFD, some of the VCs may not come up.

  Conditions: This symptom occurs when a static pseudowire is configured with VCCV BFD.

  Workaround: For the VCs that are DOWN, issue the **clear xconnect peer** *peer-ip-address* **vcid** *vcid value* command to bring the VC back UP.

- CSCts22336

  Symptom: The Cisco router may reload due to a bus error when configured with DMVPN.

  Conditions: This has been seen on Cisco IOS Release 15.1M and Cisco IOS Release 15.2T. The crash only occurs on devices that have at least one point-to-point GRE Tunnel interface configured with NHRP enabled. This type of interface is typically used to interconnect DMVPN hubs with point-to-point extension links.

  Workaround: Reconfigure the point-to-point GRE extension tunnel as an mGRE interface: -

  ```
  shutdown - no tunnel destination - tunnel mode gre multipoint - no shutdown.
  ```

The Tunnel interface must also have a static NHRP entry for the DMVPN peer, of the form:

```
ip nhrp map remote-tunnel-address remote-NBMA-address
```

where remote-NBMA-address is the same address that was configured in the "tunnel destination" statement. On an extension link, this configuration should typically already be present.

- CSCts60458

  Symptom: There is a memory leak in PfR MIB.

  Conditions: This symptom occurs when PfR is configured.

  Workaround: Reload the RP to free the memory for IOSd

- CSCtt21701

  Symptom: ASR CUBE is getting crashed when the endpoint tries to change IP address and media port in an early dialog UPDATE, but for codec change it works fine.

  Conditions: The crash is seen only when SDP passthrough is enabled and IP address and media port are being changed by an early dialog UPDATE.

  Workaround: Without SDP passthrough it works fine.

- CSCtw45592

  Symptom: The **ntp server** *DNS-name* command is not synced to the standby. When the **no ntp server** *hostname* command is issued later on the active, the standby reloads because the configuration was not added.

  Conditions: When the device is reloaded or when the DNS name is not resolved, the configuration is not added. It is seen after the standby sync failure, then issuing the **no ntp server** *hostname*.

  Workaround: Use IP/IPv6 addresses instead of the hostname for NTP configurations. The IP/IPv6 address can be found by pinging the hostname.

- CSCtx82890

  Symptom: After removing the encapsulation on MFR member interface, tracebacks are observed.

  Conditions: This symptom is observed when serial interface is configured with FR MLP configuration.

  Workaround: There is no workaround.

- CSCty12641

  Symptom: CFM ethernet ping fails with 7600 as the remote MEP end.

  Conditions: This symptom is observed after remote CFM over Xconnect MEPs with MEPs terminating on 7600 and having ESM20 LC.

  Workaround: There is no workaround. Consider using ES+LC.

- CSCty51453

  Symptom: Certificate validation using OCSP may fail, with OCSP server returning an "HTTP 400 - Bad Request" error.

  Conditions: The symptom is observed with Cisco IOS Release 15.2(1)T2 and later.

  Workaround 1: Add the following commands to change the TCP segmentation on the router:

  ```
  router(config)# ip tcp mss 1400 router(config)# ip tcp path-mtu-discovery
  ```

  Workaround 2: Use a different validation method (CRL) when possible.

- CSCty77441

  Symptom: Memory leaks are observed after unconfiguring the BFD sessions.

  Conditions: This symptom occurs after the BFD sessions are unconfigured.

  Workaround: There is no workaround.

- CSCtz33778

  Symptom: MDT remains in deleted state after several successive mdt removes/adds under the VRF.

  Conditions: The issue is seen when remove and add mdt is done quickly for multiple VRFs through a script.

  Workaround: Remove and re-add the VRF.

- CSCua24676

  Symptom: The VRF to the global packet's length is corrupted by -1.

  Conditions: This symptom occurs when the next-hop in the VRF is global and recursive going out labeled. This issue is seen from Cisco IOS Release 15.0(1)S3A onwards, but is not seen in Cisco IOS Release 15.0(1)S2.

  Workaround: Use the next-hop interface IP instead of the recursive next-hop.

- CSCua61201

  Symptom: Unexpected reload with BFD configured.

  Conditions: When a device is configured with BFD it may experience unexpected reloads.

  Workaround: There is no workaround.

- CSCua96354

  Symptom: Reload may occur when issuing the **show oer** and **show pfr** commands.

  Conditions: This symptom is observed with the following commands:

  ```
  - show oer master traffic-class performance - show pfr master traffic-class
  performance
  ```

  Workaround: There is no workaround.

- CSCub40547

  Symptom: ES+ module is crashing with "%NP_DEV-DFC1-2-WATCHDOG: Watchdog detected on NP 0" error.

  Conditions: The issue is specific to the type of packet and its content which is unique when vidmon is configured.

  Workaround: Remove vidmon configuration.

- CSCuc05929

  Symptom: After a reload, sometimes the MPLS forwarding function on some interfaces is not enabled. Some interfaces that were configured with "mpls ip" and link-state-up do not show with the **show mpls interface** command. This issue depends on a timing of the interface up.

  Conditions: Sometimes the issue occurs after a router reload or SIP/SPA reload. It is not affected when you configure "mpls ip" on an interface, admin-shutdown/no shutdown, and link-flap.

  Workaround: There is no workaround. When the issue occurs, do an admin-shutdown/no shutdown on the affected interface or disable/re-enable MPLS on the interface.

- CSCuc08477

  Symptom: All EOS and non EOS entries are missing for mLDP labels in the mid/bud node.

  Conditions: This symptom may occur due to random path flap mLDP tree changes.

  Workaround: Removing and adding the mLPD tree will trigger re-programming.

- CSCuc44306

  Symptom: The IPv6 HbH packets get punted to RP as a result of HbH rate-limiter not working.

  Conditions: This symptom is observed when IPv6 HbH packets hit the bridged interface on SIP400/SIP200 with IPv6 HbH rate-limiter configured.

  Workaround: There is no workaround.

- CSCuc55634

  Symptom: IPv6 static route cannot resolve the destination.

  Conditions: This symptom is observed under the following conditions:

  1. A VRF is configured by the old style CLI (for example “ip vrf RED”).
  2. Configure “ip vrf forwarding RED” under an interface.
  3. Configure IPv6 address under the same interface (for example 2001:192:44:1::2/64).
  4. Configure IPv6 static route via the interface configured in item 3, (for example IPv6 route 2001:192:14:1::/64 2001:192:44:1::1).
  5. Then, we are not able to ping the 2001:192:14:1::2 although we can reach 2001:192:44:1::1.

  Workaround: There is no workaround.

- CSCuc78328

  Symptom: SP crashes followed by an RP reset.

  Conditions: This symptom occurs when multicast-enabled (PIM) tunnels are protected with IPSec.

  Workaround: There is no workaround.

- CSCud22222

  Symptom: On a router running two ISIS levels and fast-reroute, the router may crash if “metric-style wide level-x” is configured for only one level.

  Conditions: This symptom may occur if metric-style wide is configured for only one level on router running both levels, and fast-reroute is configured.

  Workaround: Configure metric-style wide for both levels (by default).

- CSCud24084

  Symptom: Performing a default MDT toggling on a VRF results in the encapsulation tunnel adjacency’s MTU being set to a lower MTU.

  Conditions: This symptom is observed with Cisco IOS XE Release 3.7S (Cisco IOS Release 15.2(4)S) and later releases when the mdt default <> is toggled on a VRF.

  Workaround: Delete and add the affected VRF.

- CSCud24806

  Symptom: Compared to V1 ATM SPA, V2 SPAs are having more latency and bad bandwidth partition.

  Conditions: The symptom is observed under the following conditions:

  1. V2 SPA configured in L3 QoS mode.

2. Policy map contains “no priority queue”.
3. Policy map has more than one QoS class.
4. Each class has a WRED profile configured.

Workaround: While using a policy-map with a WRED profile, use the drop-probability value as 8. This improves the partition.

- CSCud28541

  Symptom: SP crashes on doing **no mpls ip** followed by **shut** on port-channel acting as core link for scaled VPLS and EoMPLS setup.

  Conditions: In case of VPLS going over port-channel protected by IP-FRR, when the port-channel is shut the AToM VC is going down and getting created again. Also the PPO object is getting created afresh. The VC going down is not handled for VPLS case and AToM VC’s pointer are still stored in IP-FRR’s EoMPLS list which is getting access and hence crashing.

  Workaround: There is no workaround.

- CSCud41058

  Symptom: There is a route-map which matches tags and set a new value. This route-map is used in an EIGRP outbound distribute list. One in 10 times based on the received route tag, the correct route tag value is not set while advertising out.

  Conditions: The symptom is observed when you use a route map which matches tags and sets a new tag. Used in **distribute-list route-map** *name* **out**.

  Workaround: Clear the EIGRP process or re-advertise the route.

- CSCud57841

  Symptom: When the Ethernet SPA with Catskills SFPs (GLC-SX-MMD /GLC-LH-MMD) is reloaded, the SPA could go out of service with the following error message:

  ```
  %SMC-2-BAD_ID_HW: SIP0/0: Failed Identification Test in 0/0 [7/0]
  ```

  Conditions: This symptom occurs when the Ethernet SPA is booted with the Catskills SFPs (GLC-SX MMD/GLC-LH-MMD). The defect could be hit during both reload and initialization.

  Workaround: Boot the Ethernet SPA without the Catskills SFPs and insert the Catskills SFPs after the Ethernet SPA has completely booted.

- CSCud66955

  Symptom: SPA-2CHT3-CE-ATM is flapping with Nortel Passport due to the fast bouncing of up or down 10s, after the interface is brought up.

  Conditions: This symptom is observed in E3 and DS3 mode.

  Workaround: There is no workaround.

- CSCud90950

  Symptom: Multicast traffic might not flow through when the P2P tunnel is the incoming interface in the Cisco 7600 router.

  Conditions: This symptom occurs in the Cisco IOS Release 12.2SREx and Cisco IOS Release 15.0x.

  Workaround: Shut and no shut of the P2P tunnel interface.

- CSCue01146

  Symptom: SNMP GET fails for VPDN-related MIB.

Conditions: This symptom occurs while receiving an SNMP GET for the MIB before all VPDN configurations are applied.

Workaround: Reload the Cisco router.

- CSCue02242

  Symptom: VLAN-RAM is programmed with VPN as 0. Traffic destined to a particular vpnid is dropped though it comes on a proper VLAN.

  Conditions: This symptom occurs during P2P scaled configuration when the router boots up and notices the VLAN-RAM is programmed with vpnid 0.

  Workaround: Reload the line card.

- CSCue05492

  Symptom: The DHCP snooping client ignores the IPC flow control events from CF.

  Conditions: This symptom is observed when CF gives flow control off event and the DHCP snooping client does not handle it.

  Workaround: There is no workaround.

- CSCue18133

  Symptom: The Cisco 7600 Router crashes at show_li_users.

  Conditions: This symptom is observed under the following conditions: In li-view, create an username: lawful-intercept and li_user password: lab1. Then, attempt its delete by “no username li_user”. Later, show users of LI.

  Workaround: There is no workaround.

- CSCue31321

  Symptom: A Cisco router or switch may unexpectedly reload due to bus error or SegV when running the **how ip cef ... detail** command.

  Conditions: This symptom is observed when the output becomes paginated (---More---) and the state of the CEF adjacency changes while the prompt is waiting on the more prompt.

  Workaround: Set “term len 0” before running the **how ip cef ... detail** command.

- CSCue32450

  Symptom: Filtering based on L4 ports does not happen for redirection to CE.

  Conditions: This symptom occurs when the WCCP service uses a redirect-list and this ACL has its first entry as a “deny”.

  Workaround: Make the first entry in the redirect-list ACL as a “permit”.

- CSCue36197

  Symptom: The Cisco 7600 router may crash while performing the NSF IETF helper function for a neighbor over a sham-link undergoing NSF restart.

  Conditions: This symptom occurs when a router is configured as an MPLS VPN PE router with OSPF as PE-CE protocol. OSPF in VRF is configured with a sham-link and a neighbor router over a sham-link is capable of performing an NSF IETF restart on sham-links.

  Note: This problem cannot be seen if both routers on sham-link ends are Cisco IOS routers.

  Workaround: Disable the IETF Helper Mode protocol by entering the following commands:

  ```
  enable configure terminal router ospf process-id [vrf vpn-name] nsf ietf helper
  disable end
  ```

Note: Disabling Helper Mode will result in an OSPF peer dropping adjacency if the peer is reloaded.

- CSCue43050

  Symptom: VLAN-RAM is programmed with VPN 0. PIM neighborships of random sessions (10-12 out of 30) go DOWN.

  Conditions: This symptom occurs when MVPN is configured with 30 L3VPN sessions. When there is a boot up, PIM neighborships of random sessions (10-12 out of 30) go DOWN.

  Workaround: Remove and add the VRF configuration for these MVPN sessions.

- CSCue44554

  Symptom: Traffic stops forwarding over port-channels configured with FAST LACP after an RP switch over.

  Conditions: This symptom occurs after an RP fail over.

  Workaround: A shut/no shut interface will help recover.

- CSCue47586

  Symptom: For an MGRE tunnel, internal VLANs are not allocated in the standby supervisor.

  Conditions: The symptom is observed when an HA router boots up with MGRE tunnel configurations. Internal VLANs are not allocated in the standby supervisor due to a sync issue during bootup.

  Workaround: There is no workaround.

- CSCue50101

  Symptom: ATM OAM packets are not being sent on the L2TPv3 tunnel when configured in transparent mode.

  Conditions: This symptom is observed when you enable oam-pvc manage on the CE.

  Workaround: There is no workaround.

- CSCue55739

  Symptom: PfR MC/BR session may be flapped, if PfR learn is configured with scale configuration.

  Conditions: This symptom may be observed, if PfR traffic-classes are learned by PfR global **learn** configuration.

  Workaround: Disable PfR global **learn** by configuring **traffic-class filter access-list** pointing to the **deny ip ip any** ACL, and configure PfR learn “list”.

- CSCue59592

  Symptom: Multiple crashes observed with the following tracebacks after upgrading the Cisco IOS Release from 12.2(33)SRC1 to 12.2(33)SRE6:

```
*Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to lock a
semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
9E19F1C 9E1D4FC
```

Conditions: The symptom is observed with a combination of BGP VPNv4 prefixes and PBR enabled on the interface for the VRF and during upgrade of image or reload of the device. If "mls mpls recirc agg" is enabled in global mode, then this crash will not be observed.

Workaround: Enable "mls mpls recirc agg" in global mode.

- CSCue61691

  Symptom: In a dual-homing topology, switching from the backup mode to the nominal mode ends up with the active "source" router sending a data MDT but transmitting on the default MDT.

  Conditions: The symptom is observed on a dual-homing topology with CORE GRE tunnel.

  Workaround: Use the following command:

  ```
  clear ip mroute vrf <>
  ```

- CSCue68761

  Symptom: A leak in small buffer is seen at ip_mforward in Cisco IOS Release 15.1(4)M3. Device: Cisco 2911 Cisco IOS: c2900-universalk9-mz .SPA.151-4.M3.bin

  Conditions: This symptom is observed with the Cisco 2911 running Cisco IOS Release 15.1(4)M3.

  ```
  ------------------ show buffers ------------------
  Buffer elements: 156 in free list (500 max allowed) 11839912 hits, 0 misses, 617
  created
  Public buffer pools: Small buffers, 104 bytes (total 45187, permanent 50, peak 45187 @
  10:04:00): 0 in free list (20 min, 150 max allowed) 7968057 hits, 202704 misses, 2128
  trims, 47265 created 71869 failures (680277 no memory)
  ------------------ show buffers usage ------------------
  Statistics for the Small pool Input IDB : Mu1 count: 45180 Caller pc : 0x22CF95C4
  count: 45180 Resource User: IP Input count: 45180 Caller pc : 0x22381654 count: 2
  Resource User: Init count: 2 Output IDB : Mu1 count: 4 Caller pc : 0x2380114C count: 4
  Resource User: PIM regist count: 4 Number of Buffers used by packets generated by
  system: 45187 Number of Buffers used by incoming packets:
  ++++++++++++++++++++++++++++small buffer packet++++++++++++++++++++++++++++++++
  <snip>
  Buffer information for Small buffer at 0x2A815220 data_area 0xD9DEB04, refcount 1,
  next 0x0, flags 0x2080 linktype 7 (IP), enctype 16 (PPP), encsize 2, rxtype 1 if_input
  0x30F21520 (Multilink1), if_output 0x0 (None) inputtime 00:02:46.212 (elapsed
  05:55:11.464) outputtime 00:01:22.632 (elapsed 05:56:35.044), oqnumber 65535
  datagramstart 0xD9DEB56, datagramsize 38, maximum size 260 mac_start 0xD9DEB56,
  addr_start 0x0, info_start 0xD9DEB58 network_start 0xD9DEB58, transport_start
  0xD9DEB6C, caller_pc 0x22CF0044
  source: 10.131.124.33, destination: 224.0.1.40, id: 0x55F0, ttl: 11, TOS: 192 prot:
  17, source port 496, destination port 496
  0D9DEB56: 002145C0 002455F0 .!E@.$Up 0D9DEB5E: 00000B11 F14C0A83 7C21E000 012801F0
  ....qL..|!`..(.p 0D9DEB6E: 01F00010 82211200 00000000 000000 .p...!.........
  ```

  Workaround: There is no known workaround. Reboot frees up memory.

- CSCue7605

  Symptom: On a SIP 400 with gigeV2 SPA, when EVC is configured with "encap default", it is seen that sometimes the FUGU TCAM is not programmed with correct VVID for the EVC. This results in incoming traffic reaching the linecard with wrong VVID. This can impact traffic incoming on the EVC.

  Conditions: The symptom is observed with an "encap default" configuration under EVC, or removal and re-application of "encap default" under EVC.

  Workaround: There is no workaround.

- CSCue76251

  Symptom: A BFD session is created for tunnel-tp without any BFD configuration underneath it.

  Conditions: This symptom occurs only on bootup and when there is no BFD configuration underneath tunnel-tp.

  Workaround: There is no workaround.

- CSCue86147

  Symptom: E-OAM state is going down when LACP is going down.

  Conditions: 7600--------- ALU 72

  There are LACP and E-OAM running on both the routers.

  The behavior we observe is that the Cisco 7600 puts a member link into OPER DOWN state if LACP is not received on the port (on active mode). This OPER DOWN link state is propagated to all protocols including E-OAM.

  This is incorrect as E-OAM runs below LACP and hence E-OAM must be able to receive/transmit and has a protocol state of UP irrespective of LACP indication if its state machine indicates so.

  Workaround: There is no workaround.

- CSCue94653

  Symptom: When the port-security configured interface goes to blocking state (MST), the VLANs configured on the port go to not-forwarding state temporarily. The secure mac-addresses are not added back resulting in loss of traffic.

  Conditions: The symptom is observed when the port-security configured interface goes to blocking state.

  Workaround: Shut and no shut the port-security interface to re-add the mac-addresses.

- CSCuf09006

  Symptom: Upon doing a **clear ip bgp * soft out** or **graceful shutdown** on a PE, all VPNv4/v6 routes on an RR from this PE are purged at the expiry of enhanced refresh stale-path timer.

  Conditions: This symptom is observed under the following conditions:

  1. PE must have BGP peering with at least one CE (VRF neighbor) and at least one RR (VPN neighbor).
  2. PE must have a rtfilter unicast BGP peering with the RR.
  3. OS version must have “Enhanced Refresh” feature enabled.
  4. A **clear ip bgp * soft out** or **graceful shutdown** is executed on the PE.

  Workaround: Instead of doing **clear ip bgp * soft out**, do a route refresh individually towards all neighbors.

- CSCuf17009

  Symptom: With PIM enabled on a P2P GRE tunnel or IPSec tunnel, the SP of the Cisco 7600 series router might crash.

  Conditions: This symptom occurs when there are more number of tunnels going via the same physical interface. This issue is seen in Cisco IOS Release SREx and Cisco IOS 15.S based releases only.

  Workaround: There is no workaround.

- CSCuf20409

  Symptom: Netsync: Customer seeing clock in ql-failed state on one Cisco ASR 2RU model.

  Conditions: The issue seen when distributing stratum 1 clock source through its network.

  Workaround: There is no workaround.

- CSCuf30554

  Symptom: Traffic drops with scalable EoMPLS.

  Conditions: This symptom occurs when the MPLS label allocates 21 bit for the label with TE tunnel in the core.

  Workaround: There is no workaround.

- CSCuf30798

  Symptom: SIP 600 crashes.

  Conditions: The symptom is observed with VPLS VC going over GRE tunnel and chassis having both ES+ and SIP 600 card.

  Workaround: Remove VPLS over GRE. This configuration is not supported.

- CSCuf64313

  Symptom: Linecard crash is seen with machine-check exception.

  Conditions: There is no trigger. The crash is random.

  Workaround: There is no workaround.

- CSCuf81275

  Symptom: Some ISG sessions do not pass traffic.

  Conditions: This symptom is observed when you have more than one Line Card for the ISG sessions.

  Workaround: There is no workaround.

- CSCug17808

  Symptom: Redistributed default route not advertised to EIGRP peer.

  Conditions: This symptom is observed when Cisco ASR router is rebooted or the route is cleared via the **clear ip route** command, the route disappears form the spokes.

  Workaround: Clearing the EIGRP Neighborship restores the route on the spokes.

- CSCug23348

  Symptom: The “mod” value in the SSRAM may be inconsistent to the number of ECMP paths.

  Conditions: This occurs with ECMP TE tunnels with **tunnel mpls traffic-eng load-share** *value* commands configured.

  Workaround: Remove the **tunnel mpls traffic-eng load-share** *value* commands from the TE tunnels.

- CSCug50208

  Symptom: A crash is seen due to double free of memory.

  Conditions: The symptom is seen when the accept interface VLAN goes down.

  Workaround: There is no workaround.

- CSCug56942

  Symptom: CUOM could not process “MOSCQEReachedMajorThreshold clear trap” from CUBE SP. For MOSCqe alert clear trap, CUBE should not sent “CurrentLevel Varbind” but should send “csbQOSAlertCurrentValue Varbind”.

  Conditions: This symptom is observed when CUBE SP generates clear trap for voice quality alerts.

  Workaround: The code fix is included in CUBE Cisco IOS Release 15.2(4)S4. Manually clean the alarm at CUOM after root cause is rectified if earlier CUBE version is used.

- CSCug58977

  Symptom: 2.6Gbp/s traffic is observed on both of the VPN SPA interfaces. Traffic direction: Rx on outside interface, Tx on inside interface.

  Conditions: Problem is triggered when fragmented IPSec packet arrives on clear side. Issue observed only in VRF mode.

  Workaround: Reload the IPSec card.

- CSCug68193

  Symptom: Multicast traffic across ES+ cards stop flowing across subinterfaces.

  Conditions: The symptom is observed after a linecard OIR. After the linecard comes up, multicast traffic stops flowing across subinterfaces.

  Workaround: Shut/no shut the subinterface.

- CSCug72891

  Symptom: EIGRP neighbor flaps due to EIGRP SIA. Troubleshooting shows that a race condition causes EIGRP successor loop first and it leads to EIGRP QUERY loop resulting in the neighbor flaps.

  Conditions: The issue is observed when a worse metric update is received from the successor, once the route is already in active state, in a partially peered multiaccess network.

  Workaround: There is no workaround.

- CSCug78098

  Symptom: Supervisor engine crashes and the Cisco IOS software is forced to reload due to PIM process.

  Conditions: This symptom is observed when using the command, **show ip pim rp-hash** right after the BSR RP times out, causes the crash.

  Workaround: Perform these steps in the following order:

  1. Wait for a minute after BSR RP times out before using this command.
  2. Configuring **no ip domain lookup** will make the time taken to execute **show ip pim rp-hash** to a few milliseconds. This will prevent the crash from being reproduced manually.

- CSCug94275

  Symptom: ES+ card crashes with an unexpected exception to CPU: vector 200, PC = 0x0.

  Conditions: The symptom is observed on the ES+ series linecards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCug98820

  Symptom: Multicast RP-Announcement/RP-Advertisement packet is replicated more than one copy per incoming packet. The number of copies is equal to the number of interfaces/IOitems with IC flag enabled (show ip mfib to get the number of IC interfaces).

  Conditions: This symptom is observed when AUTO-RP filter is configured on PIM interfaces.

  Workaround: There is no workaround.

- CSCuh07349

  Symptom: A Cisco 7600 Sup may crash due to SP memory corruption.

  Conditions: This issue is observed on an REP enabled router, which is part of an REP segment. The exact trigger for this issue is not clear.

  Workaround: There is no workaround.

- CSCuh07657

  Symptom: VRF Aggregate label is not re-originated after a directly connected CE facing interface (in VRF) is shut down.

  Conditions: This symptom occurs in an MPLS VPN set-up with Cisco 7600(PE) Router running on Cisco IOS Release 12.2(33)SRE4 with per VRF aggregation. For example:

  ```
  mpls label mode vrf TEST protocol all-afs per-vrf
  ```

  Workaround: Downgrade to Cisco IOS Release 12.2(33)SRE3 or earlier.

- CSCuh16927

  Symptom: Mac entries learned on a trunk link are flushed after removing VLANs.

  Conditions: The symptom is observed when some allowed VLANs are removed on a trunk link, all mac address entries learned on this link are flushed. This is issue is specific to extended VLAN IDs.

  Workaround: Executing ping to destination IP after removing VLANs will recover this condition.

- CSCuh24040

  Symptom: BGP routes are not marked Stale and considered best routes even though the BGP session with the peer is torn down. A hard or soft reset of the BGP peering session does not help.

  For BFD-related triggering, the following messages are normally produced with the BGP-5-ADJCHANGE message first, and the BGP_SESSION-5-ADJCHANGE message second. Under normal conditions, the two messages will have identical timestamps. When this problem is seen, the order of the messages will be reversed, with the BGP_SESSION-5-ADJCHANGE message appearing first, and with a slightly different timestamp from the BGP-5-ADJCHANGE message.

  In the problem case, the BGP_SESSION-5-ADJCHANGE message will also include the string "NSF peer closed the session"

  For example when encountering this bug, you would see:

  ```
  May 29 18:16:24.414: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4 Unicast vpn vrf
  VRFNAME topology base removed from session NSF peer closed the session May 29
  18:16:24.526: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD adjacency
  down
  Instead of: May 29 18:16:24.354: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME
  Down BFD adjacency down May 29 18:16:24.354: %BGP_SESSION-5-ADJCHANGE: neighbor
  x.x.x.x IPv4 Unicast vpn vrf VRFNAME topology base removed from session BFD adjacency
  down
  ```

  Log messages associated for non-BFD triggers are not documented.

Conditions: This symptom is observed when BGP graceful restart is used in conjunction with BFD, but it is possible (but very low probability) for it to happen when BGP graceful restart processing happens when any other type of BGP reset (eg: clear command) is in progress.

Affected configurations all include: router bgp ASN ... bgp graceful-restart ...

The trigger is that BGP exceeds its CPU quantum during the processing of a reset, and gives up the CPU, and then BGP Graceful Restart processing runs before BGP can complete its reset processing. This is a very low probability event, and triggering it is going to be highly dependent on the configuration of the router, and on BGP's CPU requirements.

It is not possible to trigger this bug unless BGP graceful-restart is configured.

Workaround: If you are engaged in active monitoring of router logs, and the bug is being triggered by a BFD-induced reset, you can detect this situation by watching for the reversal of log message order described in the Symptom section, and then take manual steps to remedy this problem when it occurs.

On the problematic router, issue **no neighbor <xxx> activate** command under the proper address-family will clear the stale routes.

The other option is to manually shutdown the outgoing interface which marks the routes as "inaccessible" and hence not been used anymore. This prevents the traffic blackhole but the routes will stay in the BGP table.

More Information: This bug affects all releases where CSCsk79641 or CSCtn58128 is integrated. Releases where neither of those fixes is integrated are not affected.

- CSCuh40275

  Symptom: SNMP occupies more than 90% of the CPU.

  Conditions: This symptom is observed when polling the cefFESelectionTable MIB.

  Workaround: Execute the following commands:

  ```
  snmp-server view cutdown iso included snmp-server view cutdown cefFESelectionEntry
  excluded snmp-server community public view cutdown ro snmp-server community private
  view cutdown rw
  ```

- CSCuh40617

  Symptom: Ping fails when "ncap dot1q" is configured on an FE SPA inserted in bay 1 of flexwan.

  Conditions: This symptom is observed when FE SPA is inserted in bay 1 of flexwan.

  Workaround: Move the SPA to bay 0 of flexwan.

- CSCuh43027

  Symptom: Prefixes withdrawn from BGP are not removed from the RIB, although they are removed from the BGP table.

  Conditions: A withdraw message contains more than one NLRI, one of which is for a route that is not chosen as best. If deterministic med is enabled, then the other NLRI in the withdraw message might not eventually be removed from the RIB.

  Workaround: Forcibly clear the RIB.

- CSCuh48840

  Symptom: Cisco Router crashes.

  Conditions: This symptom is observed under the following conditions:

  1. To re-create the issue:

a. Sup-bootdisk formatted and copied with big size file, like copy 7600 image file around 180M size.

b. Reload box, and during bootup try to write file to sup-bootdisk (SEA write sea_log.dat 32M bytes). Then the issue appear

2. When the issue seen, check the sea_log.dat always with 0 byte

3. No matter where (disk0 or bootdisk) to load image.

4. No matter sea log disk to sup-bootdisk or disk0:. reproduce the issue with "logg sys disk disk0:" config.

```
SEA is calling IFS API to create sea_log.dat, looks like IFS creating file hungs SP.
sea_log.c : sea_log_init_file() -> ifs_open() -> sea_zero_log() -> ifs_lseek() ->
ifs_write()
```

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(3)S5a

Resolved Caveats—Cisco IOS Release 15.1(3)S5a

Cisco IOS Release 15.1(3)S5a is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S5a but may be open in previous Cisco IOS releases.

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  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 Caveats—Cisco IOS Release 15.1(3)S5

Cisco IOS Release 15.1(3)S5 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S5 but may be open in previous Cisco IOS releases.

- CSCsx46323

  Symptoms: When a span monitor source or destination is a port-channel that is automatically created by a service module, the monitor configuration will be discarded on reloads. Also, for a redundant system, restarting the standby will cause the standby to continually reset, until the monitor session source/destination using the PO is removed.

  Conditions: This symptom occurs when the configuration is “monitor session x source interface port-channel yyy”, where yyy is the port-channel that is automatically created by the service module.

  Workaround: Remove the monitor session created on internal port-channels of service modules before any redundant SUP reset or reload. A full system reload will also cause the monitor session to be discarded and will therefore prevent a continual reload cycle of the standby.

- CSCtc42734

  Symptoms: A communication failure may occur due to a stale next-hop.

  Conditions: This symptom is observed when the static route for an IPv6 prefix assigned by DHCP has a stale next-hop for terminated users.

  Workaround: Reload the router.

- CSCtd54694

  Symptoms: A crash is seen for the **show cdp neighbor port-channel** *no and* **show cdp neighbor port-channel** *no* **de?** commands.

  Conditions: This symptom is a rare timing issue.

  Workaround: Use the **show cdp neighbor** and **show cdp neighbor detail** commands for brief and detailed CDP information. Also, the **show cdp neighbor** *interface type no* can be used with the exception that the *interface type* argument should not be *port-channel*.

- CSCtg39957

  The Resource Reservation Protocol (RSVP) feature in Cisco IOS Software and Cisco IOS XE Software contains a DoS vulnerability.

  Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-rsvp

  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

- CSCti51196

  Symptoms: SSH to any IPv6 link-local address connects to itself.

  Conditions: This symptom is observed when you configure SSH and try to connect to any link-local address using SSH.

  Workaround: There is no workaround.

- CSCtj89743

  Symptoms: The Cisco Catalyst 4000 series switches running Cisco IOS Release 12.2(54)SG experiences high CPU when issuing an unsupported command, **https://ip-address**, in which ip-address is accessible from this device.

  Conditions: This symptom is observed with the Cisco Catalyst 4000 series switches.

  Workaround: There is no workaround.

  Further Problem Description: Even if SSL handshake fails, the HTTP CORE process is looping and is scheduled repeatedly.

- CSCtn40771

  Symptoms: The process ACL Header in the **show memory allocating- process totals** command output leaks memory with per-user ACLs and PPP session churn. This will also cause the SSS feature manager process in the **show process memory** command output to appear to have a leak.

  Conditions: This symptom occurs with IPv6 per-user ACLs and session churn.

  Workaround: There is no workaround.

- CSCtn41225

  Symptoms: The IPC port disappears and error messages are displayed on the Cisco CMTS. On the Cisco c76000 platform, it causes a crash.

  Conditions: This symptom is observed while doing a quit operation using the **show ipc util** command.

  Workaround: Do not use the **show ipc util** command.

- CSCtn56097

  Symptoms: Auto mpls-lsp-monitor for pathecho fails.

  Conditions: Auto mpls-lsp-monitor feature does not work due to internal scheduling error.

  Workaround: There is no workaround.

- CSCtn84205

  Symptoms: Bidirectional multicast group traffic will be software switched on a Cisco 7600 Router.

  Conditions: This symptom is observed when there are around 20 + (A) accept interfaces on the router for the bidirectional multicast group.

  Workaround: There is no workaround.

- CSCto87436

  Symptoms: In certain conditions, a Cisco IOS device can crash with the following error message printed on the console:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Proc
  ```

  Conditions: In certain conditions, if an SSH connection to the Cisco IOS device is slow or idle, it may cause a box to crash with the error message printed on the console.

  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 6.3/5.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C CVE ID CVE-2012-5014 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/en/US/products/products_security_vulnerability_policy.html

- CSCtr44299

  Symptoms: The following error message is displayed: Config Sync: Line-by-Line sync verifying failure.

  Conditions: This symptom is observed when you configure service-engine command line interfaces.

  Workaround: There is no workaround.

- CSCtr87413

  Symptoms: Static route that is injected by "reverse-route static" in crypto map disappears when the router receives the delete notify from the remote peer. Static route also gets deleted when DPD failure occurs.

  Conditions: The symptom is observed when you configure "reverse-route static" and then receive a delete notify or DPD failure.

  Workaround: Use **clear crypto sa**.

- CSCts03251

  Symptoms: A Cisco 2921 router running Cisco IOS Release 15.1(4)M with the "logging persistent" feature configured may crash.

  Conditions: This symptom is observed with the "logging persistent" feature.

  Workaround: Disable the "logging persistent" feature.

- CSCts20857

  Symptoms: This issue is actually a fix for CSCtj96916, which is the original issue

  Conditions: This symptom occurs when changing the card type from T3 to E3.

  Workaround: There is no workaround.

- CSCts44393

  Symptoms: A Cisco ASR 1000 crashes.

  Conditions: The symptom is more likely to occur when a large number of VRFs are repeatedly configured and deleted.

  Workaround: There is no workaround.

- CSCts68626

  Symptoms: PPPoE discovery packets causes packet drop.

  Conditions: The symptom is observed when you bring up a PPPoE session and then clear the session.

  Workaround: There is no workaround.

- CSCtu14086

  *MVPN over GRE PIM vrf neighbor not up after SSO

- CSCtu28696

  Symptoms: A Cisco ASR 1000 crashes with **clear ip route ***.

  Conditions: The symptom is observed when you configure 500 6RD tunnels and RIP, start traffic and then stop, then clear the configuration.

Workaround: There is no workaround.

- CSCtu35116

  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.

  Conditions: The symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.

  Workaround: There is no workaround.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: The issue occurs after initiating TFTP copy.

  Workaround: There is no workaround.

- CSCtu42387

  Symptoms: Gigabit and 10 Gigabit Fiber link reporting threshold violation alarm in Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The "%SFF8472-3-THRESHOLD_VIOLATION: Gi0/11: Rx power high alarm" error message is seen on ports.

  Conditions: This symptom is observed on Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The messages are seen with the interface shut or no shut.

  ```
  SFF8472-3-THRESHOLD_VIOLATION Gi5/1: Rx power low alarm; Operating value:
  -28.5 dBm, Threshold value: -24.0 dBm
  ```

  Workaround: Fixing the fiber signal issue or disconnecting the fiber from the transceiver has been known to stop the messages.

- CSCtw50952

  Symptoms: A Cisco ASR series router crashes due to memory exhaustion after issuing the **clear ip ospf**. This symptom was not observed before issuing this command.

  ```
  ACC-CDC-NET-Pri#sh mem stat
                  Head    Total(b)     Used(b)     Free(b)   Lowest(b)
  Largest(b)
   Processor   30097008   1740862372   279628560   1461233812   1460477804
   1453167736
   lsmpi_io   97DD61D0     6295088     6294120         968         968
     968
  ```

  Conditions: This symptom is observed upon executing the **clear ip ospf** causing tunnel interfaces to flap.

  Workaround: There is no workaround.

- CSCtx01918

  Symptoms: On the hub if you configure IVRF for static crypto-map then, after an invalid-spi recovery, the new ISAKMP has an incorrect IVRF (global). IPsec phase II fails with a "proxy identities not supported" error message. The other related issues seen are:

  1. Initial contact not being sent when IKE SA is triggered by invalid-spi recovery.
  2. When quick mode is initiated, it picks the self-initiated IKE SA and hence the QM packet is dropped at the other end.

Conditions: The symptom is observed with a router running HSRP with VRF aware IPsec static crypto map. When you shutdown the active router's external interface, the IPsec tunnel failsover to the standby router. The standby router has an invalid-spi recovery configured. The invalid-spi recovery kicks but new ISAKMP has an incorrect IVRF and IPsec phase II fails.

Workaround: Manually clear SA at spoke site using **clear crypto sa**.

- CSCtx23014

  Symptoms: HSRP hellos cannot be sourced from certain IPs.

  Conditions: This symptom is observed when HSRP hellos cannot be sourced for an IP address with a standby IP address in the same subnet and both are configured in the global VRF. For example:

```
Router(config)#interface Ethernet0/0
Router(config-if)# ip address 192.168.68.13 255.255.252.0
Router(config-if)# standby 68 ip 192.168.70.1
Router(config-if)# standby 68 priority 120
Router(config-if)# standby 68 preempt
Router(config-if)# arp timeout 300
```

  Workaround: Use an IP from the subnet for the SVI interface in the same VRF.

- CSCtx36095

  Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCtx57154

  Symptoms: RP crashes and brings down the router.

  Conditions: This symptom is observed upon shut/no shut of an ES+ access interface configured with 5K EVC.

  Workaround: There is no workaround.

- CSCtx68100

  Symptoms: On a system having SP-RP, the reload reason is not displayed correctly. Once the system crashes, in all subsequent reloads the last reload reason is displayed as crash.

  Conditions: The symptom is observed on a system having SP-RP. The reload reason is shown wrongly when the **show version** CLI is executed.

  Workaround: There is no workaround.

- CSCty07558

  Symptoms: DHCPv6 packets are dropped on a Cisco 7600 switch. For example, they are not flooded.

  Conditions: This symptom is observed when there is no IPv6 address on an SVI or if l2 VLAN has SVI in shut state (default existence after a new ACL feature).

  Workaround: Two possible workarounds which essentially serve as the fix due to the limitations they impose:

  1. When working with a pure L2 VLAN, remove ttl rate limiter (selected as default rate limiter on Cisco7600, but not on other boxes) using "no mls rate-limit all ttl-failure". 2)
  2. If the design permits and TTL rate limiter is necessary, put a dummy IPv6 address on the SVI or simply configure IPv6 enable on the SVI.

- CSCty12312

  Symptoms: Multilink member links move to an up/down state and remain in this condition.

  Conditions: This symptom occurs after multilink traffic stops flowing.

  Workaround: Remove and restore the multilink configuration.

- CSCty59891

  Symptoms: On the node where shut/no shut is issued, traffic does not reach IPsec VSPA, which is supposed to get encrypted.

  Conditions: This symptom is observed when issuing shut/no shut on the GRE tunnel protected with IPsec and QoS configured on this IPsec tunnel.

  Workaround: Remove and attach “tunnel protection ipsec profile”.

- CSCty65189

  Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.

  Conditions: The symptom is observed when ZBFW is configured.

  Workaround: There is no workaround.

- CSCty74859

  Symptoms: Memory leaks on the active RP and while the standby RP is coming up.

  Conditions: The symptom is observed when ISG sessions are coming up on an HA setup.

  Workaround: There is no workaround.

- CSCty86039

  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with traffic going through some of the tunnels.

  Conditions: This symptom is seen with tunnel interface with QoS policy installed.

  Workaround: There is no workaround.

- CSCty99846

  Symptoms: Cisco IOS software includes a version of OpenSSL that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

  CVE-2009-1386

  This bug was opened to address the potential impact on this product.

  Conditions: This symptom occurs when device is configured with SSLVPN and **svc dtls**.

  Workaround: Disable DTSL with **no svc dtls**.

  Further Problem Description: This problem would only be seen in Cisco IOS when using Anyconnect client with Cisco IOS SSLVPNs, after the initial session has been authenticated and established. Exploitation would result in Cisco IOS reloading.

  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 6.3/5.2: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2009-1386 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/en/US/products/products_security_vulnerability_policy.html

- CSCtz28023

  Symptoms: Traffic is not forwarded for a few mroutes.

  Conditions: This issue is seen when multiple routers in the network are reloaded simultaneously.

  Workaround: Using the **clear ip mroute vrf** *vrf name* command may resolve the issue.

- CSCtz34869

  Symptoms: Aps-channel stops working.

  Conditions: This symptom occurs with an open ring and is seen in the following scenario:

  ```
  A1(po2)(RPL)<=======>(po2)A3 (gig3/2)<=======>(gig3/3)A4
  ```

  Shut down gig3/2 on A3. Does not make A1 into protection.
  => Debugs show no SF packets are being transmitted to A1 which is connected to A3 via "Port-channel"
  => A1 (po2) is RPL of the ring. It is not going to unblocked even after A3-A4 link goes down.

  Workaround: Reload the line card.

- CSCtz39917

  Symptoms: The VC status for CE routers is inactive.

  Conditions: This symptom is observed when PE1 router reload.

  Workaround: There is no workaround.

- CSCtz43626

  Symptoms: Minor or major temperature alarms reported in the syslog:

  ```
  %C7600_ENV-SP-4-MINORTEMPALARM: module 2 aux-1 temperature crossed threshold
  #1(=60C). It has exceeded normal operating temperature range.

  %C7600_ENV-SP-4-MINORTEMPALARM: EARL 2/0 outlet temperature crossed threshold
  #1(=60C). It has exceeded normal operating temperature range.
  ```

  Conditions: The symptom is observed on ES+ series line cards of Cisco 7600 series routers. Specifically, the reported temperature will be far off from reading of other sensors on the line card.

  Workaround: There is no workaround.

- CSCtz44989

  Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.

  Conditions: The issue is seen with IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it become 0.0.0.0). Now this route becomes invalid and BGP is not able to export to another VRF.

  Workaround: There is no workaround.

- CSCtz58941

  Symptoms: The router crashes when users execute the **show ip route XXXX** command.

  Conditions: This symptom is observed during the display of the **show ip route XXXX**, when the next-hops of "XXXX" networks are removed.

  Workaround: The **show ip route XXXX** command (without "XXXX") does not have the problem.

- CSCtz65541

  Symptoms: The following error is encountered in Console logfile:

  ```
  %AAA-3-PARSEERR: Error(2) parser is unable to parse nono IP route vrf
  ```

Conditions: This symptom is observed when large number of L2TP sessions with Radius defined VRF routes are cleared or disconnected.

Workaround: There is no workaround.

- CSCtz71084

  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

```
CE0------------------PE0--------------------RR
                         |                      |
                         |                      |
CE1------------------PE1----------------------|
```

  Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

  This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: no network x.x.x.x mask y.y.y.y

  Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.

  Workaround: Hard clear.

- CSCtz86024

  Symptoms: There is a long delay in joining mcast stream with Cisco IOS 15S releases that are running on RP.

  Conditions: This symptom is seen when there is no (*,G) on the box, and the first packet for the stream creates this entry.

  Workaround: With static joins we can make sure that entry is present in mroute table.

- CSCtz88879

  Symptoms: When testing for DMVPN in a HUB-SPOKE topology, where there are 170 tunnels protected with IPsec on Spoke and one mGRE tunnel on hub. B2B redundancy is configured. No QoS is applied on the scaled IPSec tunnels. Upon doing SSO with this configuration, the a "%VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnelx: allocated idb has invalid vlan id" error message is seen repeatedly on the new active and the router becomes almost inaccessible. As can be seen from **show vlan int usage** command output, there are more than 3K free VLANs on both the Hub and Spoke.

```
*May 14 12:31:10.315: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel87: allocated idb has
invalid vlan id
*May 14 12:31:10.511: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel26: allocated idb has
invalid vlan id
*May 14 12:31:10.543: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel28: allocated idb has
invalid vlan id
*May 14 12:31:10.575: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel90: allocated idb has
invalid vlan id
```

After a continuous flood of error messages, a Granikos crash is seen, and the **show cry eli** command shows only one SPA and this SPA is stuck in INIT state.

Conditions: This symptom occurs when doing a shut/no shut using the **interface range** command, and once all tunnels are up, doing an SSO.

Workaround: There is no workaround.

- CSCtz94902

  Symptoms: Memory allocation failure occurs when attaching to SIP-40 using a web browser.

  Conditions: This symptom occurs on the line card.

  Workaround: Reset the line card.

- CSCtz95756

  Symptoms: The "%INTR_MGR-3-INTR: SIP1/3: SPA ATM1/3 FPGA PCI FIFO" message is seen on 6RU.

  Conditions: This symptom is observed when reloading the PE2 router.

  Workaround: There is no workaround.

- CSCua01641

  Symptoms: The router's NAS-IP address contained in the RADIUS accounting-on packet is 0.0.0.0:

```
RADIUS:  Acct-Session-Id     [44]  10  "00000001"
RADIUS:  Acct-Status-Type    [40]  6   Accounting-On
        [7]
RADIUS:  NAS-IP-Address      [4]   6   0.0.0.0

 RADIUS:  Acct-Delay-Time     [41]  6   0
```

  Conditions: Occurs when you restart the router.

  Workaround: There is no workaround.

- CSCua06598

  Symptoms: Router may crash with breakpoint exception.

  Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.

  Workaround: Disable SNMP IPv6 polling.

- CSCua07927

  Symptoms: MLDP traffic is dropped for local receivers on a bud node.

  Conditions: This issue is seen on doing stateful switchover (SSO) on bud node.

  Workaround: Using the **clear ip mroute vrf** *vrf name* ***** command for the effected VRFs will resume the MLDP traffic.

- CSCua12396

  Symptoms: IPv6 multicast routing is broken when we have master switchover scenarios with a large number of members in stack. Issue is seen on platforms like Cisco 3750E and Cisco 3750X where IPV6 multicast routing is supported.

Conditions: This symptom is observed when IPV6 multicast routing is configured, mcast routes are populated and traffic is being forwarded. Now, in case of master switchover, synchronization between master and members is disrupted. This is seen only for IPv6 multicast routing. Observed the issue with 9-member stack and either during first or second master switchover. No issues are seen for IPv4 multicast routing.

Workaround: Tested with 5-member stack, and no issues are seen. It is recommended to enable IPv6 multicast routing when there is deployment with low members in stack.

- CSCua13848

  Symptoms: The Cisco ASR 1000 crashes.

  Conditions: This symptom is more likely to occur when a large number of VRFs are repeatedly configured and deleted.

  Workaround: There is no workaround.

- CSCua20373

  Symptoms: After SSO, all the GRE tunnels get admin down and stay down until the security module SSC-600/WS-IPSEC-3 comes up. Complete traffic loss is seen during this time.

  Conditions: This symptom is observed when Vanilla GRE tunnels are configured in the system where HA and the IPsec Module SSC-600/WS-IPSEC-3 card is present, “crypto engine mode vrf” is configured and SSO is issued.

  Workaround: Remove the “crypto engine mode vrf” configuration if IPsec is not enabled on the router.

- CSCua25671

  Symptoms: After adding the source interface in RSPAN, there is huge flooding to all trunks allowing RSPAN VLAN starts, even if there is no traffic on the RSPAN source interface.

  Conditions: This symptom is observed under the following conditions:

  1. The router has a RSPAN source session.
  2. The source interface being added to the RSPAN source session is on ES+.
  3. Any of the ES+ modules in the system has an interface on the RSPAN VLAN (that is, at least one of the interfaces on an ES+ module carries RSPAN replicated traffic).
  4. The online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, are enabled on the ES+ module which has 2 and 3 mentioned above.

  Workaround 1: Disable the online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, on the ES+ module which has the RSPAN source.

  Workaround 2: If you have to use an interface on the ES+ module as a SPAN source, make sure that no other interface on any of the ES+ modules in the system is in the RSPAN VLAN. If you have to use an interface on the ES+ module to carry RSPAN replicated traffic, make sure that no other interface on any of the ES+ modules in the system is being monitored as an RSPAN source.

- CSCua25943

  Symptoms: CPU Hog is observed on the LC when the number of IPv6 prefixes pumped in is more than 10,000.

  Conditions: This symptom is observed when more than 10,000 IPv6 prefixes are pumped into the router.

  Workaround: There is no workaround.

- CSCua26064

  Symptoms: IPv6 routes in the global routing table take up different adjacency entries.

  Conditions: This symptom is seen when there are 4 core facing tunnels that load balance traffic to these prefixes. The **show mls cef ipv6** *prefix* **detail** command shows the different adjacencies taken by different prefixes.

  Workaround: Have a single tunnel on the core facing side, instead of a load balanced path.

- CSCua26487

  Symptoms: SNMP loops at OID 1.3.6.1.4.1.9.9.645.1.2.1.1.1, and as a result, SNMP walk fails.

  Conditions: This symptom is observed only on the SNMP getbulk request on 1.3.6.1.4.1.9.9.645.1.2.1.1.1.

  Workaround: Exclude the MIB table from SNMP walk using SNMP view. See the below configurations.

  ```
  snmp-server view view name iso included
  snmp-server view view name ceeSubInterfaceTable excluded
  snmp-server community community view view name nterfaceTable excluded
  snmp-server community community view view name
  ```

- CSCua29095

  Symptoms: Spurious memory access is seen when booting the image on a Cisco 7600 router.

  Conditions: This symptom occurs while booting the image.

  Workaround: There is no workaround.

- CSCua31157

  Symptoms: One way traffic is seen on a DMVPN spoke-to-spoke tunnel one minute after the tunnel is built. Issue is only seen intermittently.

  Logs on the spoke that fails to receive the traffic show “Invalid SPI” error messages exactly one minute after the tunnel between the spokes came up.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T1.

  Workaround: There is no workaround.

- CSCua40273

  Symptoms: The Cisco ASR 1000 crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the Cisco ASR 1000 with Cisco IOS Release 15.1(2)S.

  Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: The issue is seen on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua45122

  Symptoms: Multicast even log preallocated memory space needs to be conserved on the low-end platform.

  Conditions: This symptom is observed with multicast even log.

  Workaround: There is no workaround.

- CSCua47570

  Symptoms: The **show ospfv3 event** command can crash the router.

  Conditions: The symptom is observed when “ipv4 address family” is configured and redistribution into OSPFv3 from other routing protocols is configured.

  Workaround: Do not use the **show ospfv3 event** command.

- CSCua52289

  Symptoms: CPU hog is seen on the line card due to Const2 IPv6 process.

  Conditions: This symptom occurs with 4 core facing tunnels. Upon FRR cutover, the CPU hog is observed.

  Workaround: There is no workaround.

- CSCua56999

  Symptoms: Abnormal line card reload occurs.

  Conditions: This symptom occurs when an MVPNv6 scaled router acts as PE on which source traffic is ingressing and the line card is connected on the access side.

  Workaround: There is no workaround.

- CSCua57585

  Symptoms: CPU utilization increases with XE3.3 builds.

  Conditions: Occurs when a device forwards traffic on PPPoE connections.

  Workaround: There is no workaround.

- CSCua57728

  Symptoms: Traffic loss of ~25s is seen upon doing TE FRR Cutover with IPv6 prefixes.

  Conditions: This symptom is observed with four core facing tunnels, and 100,000 IPv6 prefixes. Shut the primary interface and check for the traffic loss.

  Workaround: There is no workaround.

- CSCua61330

  Symptoms: Traffic loss is observed during switchover if,

  1. BGP graceful restart is enabled.
  2. The next-hop is learned by BGP.

  Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.

  Workaround: There is no workaround.

- CSCua67532

  Symptoms: IPsec sessions fail to come up.

  Conditions: This symptom occurs when Site-Site crypto configuration using crypto map is applied on SVI, and when no ISAKMP profile is configured under that crypto map.

  Workaround: There is no workaround.

- CSCua67998

  Symptoms: System crashes.

  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.

Workaround: There is no workaround.

- CSCua68243

  Symptoms: IGMP and PIM control packets are not reaching RP. As a result, the mac-address table for IGMP snooping entries is not populated.

  Conditions: This can be seen on a Cisco 7600 series router that is running Cisco IOS where IGMP and PIM control packets come in on an SVI only after the condition where the SVI link state goes down and comes up again. This does not affect routed ports.

  Workaround: In the SVI configuration mode:

  1. Unconfigure PIM by using **no ip pim**.
  2. Unconfigure IGMP snooping by using **no ip igmp snooping**.
  3. Re-enable both PIM and IGMP snooping.

- CSCua68398

  Symptoms: The ES+ card crashes.

  Conditions: This symptom is observed with a scaled EVC and VPLS configurations.

  Workaround: Stop the traffic. After the line cards boot up and the ports are up, start the traffic.

- CSCua75069

  Symptoms: BGP sometimes fails to send an update or a withdraw to an iBGP peer (missing update)

  Conditions: This symptom is observed only when all of the following conditions are met:

  1. BGP advertise-best-external is configured, or diverse-path is configured for at least one neighbor.
  2. The router has one more BGP peers.
  3. The router receives an update from a peer, which changes an attribute on the backup path/repair path in a way which does not cause that path to become the best path.
  4. The best path for the net in step #3 does not get updated.
  5. At least one of the following occurs:
     - A subsequent configuration change would cause the net to be advertised or withdrawn.
     - Dampening would cause the net to be withdrawn.
     - SOO policy would cause the net to be withdrawn.
     - Split Horizon or Loop Detection would cause the net to be withdrawn.
     - IPv4 AF-based filtering would cause the net to be withdrawn.
     - ORF-based filtering would cause the net to be withdrawn.
     - The net would be withdrawn because it is no longer in the RIB.

  The following Cisco IOS releases are known to be impacted if they do not include this fix:

  - Cisco IOS Release 15.2T and later releases
  - Cisco IOS Release 15.1S and later releases
  - Cisco IOS Release 15.2M and later releases
  - Cisco IOS Release 15.0EX and later releases

  Older releases on these trains are not impacted.

Workaround: If this issue is triggered by a configuration change, you can subsequently issue the **clear ip bgp** *neighbor* **soft out** command.

- CSCua85239

  Symptoms: Flapping BGP sessions are seen if large BGP update messages are sent out and BGP packets are fragmented because midpoint routers have the smaller “mtu” or “ip mtu” configured.

```
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
%BGP-5-ADJCHANGE: neighbor 6.6.6.5 Down BGP Notification sent
%BGP-3-NOTIFICATION: sent to neighbor 6.6.6.5 4/0 (hold time expired) 0 bytes
%BGP_SESSION-5-ADJCHANGE: neighbor 6.6.6.5 VPNv4 Unicast topology base removed from
session BGP Notification sent
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
%BGP-5-ADJCHANGE: neighbor 6.6.6.5 Up
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
```

  Conditions: This symptom is observed between two BGP peers with matching MD5 passwords configured and can be triggered by the following conditions:

  - f the midpoint path has the “mtu” or “ip mtu” setting that is smaller than the outgoing interface on BGP routers, it will be force the BGP router to fragment the BGP packet while sending packets through the outgoing interface.
  - Peering down and the MD5 error do not always occur. They occur only once or twice within 10 tests.

  Workaround: There is no workaround.

- CSCua85837

  Symptoms: Depending on the aces in the redirect-list ACL used, only a subnet of the traffic gets redirected based on ports.

  Conditions: This symptom is observed when the WCCP service has a redirect-list ACL applied which in turn has port-specific aces in them.

  Workaround: Remove the L4 operators from the redirect-list ACL.

- CSCua90061

  Symptoms: The WS-IPSEC-3 Module crashes post configuration change.

  Conditions: This symptom occurs when you dynamically modify the GRE tunnel protected with IPsec to the sVTI tunnel and vice versa while traffic is traversing across the IPsec tunnel.

  Workaround: There is no workaround.

- CSCua98690

  Symptoms: The ES+/ES20/SIP-400 (any card which supports EVC) card may crash due to memory corruption.

  Conditions: This symptom is observed when the MAC ACL is configured on EFP.

  Workaround: There is no workaround.

- CSCua99035

  Symptoms: When enabling the “mls mpls tunnel-recir”, the Tunnel Reserved VLAN 6RD tunnel is allocated. If there is a Tunnel Reserved VLAN, then an extra VPN is allocated. VPN space will be exceeded when you scale up the 6RD tunnel, and you will notice VPNMAP-SP-2-SPACE_EXCEEDED messages. You can verify the output of the VPN table.

```
RTHS_UUT_PE1-sp#sh platform software vpn status
Errors:
```

```
 Exceeded Space: 998  ----------------------------------------> exceeded the
VPN Space
Entries reserved for 6VPE:  255
Entries used by 6VPE:       255 ---------------------------------> We have 253
IPv6 VRF, but it is showing more than configured VRF.
Entries free on 6VPE:       0
Entries used by no-v6 VRFs: 500
Entries used by MLS applic: 3
Entries free for all no-v6: 3337
```

Conditions: This symptom is observed under the following conditions:

1. Configure the ""“mls mpls tunnel-recir” on the router along with the 6RD Tunnel configuration.
2. When you insert ES-20 into the existing system, “mls mpls tunnel-recir” will be configured by default.

Workaround: There is no workaround.

- CSCua99969

  Symptoms: IPv6 PIM null-register is not sent in the VRF context.

  Conditions: This symptom occurs in the VRF context.

  Workaround: There is no workaround.

- CSCub07673

  Symptoms: IPsec session does not come up for spa-ipsec-2g if ws-ipsec3 is also present. “Volume rekey” is disabled on Zamboni.

  Conditions: This symptom occurs if we have “volume rekey” disabled on Zamboni.

  Workaround: Do not disable the volume rekey on Zamboni.

- CSCub07855

  Symptoms: The VRF error message is displayed in the router.

  Conditions: This symptom occurs upon router bootup.

  Workaround: There is no workaround.

- CSCub10951

  Symptoms: At RR, for an inter-cluster BE case, there are missing updates.

  Conditions: This symptom is observed with the following conditions:

  1. The following configuration exists at all RRs that are fully meshed:
  – bgp additional-paths select best-external
  – nei x advertise best-external
  2. For example, RR5 is the UUT. At UUT, there is,
  – Overall best path via RR1.
  – Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called “ic_path_rr5”.
  – Initially, RR5 advertises “ic_path_rr5” to its nonclient iBGP peers, that is, RR1 and RR3.

3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.
4. At PE6, reconfigure the route so that RR5 will have "ic_path_rr5" as its "best-external (internal) path". At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.

Workaround: Hard/soft clear.

- CSCub21468

  Symptoms: UDP header is corrupted randomly.

  Conditions: This symptom is observed with the Cisco 7609-S (RSP720-3C-GE) running Cisco IOS Release 12.2(33)SRE5, with the VRF Aware LI feature.

  Workaround: There is no workaround.

- CSCub23231

  Symptoms: Very specific events/packet types cause the ES20 LC to stop passing traffic. Information on these events and packets that lead to the issue are not known currently.

  Conditions: This symptom occurs when the ES20 interface has an EVC or MPLS configuration.

  Workaround: Reload LC.

- CSCub31902

  Symptoms: Alignment correction tracebacks are seen from within the diag_dump_lc_l2_table() cosmetic issue, which create temporary memory inconsistencies in the function.

  Conditions: This symptom occurs in normal conditions, during bootup time, provided testMacNotification fails.

  Workaround: Disable bootup diagnostics or disable the testMacNotification health monitoring test.

- CSCub36356

  Symptoms: Scaling up routes result in huge memory allocations, eventually depleting the SP memory, leading to MALLOC FAIL and subsequent system crash.

  Conditions: This symptom occurs in normal conditions.

  Workaround: There is no workaround.

- CSCub36376

  Symptoms: Traffic is seen to be sent out of the bridging subinterface even when it is in the shutdown state. This issue is seen on the SPA Gigabit Ethernet interface. The issue occurs on all V2 Gigabit Ethernet SPAs.

  Conditions: This symptom is observed when the Gigabit Ethernet interface on the SPA sends traffic even in shutdown state.

  Workaround: There is no workaround.

- CSCub39268

  Symptoms: Cisco ASR 1000 devices running an affected version of IOS-XE are vulnerable to a denial of service vulnerability due to the improper handling of malformed IKEv2 packets. An authenticated, remote attacker with a valid VPN connection could trigger this issue resulting in a reload of the device. Devices configured with redundant Route Processors may remain active as long as the attack is not repeated before the affected Route Processor comes back online.

  Conditions: Cisco ASR1000 devices configured to perform IPSec VPN connectivity and running an affected version of Cisco IOS-XE are affected. Only authenticated IKEv2 connection is susceptible to this vulnerability.

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-2012-5017 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/en/US/products/products_security_vulnerability_policy.html

- CSCub39296

  Symptoms: Unexpected exception to CPU: vector 200, PC = 0x0. Traceback decode is irrelevant.

  Conditions: The symptom is observed on the ES+ series line cards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCub47520

  Symptoms: "Match dscp default" matches router initiated ARP packets.

  Conditions: This issue seen on Cisco 7600 ES+ line cards.

  Workaround: Classify router generated packets using source mac address using a MAC ACL.

- CSCub48120

  Symptoms: Sp crash is observed @oce_to_sw_obj_type on a router reload.

  Conditions: This symptom is seen with core link flap at remote end during IP- FRR cutover.

  Workaround: There is no workaround.

- CSCub48262

  Symptoms: The router crashes in ROMmon.

  Conditions: This symptom occurs in RSP.

  Workaround: There is no workaround.

- CSCub53398

  Symptoms: The router crashes on bootup.

  Conditions: This symptom occurs when the router is booted up with a scaled MVPNv6 configuration. This issue is highly dependent on the "back walk" timing and sequence; hence, the probability to encounter the issue is low.

  Workaround: Disable power to all DFC modules on reload and bring them up one by one post reload.

- CSCub54261

  Symptoms: In an MLDP + MVPNv6 setup, abnormal RP reload occurs after the deletion and addition of few subinterfaces on the encapsulated PE.

  Conditions: This symptom occurs after deletion and addition of few subinterfaces on the router acting as the encapsulated PE on the access side for a few VRFs running MLCP inband.

  Workaround: There is no workaround.

- CSCub54872

  Symptoms: A /32 prefix applied to an interface (e.g.: a loopback) is not being treated as connected. This can impact the connectivity of the /32 prefix.

Conditions: The symptom is observed when the prefix applied to an interface is for a host route (/32 for IPv4 or /128 for IPv6).

Workaround: Use a shorter prefix.

Further Problem Description: This issue does not affect software switching platforms.

- CSCub58312

  Symptoms: When IGMP query with source IP address 0.0.0.0 is received on an interface, it is marked as mrouter port for that VLAN.

```
Router#show ip igmp int vlan 1
Vlan1 is up, line protocol is up
  IGMP querying router is 0.0.0.0 <----

Router#sh ip igmp snooping mrouter
vlan            ports
-----+---------------------------------------
   1  Po1,Po8,Router<-----
```

  Conditions: This symptom is seen when IGMP query with source IP address 0.0.0.0 is received.

  Workaround: There is no workaround.

- CSCub70336

  Symptoms: The router can crash when “clear ip bgp *” is done in a large-scale scenario.

  Conditions: This symptom is observed only in a large-scale scenario, with ten of thousands of peers and several VPNv4/v6 prefixes.

  Workaround: “clear ip bgp *” is not a very common operation. Hence, this issue has not been observed by customers. The crash can only happen when “clear ip bgp *” is done. The workaround is not to execute “clear ip bgp *”.

- CSCub73787

  Symptoms: The RSP720 may crash if a high rate of traffic is punted to the RP.

  Conditions: This symptom occurs on a Cisco 7600 with RSP720. It is specific to a driver used only by the RSP720. Other supervisor models are not affected. The issue is only seen in Cisco IOS Release 15.1(03)S and later releases, because of a code change made to the RSP720 driver.

  Workaround: Isolate and stop the traffic being punted to the RP.

- CSCub78830

  Symptoms: Traffic matching WCCP service gets black-holed.

  Conditions: This symptom is observed in vrf-wccp scenario and on redirection into MPLS cloud using GRE encap.

  Workaround: There is no workaround.

- CSCub79035

  Symptoms: Multicast traffic will get route cached on the receiver/decap node resulting in traffic drop and slight increase in RP/SP CPU.

  Conditions: This symptom is seen when multicast traffic flowing over GRE tunnel protected with IPsec and PIM is enabled on the GRE tunnel.

  Workaround: There is no workaround.

- CSCub86706

  Symptoms: After multiple RP switchover, the router crashes with the "UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO" error.

  Conditions: This symptom is observed with MVPN with 500 VRFs, when performing multiple switchovers on PE1.

  Workaround: There is no workaround.

- CSCub87579

  Symptoms: Multicast traffic gets forwarded to the wrong tunnel protected with IPsec.

  Conditions: This symptom is observed when Multicast (PIM) is enabled on the GRE tunnel protected with IPsec on the Cisco 7600.

  Workaround: Shut/no shut on the tunnel protected with IPsec resolves the issue.

- CSCub89711

  Symptoms: The **atm** keyword for the **show** command disappears.

  Conditions: This symptom occurs when you do a powered shutdown of the SPA card and bring it back up using the **no** form of the previous command.

  Workaround: There is no workaround.

- CSCub91428

  Symptoms: Internal VLAN is not deleted even after waiting for 20 minutes, and the VLAN cannot be reused.

  Conditions: This symptom is seen with any internal VLAN allocated dynamically that is not freed up after 20 minutes in the pending queue.

  Workaround: There is no workaround.

- CSCub91546

  Symptoms: Traffic is dropped silently on the VLAN.

  Conditions: This symptom is observed when all the VLANs in the router are used (0 free VLAN). Any new internal VLAN creation will fail, and an appropriate error message is not shown.

  Workaround: There is no workaround.

- CSCub91815

  Symptoms: Certificate validation fails with a valid certificate.

  Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.

  Workaround: There is no known workaround.

- CSCub98140

  Symptoms: The router crashes at pak_subblock_share. CDETS commit is a cause for this issue. It is not a part of the released code.

  Conditions: This symptom occurs at pak_subblock_share. This issue is not a part of the released code.

  Workaround: There is no workaround.

- CSCub98588

  Symptoms: The IPsec session does not come up for spa-ipsec-2g if you have disabled "Volume Rekey".

Conditions: This symptom occurs when “Volume Rekey” is disabled on spa-ipsec-2g.

Workaround: Do not disable the “Volume Rekey” on spa-ipsec-2g.

- CSCuc06024

  Symptoms: Traffic flowing through EVCs that do not belong to any service group will see incorrect bandwidth values because of wrong bandwidth value programmed on the port-default node.

  Conditions: This symptom is seen when a mixture of flat and HQoS SGs having bandwidth configurations on their policies are applied on PC EVCs. Two mem- links are part of this PC, and default load-balancing is used.

  Workaround: There is no workaround.

- CSCuc10586

  Symptoms: In the Cisco 7600, multicast traffic does not flow in some scenarios. In the case of PIM SM mode, many times, (*,G) is present, but not (S,G) in mroute. In the case of PIM SSM mode, (S,G) is present but still traffic does not flow through.

  Conditions: This symptom is observed only with Cisco IOS Release 15S-based releases.

  Workaround:

  – Either use a different source IP or a different group IP.
  – Reload the module.

- CSCuc15810

  Symptoms: MVPN over GRE PIM VRF neighbor is not up after SSO.

  Conditions: This symptom is seen when MVPN over GRE PIM VRF neighbor is not up after SSO.

  Workaround: There is no workaround.

- CSCuc19046

  Symptoms: Active Cisco IOSd was found to have crashed following the “clear ip mroute *” CLI.

  Conditions: This symptom occurs with 4K mroutes (2k *,G and 2K S,G) running the FFM performance test suite.

  Workaround: There is no workaround.

  Further Problem Description: So far, this issue is only seen in the FFM performance test script.

- CSCuc28757

  Symptoms: IPv6 HbH Traffic traversing across BD SVIs will not be rate-limited by HbH rate-limiter that is configured.

  Conditions: This symptom is seen when enabling HbH rate-limiter on an NP of ES+ and IPv6 HbH traffic traversing across SVIs part of EVC BD of ES+ interface.

  Workaround: There is no workaround.

- CSCuc29884

  Symptoms: Outage and CPU remain astonishingly high against XDR MCAST process on a scaled HWO BFD testbed.

  Conditions: This symptom is seen after a router reload, when OSPF converge is getting completed, and started 10g traffic through the box.

  Workaround: There is no workaround.

- CSCuc32119

  Symptoms: Traffic drop is seen due to misprogramming in the VLAN RAM table.

  Conditions: This symptom is observed when the router is reloaded multiple times.

  Workaround: There is no workaround.

- CSCuc35935

  Symptoms: Traffic coming in with a particular label might experience drops on ES+.

  Conditions: This symptom is observed with traffic coming in on the ES+ interface with MPLS enabled. This issue is seen when the box has AToM (Scalable mode on the Cisco 7600) configured.

  Workaround: Reset the core facing ES+ module.

- CSCuc38851

  Symptoms: DHCP snooped bindings are not restored after an RTR reload.

  Conditions: This symptom might occur when bindings are learnt on Cisco ES20 EVCs.

  Workaround: After the RTR is UP, renew from the agent database by issuing the **renew ip dhcp snooping database** *URL* command.

- CSCuc41369

  Symptoms: Complete traffic loss occurs for V6 mroutes.

  Conditions: This symptom occurs during deletion and addition of VRFs for the MVPNv6 inband signaling configuration.

  Workaround: There is no workaround.

- CSCuc46356

  Symptoms: Router hangs and crashes by WDOG.

  Conditions: This symptom occurs when IPv6 ACL is applied to a port-ch sub-if. The sub-if is deleted followed by deletion of the ACL.

  Workaround: Delete the ACL before deleting the port-ch sub-if.

- CSCuc48162

  Symptoms: EVC Xconnect UP MEP is sending CCMs when the remote EFP is shut.

  Conditions: This symptom occurs when EFP is admin down.

  Workaround: There is no workaround.

- CSCuc55346

  Symptoms: SNMP MIB cbQosCMDropPkt and cbQosCMDropByte report 0.

  Conditions: This symptom is observed with Cisco IOS Release15.1(3)S1 and Cisco IOS Release 15.2.This issue is not seen with Cisco IOS Release 12.2(33)SRE4.

  Workaround: Use SNMP MIB cbQosPoliceExceededPkt and cbQosPoliceExceededByte.

- CSCuc60245

  Symptoms: Pseudowires stop passing traffic until the LSP is reoptimized.

  Conditions: This symptom is observed when pseudowires stop passing traffic until the LSP is reoptimized.

  Workaround: The common fix is reoptimizing the LSP onto a new path in one or both directions.

- CSCuc65424

  Symptoms: On dual RP configurations, a standby route processor might crash when establishing new interfaces (could be PPP sessions).

  Conditions: This symptom is observed when IDB reuse is turned on on a dual RP configuration, and when some interfaces are deleted and created again.

  Workaround: Turn off the IDB reuse option.

- CSCuc72244

  Symptoms: On the Cisco 7600, both sides running Cisco IOS Release SRE4, Ethernet SPA configured with “negotiation Auto” and changed to “no negotiation auto”. The interface is operating in half-duplex instead of full-duplex mode.

  Conditions: This is a timing issue seen when configuring/un-configuring auto-negotiation or when doing continuous router reload.

  Recovery action: Configuring “shut" “ and “no shut” on the interface changes the duplex state to full-duplex.

  Workaround: There is no workaround.

- CSCuc90011

  Symptoms: Memory leak is caused by executing “show vpdn history failure” after PPP authentication failure.

  Conditions: This symptom occurs when executing the “show vpdn history failure” CLI.

  Workaround: There is no workaround.

- CSCuc96345

  Symptoms: ARP exchange between the Cisco 7600 and the client device fails. The Cisco 7600 has an incomplete ARP entry in its ARP table for the client. This issue is likely to be seen between the Cisco 7600 and other Cisco platforms with MAC address 6073.5Cxx.xxxx. The incoming ARP reply is parsed by the platform CEF as an IP packet and dropped.

  The following OUIs (as of October 30, 2012) are affected: (first 3 bytes from MAC address/MAC starts with)

  14-73-73

  20-73-55

  4C-73-67

  4C-73-A5

  54-73-98

  60-73-5C (One of Cisco's OUI ranges)

  64-73-E2

  70-73-CB

  8C-73-6E

  98-73-C4

  A0-73-32

  C4-73-1E

  D0-73-8E

  F0-73-AE

F4-73-CA

Conditions: This symptom is observed with the EVC pseudowire and 802.1q subinterface on the same physical interface, and connectivity via the subinterface is affected.

Sample configuration:

```
interface TenGigabitEthernet3/1
  service instance 2013 ethernet
    encapsulation dot1q 411 second-dot1q 200
    rewrite ingress tag pop 2 symmetric
    xconnect 10.254.10.10 3350075 encapsulation mpls
interface TenGigabitEthernet3/1.906
  encapsulation dot1Q 906
  ip address 10.10.10.1 255.255.255.0
```

Workaround:

- There should be a static ARP entry on the Cisco 7600 for the client's MAC and IP.
- Change the MAC address of client to a nonaffected OUI.

- CSCuc97711

  Symptoms: After SSO, traffic on the P2P-GRE tunnel within an MVPN may be affected.

  Conditions: This symptom is observed with Cisco IOS Release SREx- and RLSx-based releases.

  Workaround: Shut/no shut the P2P tunnel interface.

- CSCud03273

  Symptoms: All the paths using certain next-hops under the route-map are marked inaccessible.

  Conditions: This symptom occurs under the following conditions:

  1. Configure peer groups.
  2. Apply BGP NHT with route-map (no BGP neighbors are created or added to peer groups).
  3. Configure the Prefix-list.
  4. Configure the route-map.
  5. Configure the BGP neighbor and add them to peer groups.

  Workaround: Configure "route-map permit *seq-num name*" or activate at least one neighbor in "address-family ipv4".

- CSCud07856

  Symptoms: SP crashes at "cfib_update_ipfrr_lbl_ref_count".

  Conditions: This symptom is observed with a scaled IP-FRR configuration.

  Workaround: Remove the IP-FRR configuration.

- CSCud17934

  Symptoms: PW redundancy on the Cisco 7600 does not work when the primary VC goes down and the backup VC takes over, and CE to CE communication is broken.

Conditions: This symptom is observed with the following conditions:

- The MPLS facing LC is WS-X6704-10GE. - The CE facing LC is ES+.

Workaround: Use another HW on the MPLS core.

- CSCud19230

  Symptoms: ES+ line card reload occurs with the following error messages:

```
%PM_SCP-SP-1-LCP_FW_ERR: System resetting module 2 to recover from error:
x40g_iofpga_interrupt_handler: LINKFPGA IOFPGA IO Bus Err val: 4214784 Bus
Error Add:332 Bus Err
data: 0

%OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled Off (Module Reset
due to exception or
user request)

%C7600_PWR-SP-4-DISABLED: power to module in slot 2 set Off (Module Reset due
to exception or user
request)
```

  Conditions: This symptom is observed with the ES+ line card.

  Workaround: There is no workaround.

- CSCud19257

  Symptoms: NAT CLIs expose the **vrf** keyword on the Cisco 7600, which is not supported.

  Conditions: This symptom is observed with a NAT configuration.

  Workaround: Do not use the **vrf** keyword for NATing on the Cisco 7600.

- CSCud27379

  Symptoms: WS-SUP720-3B running Cisco IOS Release 12.2(33)SRE4 crashes at get_alt_mod after issuing “sh run int g4/13” with several trailing white spaces until the cursor stops moving.

  Conditions: This symptom occurs when you issue the **show run interface** command with trailing spaces until the cursor stops moving.

  Workaround: Do not specify trailing spaces at the end of the **show run interface** command.

- CSCud28759

  Symptoms: SPA crash is seen when invoking spa_choc_dsx_cleanup_atlas_ci_config with no data packed.

  Conditions: This symptom is observed when the packed data size should be 1 and the status should be success.

  Workaround: There is no workaround.

- CSCud33564

  Symptoms: BFD sessions are not offloaded.

Conditions: This symptom occurs when XDR infra creates a split event for an XDR mcast_grp and the BFD client ignores it. For this bug, the reason for the split is that a slot is not able to process messages as fast as other slots, thus causing distribution for all slots to block while it catches up. This issue typically occurs with either of the following conditions:

1. The slot has a slower CPU than the others.
2. The amount of work being down during processing of messages is greater than on other slots.

Workaround: Reload ES+ cards.

- CSCud36208

  Symptoms: The multilink ID range has to be increased from the existing 65535.

  Conditions: This symptom is observed specifically with the Cisco MWR1.

  Workaround: There is no workaround. The range is now made configurable based on PD.

Resolved Caveats—Cisco IOS Release 15.1(3)S4

Cisco IOS Release 15.1(3)S4 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S4 but may be open in previous Cisco IOS releases.

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  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

- CSCtj93356

  Symptoms: Batch suspending from platform causes the MFIB on line card to go into reloading state.

  Conditions: This symptom occurs when MFIB on line card goes into reloading state and then finally to purge state after removal/addition of MVRFs is done followed by a line card reset.

  Workaround: There is no workaround.

- CSCtl01184

  Symptoms: Sometimes an EVC that is configured on ES+ sends frames out with CFI bit set in the VLAN tag.

  Conditions: This symptom is observed on EVCs that are configured on ES+.

  Workaround: There is no workaround.

- CSCto02712

  Symptoms: A router that is running Cisco IOS Release 15.1(4)M1 with “proxy- arp” enabled will incorrectly reply to duplicate address detection ARP requests sourced from end devices.

  Some end devices will send an ARP request for their assigned IP to check for duplicate address detection per RFC5227. When this occurs the router should ignore this ARP request. With this issue, the router will respond to the request, which triggers the duplicate address detection on the end device and breaks connectivity between the router and end device.

  Conditions: The symptom is observed with the following conditions:

  – “Proxy-arp” is enabled on client facing Layer-3 interface.

  – End device sends a “duplicate address detection” ARP request on its local subnet.

  Workaround 1: Configure **no ip proxy arp** on client-facing interface.

  Workaround 2: Disable “duplicate address detection” on the end device.

- CSCto16377

  Symptoms: DPD deletes only IPSec SA and not IKE SA.

  Conditions: This symptom is observed when DPD is enabled and peer is down.

  Workaround: Manually delete the stuck ISAKMP session by using the **clear crypto isakmp conn-id** command. You can get the conn-id from the **show crypto isakmp sa** command output.

- CSCto85731

  Symptoms: Crash seen at the nhrp_cache_info_disseminate_internal function while verifying the traffic through FlexVPN spoke-to-spoke channel.

  Conditions: The symptom is observed under the following conditions:

  1. Configure hub and spokes (flexvpn-nhrp-auto connect) as given in the enclosure.
  2. Initiate the ICMP traffic through spoke-to-spoke channel between spoke devices.
  3. Do a **clear crypto session** at Spoke1.
  4. Repeat steps 2 and 3 a couple of times.

  Workaround: There is no workaround.

  Further Problem Description: In the given conditions, one of the spoke device crashed while sending ICMP traffic (10 packets) through FlexVPN spoke-to- spoke channel. The crash decode points to “nhrp_cache_info_disseminate_internal” function

- CSCtq99664

  Symptoms: Traffic does not egress from the interface.

  Conditions: The VRF set on the interface is originally configured for IPv4 and IPv6 address family. If the VRF is reconfigured to remove the IPv4 address family, then all interfaces in that VRF stop sending traffic.

  Workaround: Shut down and re-enable the interface in question.

- CSCtr61623

  Symptoms: The RP crashes at _be_ace_create_acl_node.

  Conditions: This symptom is observed when configuring the 4K DVTI VT.

  Workaround: There is no workaround.

- CSCts12499

  Symptoms: SPA firmware crash at one bay leads to SPA crash in another bay.

  Conditions: This symptom is observed when “test crash cema” is executed from the SPA console. leading to the SPA in the other bay to reload. Also, the crashinfo is not present in the RP disk.

  Workaround: There is no workaround.

- CSCts16569

  Symptoms: The router might reload unexpectedly with scaled serial interfaces configuration.

  Conditions: This symptom occurs during scaling to 4000 NSR peers with 1.5M routes.

  Workaround: There is no workaround.

- CSCts27674

  Symptoms: The static route is not injected to the routing table after enabling crypto map on the interface.

  Conditions: This symptom occurs when you configure “reverse-route static” in the crypto map.

  Workaround: Reconfigure “reverse-route static”.

- CSCts56044

  Symptoms: A Cisco router crashes while executing a complex command. For example:

  ```
  show flow monitor access_v4_in cache aggregate
  ipv4 precedence sort highest ipv4 precedence top 1000
  ```

  Conditions: This symptom is observed while executing the **show flow monitor top** top-talkers command.

  Workaround: Do not execute complex flow monitor top-talkers commands.

- CSCts72911

  Symptoms: In case of a GR/NSF peering, after an SSO switchover, the restarting router (PE, in this case) does not advertise RT constrain filters to the non-restarting peer (RR, in this case).

  Conditions: The symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.

  Workaround: There is no workaround.

- CSCts83046

  Symptoms: Back-to-back ping fails for P2P GRE tunnel address.

  Conditions: The symptom is observed when HWIDB is removed from the list (through **list remove**) before it gets dequeued.

  Workaround: There is no workaround.

- CSCts84132

  Symptoms: Kingpin crashes.

  Conditions: This symptom is occurs during reload with a 4096 subinterface.

  Workaround: Disable CDP.

- CSCtt17762

  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.

  Conditions: The symptom is observed on an IP PIM multicast network.

Workaround: There is no workaround.

- CSCtt43552

  Symptoms: A Cisco router reloads with the **warm-reboot** command.

  Conditions: This symptom is observed on the Cisco router while running Cisco IOS Release 15.2(2.2)T.

  Workaround: There is no workaround. Remove CLI “warm-reboot” from configuration (router will not be able to use warm reboot feature).

- CSCtt99627

  Symptoms: The **lacp rate** and **lacp port priority** commands may disappear following a switchover from active to standby RP.

  Conditions: This affects the Cisco 7600 platform.

  Before performing a switchover one may check the configuration on the standby RP to see if the commands are present or not. If the commands are not present on the standby RP then they will disappear if a switchover occurs.

  Workaround: Prior to switchover if the commands do not show up on the standby RP as described above, then unconfiguring and reconfiguring the command on the active RP will fix the issue.

  Otherwise if the commands disappear after a switchover then the commands must be reconfigured on the newly active RP.

- CSCtu01601

  Symptoms: A Cisco ASR1000 series router may crash while executing the **write memory** command.

  Conditions: This issue may be triggered when the memory in the router is low.

  Workaround: There is no workaround.

- CSCtu23195

  Symptoms: SNMP ifIndex for serial interfaces (PA -4T/8T) becomes inactive after PA OIR.

  Conditions: The symptom is observed with a PA OIR.

  Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.

- CSCtv36812

  Symptoms: Incorrect crashInfo file name is displayed during crash.

  Conditions: The symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw46229

  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.

  Conditions: The symptom is observed with PPP negotiations and the session involving PPPoA.

  Workaround: Ensure all your PPP connections stay stable.

- CSCtw53121

  Symptoms: ES+ goes into major state occasionally on reload or SSO.

  Conditions: This issue is seen in the Cisco 7600 router with 40 gig ES+ line card that is running Cisco IOS Release 15.2(2)S.

Workaround: There is no workaround.

- CSCtw55401

  Symptoms: The SPA-1XCHSTM1/OC3 card goes to out of service after SSO followed by OIR.

  Conditions: This issue is seen with the SPA-1XCHSTM1/OC3 card with Cisco 7600- SIP-200 combination.

  Workaround: There is no workaround.

- CSCtw61872

  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.

  Conditions: The symptom is observed when executing a complex sort with top- talkers on a show command from multiple CLI sessions (note that normal show commands without top-talkers are fine):

  ```
  sh flow monitor QoS_Monitor cache sort highest counter packets top 1000
  sh flow monitor QoS_Monitor cache sort highest counter packets top 10000
  ```

  Workaround: Do not execute complex sorts with top-talkers on the show output from multiple CLI sessions.

- CSCtw70298

  Symptoms: A router crashes after the router boots up with scaled configuration and L2/L3 Distributed EtherChannel (DEC) or port-channel.

  Conditions: This symptom occurs only if there are more than two or more DFCs (ES+ and other equivalents) and with L2/L3 DEC configured such that one of the DFCs takes much longer to come up than the other.

  Workaround: There is no workaround.

- CSCtw80678

  Symptoms: Multilink PPP ping fails when the serial interfaces experience QMOVESTUCK error.

  Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.

  Workaround: “no shut” interface in QMOVESTUCK error message, remove QoS policies on interface & sub-interfaces, remove interface from T1/T3 controller; then rebuild configuration.

- CSCtw88599

  Symptoms: If “port acl” is configured, diagnostics for the port fail during bootup. If the port ACL is on a supervisor port then the router goes for a reload.

  Conditions: The symptom is observed when you configure “port acl” on a switch port and reload the router.

  Workaround: Disable diagnostics for the module.

  This issue will effect only if there is a switchport configured on the router. The issue will not affect the traffic or the filtering based on the ACL, even if the testAclDeny fails and the card is on MajFail (due to this test only).

  As a workaround, we can remove the switchport configs for the ports (if they exist), then give a reload and apply the configs after the router has come up. Alternatively, we can do a “no diagn crash” and try to bring up the router.

In case the router reloads, the ports will not go into shutdown state. Hence, it is a cosmetic issue. It can be ignored. If reloaded in presence of the switchport configs, it should come up after two reloads into minor error state.

- CSCtw98200

  Symptoms: Sessions do not come up while configuring RIP commands that affect the virtual-template interface.

  Conditions: This symptom is observed if a Cisco ASR1000 series router is configured as LNS.

  RIP is configured with the **timers basic** *5 20 20 25* command. Also, every interface matching the network statements is automatically configured using the **ip rip advertise** *5* command. These interfaces include the loopback and virtual-template interfaces too.

  On a Cisco ASR1000 series router, this configuration causes the creation of full VAIs which are not supported. Hence, the sessions do not come up. On Cisco ISR 7200 routers, VA sub-interfaces can be created.

  Workaround: Unconfigure the **timers rip** command.

- CSCtw99991

  Symptoms: Chunk memory leak is seen in the ES+ LC after configuring the IP source guard EVC configurations.

  Conditions: This issue is seen on a Cisco 7600 router with ES+ LC running Cisco IOS interim Release 15.2(1.16)S.

  Workaround: There is no workaround.

- CSCtx04709

  Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as “active” in the EIGRP topology table, and the active timer is “never”.

  Conditions: This symptom is seen when a multiple route goes down at the same time, and query arrives from neighbor router. Finally, neighbor detects SIA for affected router and neighbor state is flap. However, active entry is remaining after that, and route is not updated.

  Workaround: The **clear ip eigrp topology** *network mask* command may remove unexpected active entry.

- CSCtx11598

  Symptoms: A router reload causes a Cisco Shared Port Adapter (SPA) failure with the following error message:

  ```
  % CWAN_SPA-3-FAILURE: SPA-2CHT3-CE-ATM[2/2]: SPA failure
  ```

  This failure can cause the SPA to go to one of the following states:

  - none
  - standby reset
  - down

  This failure leads to unexpected system reload.

  Conditions: This symptom is observed during router reload for 15-20 times.

  Workaround: Ensure that all of the library shared objects are loaded at the time of the SPA initialization.

- CSCtx19332

  Symptoms: A Cisco router crashes when “remote mep” is unlearned while auto EOAM operations are executing.

  Conditions: This symptom is observed if “remote mep” is unlearned from the auto database (shutdown on interface or remote mep reload) while the “IP SLA ethernet-monitor jitter” operation is still running. The crash occurs if the initial control message times out.

  Workaround: There is no workaround.

- CSCtx32329

  Symptoms: When using the **show ipv6 rpf** command, the router crashes or displays garbage for RPF idb/nbr.

  Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.

  Workaround: Do not use static multicast routes, or make sure that the next hop specified can always be resolved. Do not use the **show** command.

- CSCtx42751

  Symptoms: The following error message is displayed:

  ```
  %TRANSCEIVER-3-INIT_FAILURE: SIP2/0: Detected for transceiver module in
  TenGigabitEthernet2/0/0, module disabled
   %LINK-3-UPDOWN: SIP2/0: Interface TenGigabitEthernet2/0/0, changed state to down
  ```

  Conditions: This symptom is observed with the XFP-10GLR-OC192SR transceiver.

  Workaround: Configure “service unsupported-transceiver”.

- CSCtx45373

  Symptoms: Under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command, the “VRF specified does not match this router” error message is displayed. When you issue the **redistribute eigrp 1** command, it gets NVGENd without AS number.

  Conditions: This symptom occurs under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command.

  Workaround: Instead of using the **exit-af-interface** command to exit, if you give a parent mode command to exit, the issue is not seen.

- CSCtx48473

  Symptoms: A router crashes when the following command is executed:

  sh platform software xconnect circuit-index interface *tunnel-name* | **i** *VC- number*

  No crashinfo is generated on the RP and SP. Please see the attached console before the crash.

  Conditions: The above command must be executed.

  Workaround: There is no workaround.

- CSCtx59669

  Symptoms: Spikes are observed in UDP jitter RTT values for MPLS VPN based operations.

Conditions: This symptom is seen on a Cisco 7600 series router when there are a large number of packets configured per UDP operation. Some packets (~1%) exhibit large RTT delays. This is especially noticeable when BGP is exchanging a large number of routes.

Workaround: There is no workaround.

- CSCtx62138

  Symptoms: Standby resets continuously due to Notification timer that Expired for RF Client: Cat6k QoS Manager.

  Conditions: This symptom is observed on a Cisco 7600 HA loaded with scale QoS and GRE + IPsec configurations.

  Workaround: There is no workaround.

- CSCtx66046

  Symptoms: The Standby RP crashes with a traceback listing db_free_check.

  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

  Workaround: Before removing the address, remove the network statement which covers he address of the loopback interface.

- CSCtx66804

  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.

  Conditions: The symptom is observed with the following conditions:

  - “ppp lcp delay 0” is configured.
  - The symptom can be seen on Cisco IOS Release 15.0(1)M5.

  Workaround: Set delay timer without 0.

- CSCtx74051

  Symptoms: When doing an ISSU downgrade, IPv6 Flexible Netflow monitors may be displayed and running config shown with incorrect sub-traffic types.

  Conditions: This symptom happens on a downgrade to Cisco IOS Release 15.2(1)S (XE3.5). The monitors affected are those applied to IPv6. For example CLI like the following:

  ```
  interface fa0/0/0
    ipv6 flow monitor monitor-name input
  ```

  Workaround: Netflow code should still capture packets as expected on Cisco IOS Release15.2(1)S. However do a reboot of the device should be done before saving the running config, as the affected config saved will be incorrect and so will then fail to work on start-up.

- CSCtx74342

  Symptoms: After interface goes down or is OIRed, in a routing table you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next hop interface set to the interface that is down.

  Conditions: The symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).

  Workaround: Configuring SPF throttle timer can change the interval.

  Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

```
Routershow ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/64 [110/10]
     via Ethernet0/0, directly connected
```

- CSCtx77501

  Symptoms: Traffic is dropped at decap side of PE box.

  Conditions: This symptom occurs with SSO at decap side of MVPN set-up, DFC core-facing, 6748 access facing.

  Workaround: Do a switchover.

- CSCtx79462

  Symptoms: OSPF neighborship does not get established.

  Conditions: This symptom is observed when Enabling PFC on a multilink bundle in SIP-400. The OSPF neighborship does not get established.

  Workaround: There is no workaround. Disable PFC to bring up the OSPF neighborship.

  Further Problem Description: The OSPF hello packets get dropped by the peer end because the IP header is corrupted.

- CSCtx85247

  Symptoms: An ES20 line card is reset on doing redundancy switchover of RSPs.

  Conditions: This symptom is seen with redundancy switchover of RSPs.

  Workaround: There is no workaround.

- CSCtx89260

  Symptoms: Re-adding the deleted port channel interface is not initializing the snmp-index.

  Conditions: The symptom is observed when re-adding the deleted port channel interface.

  Workaround: Reloading the standby and then doing an RP switchover or doing a double RP switchover corrects the configuration.

- CSCtx94279

  Symptoms: A line card crashes.

  Conditions: This symptom is observed in switch traffic and flood traffic (line rate and less that 128-byte packet size) with more than one port in the egress path flood.

  Workaround: There is no workaround.

- CSCty03745

  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

Conditions: This symptom occurs when the IPv4 default route exists, that is:

```
ip route 0.0.0.0 0.0.0.0 <next-hop>.
```

Or a certain static/IGP route exists: For example:

```
ip route 0.0.253.0 255.255.255.0 <next-hop>.
```

Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. For example:

```
router bgp 65000
  address-family l2vpn vpls
   neighbor 10.10.10.10 next-hop-self
```

Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- CSCty05092

  Symptoms: EIGRP advertises the connected route of an interface which is shut down.

  Conditions: This symptom is observed under the following conditions:

  1. Configure EIGRP on an interface.
  2. Configure an IP address with a supernet mask on the above interface.
  3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

  Workaround 1: Remove and add INTERFACE VLAN xx.

  Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty05150

  Symptoms: After SSO, an ABR fails to generate summary LSAs (including a default route) into a stub area.

  Conditions: This symptom occurs when the stub ABR is configured in a VRF without “capability vrf-lite” configured, generating either a summary or default route into the stub area. The issue will only be seen after a supervisor SSO.

  Workaround: Remove and reconfigure “area x stub”.

- CSCty06191

  Symptoms: When an IPHC configuration is applied on a multilink bundle interface and the interface is flapped, the IPHC configuration does not apply successfully on a line card.

  Conditions: The symptom is observed with a multilink interface flap.

  Workaround: Unconfigure and then reconfigure the IPHC configuration on the multilink interface.

- CSCty06990

  Symptoms: Intercepted packets are not forwarded to MD.

  Conditions: The symptom occurs randomly after applying an LI tap on a Cisco 7600 with a SIP400 as the dedicated LI service card.

  Workaround: Remove and reapply TAP.

- CSCty13647

  Symptoms: Symptoms vary from one image to another. The following symptoms have been mostly observed:

  1. Spurious memory access tracebacks from SPAN code even when SPAN is not configured.
  2. RP crash when unconfiguring a SPAN session with a particular session number.

Conditions: Always seen on a particular SPAN session number.

Workaround: Use a different a SPAN session number for SPAN configurations to avoid the router crash. Shutdown the SPAN session if not in use. There is no workaround to avoid spurious memory access messages.

- CSCty14596

  Symptoms:

  1. PIM neighbor is not established over routed pseudowire.
  2. PW cannot pass PIM traffic when destination LTL in DBUS header is 0x7ff8.

  Conditions: These symptoms are seen under the following conditions:

  - Configure PIM over routed pseudowire.
  - -Core facing card is ES+.
  - Outgoing interface of the PW is a TE Tunnel over the physical interface.
  - Cisco IOS 15.0(1)S and later releases.

  Workaround: Make the outgoing interface of PW:

  1. Over physical interface only (i.e. without tunnel).
  2. TEFRR over port-channel interface.
  3. Issue will not be observed on ES20.
  4. Issue will not be observed in Cisco IOS Release 15.0(1)S and later releases.

- CSCty21638

  Symptoms: The Cisco 3945 router crashes with the base configuration of SAF/EIGRP.

  Conditions: This symptom occurs when enabling the SAF Forwarder on the Cisco 3945 router box.

  Workaround: There is no workaround.

- CSCty24606

  Symptoms: Under certain circumstances, the Cisco ASR 1000 series router's ASR CUBE can exhibit stale call legs on the new active after switchover even though media inactivity is configured properly.

  Conditions: This symptom is observed during High Availability and box to box redundancy, and after a failover condition. Some call legs stay in an active state even though no media is flowing on the new active. The call legs can not be removed manually unless by a manual software restart of the whole chassis. The call legs do not impact normal call processing.

  Workaround: There is no workaround.

- CSCty29230

  Symptoms: CMFIB entries are not being programmed on the SP and DFCs. Mroute shows both Accept and OILS, ip mfib output also shows Accept interface and Forwarding interface, but CMFIB entries are not programmed.

  Conditions: Cisco 7600 running a Cisco IOS Release 15.1(3)S throttle.

  Workaround: There is no workaround.

- CSCty32851

  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to "multilink ppp".

Conditions: The symptom is observed when the interface is configured with a VRF.

Workaround: Shut down the interface before making the encap configuration change.

- CSCty34020

  Symptoms: A Cisco 7201 router's GigabitEthernet0/3 port may randomly stop forwarding traffic.

  Conditions: This only occurs on Gig0/3 and possibly Fa0/0 as they both are based on different hardware separate from the first three built-in gig ports.

  Workaround: Use ports Gig0/0-Gig 0/2.

- CSCty38305

  Symptoms: The **xconnect vfi vpls** command gets rejected.

  Conditions: This symptom occurs while configuring "xconnect vfi vpls" under the interface VLAN. The error message "command rejected" is received.

  Workaround: There is no workaround.

- CSCty45999

  Symptoms: The "aps group acr 1" line disappears after power off and on a Cisco 7600 router in working and protection groups.

  Conditions: This symptom occurs when the Cisco 7600 router suddenly loses power, and the "aps group acr 1" line does not appear again. If you run the **show controller SONET 1/1/0** command, you will see every E1 on "unconfigured" status.

  Workaround: Delete the "aps protect 1 X.X.X.X" and "aps working 1" lines. The "framing" must be changed in order to delete every E1 channel configuration, then "framing" should be configured as it was in the beginning. Then "aps group acr 1" line is configured as well as "aps protect 1 X.X.X.X" and "aps working 1" lines. Finally every E1 must be configured as it was before this issue occurs. You can copy the E1 configuration before to delete anything and then paste it at the end.

- CSCty51172

  Symptoms: The MAC address learned on L2 DEC on 7600-ES+40G3CXL is not installed as the primary entry on all the member interfaces, if the ingress traffic is on the non-hashed interface for that EFP.

  Conditions: Layer 2 distributed EtherChannel traffic is learned on a hashed interface first and then moved to a non-hashed interface.

  Workaround: Do not use Layer 2 distributed EtherChannel.

- CSCty53654

  Symptoms: Traffic through 6RD tunnel is getting dropped. In the **show mls cef ipv6** *prefix* **detail** command, vlan *vlanid* field will be present. On ES+ line card, the **show platform npc 6rd egress-table vlan** *vlanid* command does not produce any output.

  Conditions: This symptom occurs when using the **clear ipv6 neighbors** command.

  Workaround: There is no workaround.

- CSCty54885

  Symptoms: The Standby RP crashes when the Active RP is removed to do a failover.

  Conditions: This symptom is observed when the last switchover happens with redundancy forced-switchover.

  Workaround: Do a switchover only with redundancy forced-switchover instead of removing the RP physically.

- CSCty68348

  Symptoms: If the OSPF v2 process is configured with the **nsr** command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

  Conditions: This symptom is observed under the following conditions:

  - The OSPF router is configured for “nsr”.
  - **Shutdown/no shutdown** of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- CSCty78435

  Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

  Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

  Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty94289

  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.

  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.

  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- CSCty96049

  Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp

- CSCty96052

  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

  Conditions: It is an extreme corner case/timing issue. Has been observed only once on release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty99331

  Symptoms: CPU hog messages are seen on the console.

  Conditions: This symptom is seen when applying huge rmap with more than 6k sequences on an interface.

Workaround: There is no workaround.

- CSCty99711

  Symptoms: SIP-400 crash may be observed due to illegal memory access.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SRE4 when SIP-400 has PPPoE session scale.

  Workaround: There is no workaround.

- CSCtz01361

  Symptoms: Traffic gets black holed when TE auto-backup is enabled on midpoint router and FFR is configured on the P2MP TE tunnel head end.

  Conditions: This symptom is seen when enabling FRR on the head end with auto- backup already configured on the box.

  Workaround: Remove auto-backup configuration from the midpoint router.

- CSCtz06611

  Symptoms: IPSec tunnel states are UP-IDLE because of broadcast packets that are punted to the CPU. The mac-address of VPN-SPA is not learned properly.

  Conditions: This symptom is a timing issue. You may see it first time or need to try multiple times. This symptom is seen with crypto map plus vrf configuration.

  1. Reload the router with above configuration: the mac-address changes to all FF.
  2. Default the configuration of VLAN (where crypto map and engine is applied), then configure it again with old configuration. Now the mac-address will show all FF.
  3. Create the vlan. Do a **no shutdown**. Attach vrf. Then add crypto map to it.

  Workarounds: For the steps mentioned in condition section above, below are the workarounds respectively.

  Workaround 1: Remove and add “ip vrf forwarding” and then remove and add the **crypto engine** command.

  Workaround 2: Remove and add the **crypto engine** command.

  Workaround 3: Do a **shut/no shut** on the VLAN interface.

- CSCtz08746

  Symptoms: On the 12in1 Serial SPA with hardware version lower than 2.0, an upgrade using “test upgrade” with the latest Cisco 7600 FPD bundles results in the SPA FPD device being downgraded from version 1.2 to 1.1. Subsequently, both auto and manual upgrades fail to bring the SPA FPD version back to 1.2. The SPA goes to the OutOfServ or FpdUpReqd state.

  Conditions: This issue is seen only with the older SPA hardware (hardware version lower than 2.0) when it is plugged into a SIP200 or SIP400 on the Cisco 7600 platform.

  Workaround: Use the latest SPA hardware (hardware version 2.0 or above).

- CSCtz13465

  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.

  Conditions: This symptom is observed with an interface with a policy installed.

  Workaround: There is no workaround.

- CSCtz13818

  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.

  Conditions: The symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use **clear ip route vrf** *vrf-name net mask*.

  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz24047

  Symptoms: Free process memory is being depleted slowly on line cards in the presence of the DLFIoATM feature configured on a PA-A6-OC3 (enhanced Flexwan). Finally memory allocation failures are observed. Use the **show memory proc stat history** command to display the history of free process memory.

  Conditions: Slow Proc Memory depletion is observed on 7600-ES+ cards when installed on a Cisco 7600 router that has DLFIoATM configured on a PA-A6-OC3 hosted on an enhanced Flexwan module.

  Workaround: There is no workaround.

- CSCtz25953

  Symptoms: “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.

  Conditions: The symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- CSCtz26188

  Symptoms: Packet loss is observed on platforms in certain deployments having a large number of prefixes routing traffic onto a TE tunnel.

  Conditions: This symptom occurs if the configured value of the cleanup timer is 60 seconds, then packets might be lost on the platforms where the forwarding updates take longer.

  Workaround: Configure the value of the cleanup timer to 300 seconds.

  mpls traffic-eng reoptimize timers delay cleanup 300

- CSCtz30983

  Symptoms: Crash on ES+ line card upon issuing the “show hw-module slot X tech- support” or “show platform hardware version” command.

  Conditions: This symptom occurs on an ES+ line card.

  Workaround: Do not issue the “show hw-module slot X tech-support” or “show platform hardware version” command on an ES line card unless explicitly mentioned by Cisco.

- CSCtz31888

  Symptoms: After state change of one of the L3 uplink interfaces, STP cost of BPDU PW increases from 200 to 2M, which can lead to blocking state in STP for this PW.

  Conditions: This symptom occurs with state change of one of the uplink L3 interfaces.

  Workaround: Increase the cost of access ring to more then 2M to avoid blocking of the BPDU PW.

- CSCtz54823

  Symptoms: Configuration is getting locked on chopper SPA.

  Conditions: This symptom happens as follows:

  1. Shut down the controller of the SPA.
  2. Reload will bring the SPA in the locked state.

  Workaround: There is no workaround. Erase start up and reload the system to get back to configuration mode.

- CSCtz62680

  Symptoms: “DFC WAN Line Card Software Element Not Found - QOS: TCAM Class ID” errors appear along with BADCHUNKFREEMAGIC errors, leading to an ES20 crash.

  Conditions: When service policies less than 128 kb are added or removed.

  Workaround: There is no workaround.

- CSCtz66770

  Symptoms: When under ATM PVC (SPA-4XOC3-ATM or v2) with MUX encapsulation and OAM enabled, L3 policy-map is applied and PVC goes down.

  Conditions: This symptom occurs when policy-map sets DSCP (to 7) for default- class, and it affects OAM communication.

  Workaround: Use aal5snap encapsulation.

- CSCtz72615

  Symptoms: All interfaces on a Cisco 7600-SIP-200 are down after Cisco IOS downgrade.

  Conditions: This symptom is observed on Cisco 7600 series routers.

  Workaround: There is no workaround.

- CSCtz73836

  Symptoms: The router crashes.

  Conditions: This symptom is observed when the router is running NHRP.

  Workaround: There is no workaround.

- CSCtz78194

  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.

  Conditions: The symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.

  Workaround: Shorten the ISAKMP profile name to less than 31.

- CSCtz80643

  Symptoms: A PPPoE client’s host address is installed in the LNS’s VRF routing table with the **ip vrf receive** *vrf name* command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive** *vrf name* command via the Virtual-Template or RADIUS profile.

  Workaround: There is no workaround.

- CSCtz85907

  Symptoms: A Cisco 7600 should have an MVPNv4 configuration and the system replication mode as egress. Now if “address-family ipv6” is configured under the VRF definition, MVPN traffic might be affected.

  Conditions: SREx and RLSx releases.

  Workaround: Use ingress replication.

- CSCtz89485

  Symptoms: NAT traffic passes through the new standby router following HSRP switchover.

  Conditions: This symptom is observed with HA NAT (NAT with HSRP) mappings with inside global addresses that overlap a subnet owned by a router interface.

  Workaround:

  1. Force a HSRP switchover so that the initial standby router takes activity.
  2. Remove and re-add HSRP NAT mappings on the newly active router.
  3. Force a HSRP switchover back to the initial active router.

- CSCtz97755

  Symptoms: ES card crash and alignment tracebacks on SP are seen.

  Conditions: This symptom is observed with IPv6 unicast and multicast traffic up and running. Unconfiguring IPv6 unicast-routing will lead to this issue.

  Workaround: There is no workaround.

- CSCua10377

  Symptoms: A Cisco router with Circuit Emulation SPA may suffer an SPA crash.

  Conditions: This symptom occurs when the CE T1 circuit is configured by the end user for AT&T FDL, and the end user transmits FDL messages requesting 4- hour or 24-hour performance statistics.

  Workaround: There is no workaround. If possible, contact the end user and have them reconfigure their device for ANSI FDL.

- CSCua13418

  Symptoms: RP-Announce packets are being replicated across all the tunnel interfaces and the count of replication is equal to the number of tunnel interfaces. For example, if there are 3 tunnel interfaces, then each tunnel should forward 1 RP-Announce packet each minute (with the default timer configured). However, in this case, each tunnel is forwarding 3 RP-Announce packets across each tunnel interface. This issue is not specific to the number of interfaces. It can happen with any number of tunnel interfaces.

  Conditions: This symptom is observed when filter-autorp is configured with the **ip multicast boundary** command. This issue is seen on the Cisco 3725 router too, where the incoming packets are being replicated because of the **filter-autorp** command.

  Workaround: Removing filter-autorp resolves the issue. However, you need to remove the **pim** and **boundary** commands first and then reapply the pim and boundary list without the **filter-autorp** keyword. Also, doing this might lead to redesigning of the topology to meet specific requirements.

  int Tun X no ip pim sparse-dense mode no ip multicast boundary XXXXXX filter-autorp

  int TuX ip pim sparse-dense mode ip multicast boundary XXXXXX

- CSCua16786

  Symptoms: When a Cisco 7600 router is placed as a mid-hop-router between the first hop router (FHR) and rendezvous point (RP), with P2P GRE tunnel interface as the FHR facing interface, then PIM-registration might not get completed. The unicast PIM-registration packet might get dropped at the Cisco 7600 router.

  Conditions: This symptom is seen in Cisco IOS Release 12.2(33)SRE6 and RLSx releases.

  Workaround: Delete and create the FHR facing p2p tunnel interface at Cisco 7600 router, which is acting as mid-hop-rtr.

- CSCua30259

  Symptoms: EVC egress traffic does not flow. The frames are dropped by Selene.

  Conditions: This symptom occurs when SPAN is configured on service instance.

  Workaround: There is no workaround.

- CSCua31794

  Symptoms: After reload with the debug image, framed E1 lines are down.

  Conditions: On checking the “show controller SONET”, the default controller framing mode is taken as “crc4”. However before reload the configuration for those E1s were configured as “no-crc4”. Customer configured them on the E1s as “no-crc4” and it started working fine and the “show controller SONET” framing output changed to “no-crc4”. As per running configuration still the configuration is not showing “no-crc4”, as it should show as the default is CRC4. So the current issue is configuring “No-crc4”, it is not showing in running configuration and not saved and after reload it shows again CRC4 and services go down again.

  Workaround: Configure E1s as “no-crc4” and they would be working fine, but such changes are not being saved in configuration, so if reload reoccurs all these services go down again.

- CSCua33287

  Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.

  Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.

  This condition will recover after executing **shut/no shut** on physical interfaces.

  Workaround: There is no workaround.

- CSCua41464

  Symptom: LC crash is seen with script run.

  Conditions: This symptom occurs when the script configures 50 MVPN GRE VRFS, 50 MLDP VRFS, with 100 mroutes each. Crash happens when traffic is sent.

  Workaround: There is no workaround.

- CSCua42089

  Symptoms: Configuring Ingress redirection for service group 61 (Mask) and applying an extended ACL in the outbound direction on the same interface causes software switching even when there are no punt entries in the TCAM.

  Conditions: This symptom is observed when WCCP service 61 with Mask assignment in the Ingress indirection, along with an outbound ACL, is configured on the same interface.

  Workaround: Do not configure the outbound ACL along with a WCCP service.

- CSCua64700

  Symptoms: IPSec tunnel states go to Up-Idle after 4-5 days of router up and running.

  Conditions: This symptom is observed if you have low re-key value. The chances of hitting this issue is high, as with the re-key the new spi gets allocated. This issue is seen with WS-IPSEC-3 and to verify this, check the below counter with the **show crypto ace spi** command.

  If no decrement in spi allocated counter and there is the consistent increment in counter, the chances are high, you will hit this issue.

  Once the value reaches to 61439, you will hit this issue.

```
MTCVPNK03#sh cry ace spi
SPI in use ........................... 0
Normal SPI allocated ................. 61439
```

  Workaround: There is no workaround.

- CSCua88341

  Symptoms: Multicast traffic on P2P GRE tunnel will get dropped.

  Conditions: This symptom usually happens in scenarios where SSO is done after vrf del/add. Here the P2P GRE tunnel will be in the VRF.

  Workaround: **shut/no shut** of the P2P GRE tunnel interface.

Resolved Caveats—Cisco IOS Release 15.1(3)S3

Cisco IOS Release 15.1(3)S3 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S3 but may be open in previous Cisco IOS releases.

- CSCee38838

  Symptoms: A crashdump may occur during a two-call-per-second load test on a gateway, and the gateway may reload.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(7)T and that functions as a gateway when you run a two-call-per-second load test that uses H.323, VXML, and HTTP. The crash occurs after approximately 200,000 calls.

  Workaround: There is no workaround.

- CSCtd86428

  Symptoms: SSH session does not accept IPv6 addresses in a VRF interface, but will accept IPv4 addresses.

  Conditions: The symptom is observed when you specify the VRF name with an SSH that belongs to an IPv6 interface.

  Workaround: You can specify the source interface.

  Further Problem Description: SSH sessions not accept IPv6 addresses in VRF interface, but accepts IPv4 address:

  - Telnet session accepts both v6 and v4 addresses in VRF interface.
  - “Destination unreachable; gateway or host down” message shows in SSH session to IPv6 address in VRF interface.

- CSCtg57657

  Symptoms: A router is crashing at dhcp function.

Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

Workaround: There is no workaround.

- CSCti00319

  Symptom 1: The warning message “Fatal error FIFO” occurs repeatedly upon PPPoEoA Session teardown.

  Symptom 2: On the LC console, the message “Command Indication Q wrapped” keeps appearing.

  Conditions: This symptom is observed on a Cisco ASR1001 router and kingpin router chassis under the following conditions:

  1. High scale session counts.
  2. Range configuration with more than 100 virtual channels (VC).
  3. Back to back creation and deletion of multiple VCs with no time gap.

  Workaround: There is no workaround.

- CSCtj64807

  Symptoms: Router crashes while issuing the **show vlans dot1q internal** command.

  Conditions: The symptom is observed with the following conditions:

  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.

  Workaround 1: For any Cisco 10000 series router which has had its first crash: on any subinterface if the outer VLAN has second-dot1q VLAN as only “any”, immediately delete the subinterface and recreate it. Then add a dummy VLAN/sub-interface to this outer VLAN.

  Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.

  Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only “any” and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtj95685

  Symptoms: A router configured as a voice gateway may crash while processing calls.

  Conditions: The symptom is observed with a router configured as a voice gateway.

  Workaround: There is no workaround.

- CSCtn02372

  Symptoms: QoS installation fails on the CEoP SPA or traffic is not forwarded correctly after a lot of dynamic changes that continuously remove and add VCs, as on CEoP SPA, IfIDs are not freed upon deleting the PVC.

  Conditions: This symptom occurs when continuous bring-up and tear down of VCs causes the SPA to run out of IfIDs.

  Workaround: Reload the Cisco SIP-400 line card.

- CSCtq09712

  Symptoms: A Cisco ASR’s RP crashes due to L2TP management daemon:

```
%Exception to IOS: Frame pointer 0xXXXXXXXXXXXX, PC = 0xZZZZZZZZ IOS Thread backtrace:
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = L2TP mgmt daemon
```

Conditions: This symptom is observed with L2TP when clearing the virtual access interfaces.

Workaround: There is no workaround.

- CSCtq24557

  Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.

  Conditions: The symptom is observed in a large scale scenario.

  Workaround: There is no workaround.

- CSCtq59923

  Symptoms: OSPF routes in RIB point to an interface that is down/down.

  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

  Workaround: Configure “ip routing protocol purge interface”.

- CSCtq77024

  Symptoms: Metrics collection fails on hop0 if route change event occurs.

  Conditions: This symptom is observed when the mediatrace is not passing up an interface type that is acceptable to DVMC when a route change occurs on the node which has the initiator and responder enabled.

  Workaround 1: Remove and reschedule mediatrace session.

  Workaround 2: Remove and reconfigure mediatrace responder.

- CSCtq99488

  Symptoms: Session is poisoned on standby RP after performing account-logon on native IPv6 session.

  Conditions: The symptom is observed upon doing an account-logon on an unauthenticated IPv6 session with L4R applied. The session gets poisoned on the standby. The operation is, however, successful on the active RP.

  Workaround: There is no workaround.

- CSCtr06882

  Symptoms: In some cases, multicast traffic stops to flow on some subinterfaces upon router reload.

  Conditions: This symptom is observed with Cisco IOS Release RLS7.3a.

  Workaround: Perform shut/no shut of the subinterface.

- CSCtr47317

  Symptoms: After a switchover, a Cisco Catalyst 6500 series switch may be replicating some spanned traffic indefinitely and flooding the network with the span copies.

  Conditions: The issue is seen after the following sequence:

  – An internal service module session for a FWSM or other service modules exists:

```
UUT#show monitor session all
Session 1
Type : Service Module Session
```

  – If you attempt to configure a span session with the session number already in use:

```
UUT(config)#monitor session 1 source interface Gi2/7 , Gi2/40
% Session 1 used by service module
```

  - The command seems to be rejected, but it is synchronized to the standby supervisor.
  - A switchover happens.

  Workaround: There is no workaround.

- CSCtr47642

  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the **bgp additional-paths select best- external** command, a specific prefix may not have bestpath calculated for a long time.

  Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

  1. Configure: **bgp additional-paths install** under vpnv4 AF
  2. Configure: **bgp additional-paths select best-external**

  Immediately disable backup path calculation/installation using the **no bgp additional-paths install** command.

  The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

  Workaround: Configure the **bgp additional-paths install** command and the **bgp additional-paths select best-external** command with a delay of 10 seconds.

- CSCtr52740

  Symptoms: Query on an SLA SNMP MIB object using an invalid index can cause the device to crash.

  Conditions: The symptom is observed when querying history information from rttMonHistoryCollectionCompletionTime object using invalid indices.

  Workaround: Instead of using “get”, use “getnext” to list valid indices for the MIB OID.

- CSCtr79905

  Symptoms: Error message seen while detaching and reattaching a service policy on an EVC interface.

  Conditions: The symptom is observed when detaching and reattaching the service policy on an EVC interface when port shaper is configured on the interface.

  Workaround: There is no workaround.

- CSCtr87070

  Symptoms: Enable login failed with error “% Error in authentication”.

  Conditions: The symptom is observed with TACACS single-connection.

  Workaround: Remove TACACS single-connection.

- CSCtr88739

  Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

  Symptom 2: The routes in BGP may not get installed to RIB.

Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

Workaround for symptom 1: Remove “import-route target” and reconfigure route-target.

Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- CSCts13255

  Symptoms: Standby SUP720 crash is observed on the Cisco 7600 router in c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

  ```
  %CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive
  heartbeats
  ```

  Conditions: This symptom is observed on the Cisco 7600 router with mistral based supervisors like SUP720. This issue is fairly uncommon, but affects all the versions after Cisco IOS Release 12.2(33)SRE, including Cisco IOS Releases 15.0S, 15.1S and 15.2S. This does not affect RSP 720.

  Workaround: There is no workaround.

- CSCts15034

  Symptoms: A crash is seen at dhcpd_forward_request.

  Conditions: This symptom is observed with the DHCP relay feature when it is used with a scaled configuration and significant number of DHCP relay bindings.

  Workaround: If possible, from a functional point of view, remove the **ip dhcp relay information option vpn** command. Otherwise, there is no workaround.

- CSCts31111

  Symptoms: Coredump generation fails on the Cisco 800.

  Conditions: This symptom occurs when coredump is configured.

  Workaround: Go to ROMmon, and set a variable WATCHDOG_DISABLE before the coredump happens, as follows:

  ```
  conf t
  config-reg 0x0
  end
  wr
  reload
  yes
  <rommon prompt>
  DISABLE_WATCHDOG=yes
  sync
  set
  conf-reg 0x2102
  reset
  ```

- CSCts57108

  Symptoms: Standby reloads continuously after ISSU RV.

Conditions: The symptom is observed during a downgrade scenario where the active is running Cisco IOS Release 15.1 and the standby is running Release 12.2. Cisco IOS Release 15.1 will be syncing “snmp-server enable traps ipsla” keyword to the standby, but the standby does not understand the new keyword.

Workaround: Remove references to “snmp-server enable traps ipsla” and then perform the downgrade.

- CSCts59564

  Symptoms: PIM neighbor over MDT tunnel goes down.

  Conditions: The symptom is observed with **hw-module reset** of access and core card, followed by an SSO.

  Workaround: There is no workaround.

- CSCts65564

  Symptoms: In a large scale DMVPN environment, a DMVPN hub router may crash in the IOS process under high scale conditions.

  Conditions: This only occurs if CRL caching is disabled (with the command **crl cache none** under the pki trustpoint configuration).

  Workaround: Enable CRL caching (this is the configured default).

- CSCts67465

  Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.

  Conditions: The symptom is observed always, if the standby is configured as an SSO.

  Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCts70790

  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

  Workaround: Remove and re-add the **neighbor default- originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCts71958

  Symptoms: When the router is reloaded due to crash, the **show version** output shows the reload reason as below:

  ```
  Last reload reason: Critical software exception, check
  bootflash:crashinfo_RP_00_00_20110913-144633-PDT
  ```

  After this, the same reason is shown even if the router is reloaded several times using the **reload** command.

  Conditions: The issue seen after a crash.

  Workaround: There is no workaround.

- CSCts97856

  Symptoms: PIM Assert is sent out from a router with metric [0/0], though the router has a less preferred path to reach the Source or RP.

Conditions: This symptom occurs when an mroute is first created and its RPF lookup to the Source or RP is via BGP or Static, which involves recursive lookup, or there is no valid path to reach Source or RP. This issue only occurs in a small window in milliseconds. After the window, the metric [0/0] is corrected.

Workaround: There is no workaround.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCtt02313

  Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

  Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

  Workaround: There is no workaround.

- CSCtt17785

  Symptoms: In the output of **show ip eigrp nei** *det*, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.

  Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).

  Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- CSCtt17879

  Symptoms: The **bgp network backdoor** command does not have any effect.

  Conditions: This symptom occurs:

  – On 64-bit platform systems.

  – When the network is learned after the backdoor has been configured.

  Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt26074

  Symptoms: Memory leak with IP SLAs XOS Even process.

  Conditions: The symptom is observed with IP SLA configured.

  Workaround: There is no workaround.

- CSCtt36757

  Symptoms: The following error message is noticed when configuring QoS on the interface of an ES+ card:

  ```
  %X40G_QOS-DFC9-3-CFN: qos tcam programming failed for policymap
  AGGR-CHA-INTERFACE-OUTPUT-POLICY
  ```

Conditions: The symptom is observed after a misconfiguration in the interface. The interface was misconfigured as switchport which removed the QoS configuration from the interface configuration but not from the linecard. After the interface was configured back to an L3 port, the issue started occurring when the same policy was reapplied.

Workaround: A new policy can be applied but the required policy cannot be applied again.

- CSCtt37516

  Symptoms: Linecard crash with priority traffic when QoS policy is applied.

  Conditions: The symptom is observed with the QoS priority feature.

  Workaround: There is no workaround.

- CSCtt39944

  Symptoms: The **show mls cef adjacency usage** is not showing the adjacency count correctly.

  Conditions: The symptom is observed in highly scaled networks. The platform code is not counting the last non-stats region allocation for adjacency usage.

  Workaround: There is no workaround.

- CSCtt43834

  Symptoms: Netflow counter gets incremented when sending SSM group range as v2.

  Conditions: The symptom is observed when doing an SSO.

  Workaround: There is no workaround.

- CSCtt43843

  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.

  Conditions: This symptom is occurring with a Cisco 7200 platform that is loaded with the Cisco IOS Interim Release 15.2(1.14)T0.1 image.

  Workaround: There is no workaround.

- CSCtt46638

  Symptoms: A Cisco 7604 running Cisco IOS Release 12.2(33)SRE4/SRE5 crashes when changing the tunnel source and destination of an IPsec sVTI.

  Conditions: The symptom is observed once the IPsec session is up and traffic is flowing through. If the tunnel source or destination is changed, the router crashes. This does not occur with a plain GRE tunnel.

  Workaround: There is no workaround.

- CSCtu00699

  Symptoms: On a DMVPN hub router, the IOS processor memory pool can get fragmented due to memory allocated for “Crypto NAS Port ID”.

  Conditions: This happens when there is network instability potentially causing tunnels to flap frequently.

  Workaround: There is no workaround.

- CSCtu28990

  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.

  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.

Workaround: There is no workaround.

- CSCtu32301

  Symptoms: Memory leak may be seen.

  Conditions: This is seen when running large **show** commands like **show tech-support** on the linecard via the RP console.

  Workaround: Do not run the show commands frequently.

- CSCtu36674

  Symptoms: Packets stop being transmitted in the output direction on L2transport local connect PVC on the ATM interface.

  Conditions: This symptom is observed when local connect is configured and a new ATM subinterface is configured on the same ATM main interface as the one with local connect PVC.

  Workaround 1: Perform shut/no shut on local connect.

  Workaround 2: Unconfigure/reconfigure local connect.

- CSCtu38244

  Symptoms: After bootup, the GM cannot register and is stuck in "registering" state. Issuing the **clear crypto gdoi** command is required for a successful registration to the keyserver.

  Conditions: The symptom is observed upon router bootup.

  Workaround: Either do a **clear crypto gdoi** after a reload, or configure a second keyserver entry. This does not have to be an existing keyserver, it can be just a dummy address.

- CSCtu39819

  Symptoms: The Cisco ASR 1002 router configured as an RSVPAgent for Cisco Unified Communication Manager crashes under extended traffic.

  Conditions: This symptom is observed on a Cisco ASR 1002 router configured as an RSVPAgent for CUCM End-to-End RSVP feature. The router crashes after 45 minutes of traffic run with 150 simultaneous up MTP-RSVP sessions.

  The image used is "asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin".

  Workaround: There is no workaround.

- CSCtu41137

  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.

  Conditions: The core is observed while doing unconfiguration.

  Workaround: There is no workaround.

- CSCtu51904

  Symptoms: You can observe decrementing free memory by each repetition of the process by using the **show memory statistics** command under the active SP.

  Conditions: The symptom is observed by removing "default mdt" under the VRF configuration and then adding it back. The memory leak is recognized on the active SP.

  Workaround: Reload the router.

- CSCtu60863

  Symptoms: IGMP reports do not get installed in the IGMP group list.

  Conditions: The symptom is observed when the port-security feature is enabled on the switchport which is part of the VLAN on which the IGMP reports are received.

Workaround: Remove “switchport port-security” from ports associated with the VLAN on which the IGMP reports are received.

- CSCtw45055

  Symptoms: A Cisco ASR router may experience a crash in the BGP scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
%BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold
time expired) x bytes
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification
received
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up

Exception to IOS Thread:
Frame pointer 0x3BE784F8, PC = 0x104109AC

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler
```

  The scheduler process will attempt to reference a freed data structure, causing the system to crash.

  Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

  Workaround: There is no workaround.

- CSCtw46625

  Symptoms: The QL value is DNU although the four least significant bits of SSM S1 byte are pointing to PRC (bits: 0010).

  Conditions: This symptom is observed when SSM S1 byte is received on CEoPs SPAs or channelized SPA-1XCHSTM1/OC3.

  Workaround: Force the QL PRC value by executing the following command:

  network-clock quality-level rx QL-PRC controller SONET 1/2/0

- CSCtw48209

  Symptoms: High-end Cisco devices running Cisco IOS are likely affected. Active features at the time of this problem manifestation include any condition that leads to RSVP SNMP notification generation in Cisco IOS. BGP/MPLS TE instability, leading to changes to RSVP session status change, is observed in a test scenario while running Cisco IOS Release SXI4 and Cisco IOS Release SXI7. The issue is not reproducible consistently.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SXI4, Cisco IOS Release 12.2(33)SXI7, Cisco IOS Release 12.2SR, Cisco IOS Release 12.2SX, and Cisco IOS Release 15S.

  Workaround: Disable RSVP notification using the **no snmp-server enable traps rsvp** command.

- CSCtw52610

  Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.

  Conditions: The issue is seen when primary link is considered OOP based on utilization despite using the **no resolve utilization** command.

Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure “max-xmit-utilization percentage 100”.

- CSCtw56439

  Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.

  Conditions: The symptom is observed with IPsec and the **ip mtu** over a tunnel interface.

  Workaround: There is no workaround.

- CSCtw62310

  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service- policy”.

  Conditions: The symptom is observed when removing the policy-map from map-class.

  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw64040

  Symptoms: Crash due to MPLS, which appears to be associated with load- balancing.

  Conditions: This symptom occurs when MPLS is configured.

  Workaround: There is no workaround.

- CSCtw71564

  Symptoms: Not all data packets are accounted for in the “show stats” output of the video operation.

  Conditions: The symptom is observed with heavy load on the responder caused either by many video sessions or other processes.

  Workaround: Reduce processor load on device running the responder.

- CSCtw72708

  Symptoms: Malloc failure, CPU hog, and memory leaks are seen creating the MD entry with your own IP address as the next-hop listener.

  Conditions: Issue is seen on a Cisco 7600 series router that is running Cisco IOS 15.2(04)S version. There are two triggers:

  1. When LI is configured on the Cisco 7600 with the remote’s MDip as one of your own; resulting in CPU hog and memory failures.
  2. When one generic stream is deleted, an internal counter is decremented twice. Thus disabling the LI feature even when there is another active tap installed.

  Workaround: Configure the MD listener IP address with the correct IP address.

- CSCtw76044

  Symptoms: Need IGMP/MLD information to make IGMP/MLP snooping work.

  Conditions: The symptom is observed under all conditions.

  Workaround: There is no workaround.

- CSCtw78451

  Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.

  Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.

  Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

- CSCtw88094

  Symptoms: The standby management processor reloads during configuration sync when there is a mismatch in the IP SLA configuration.

  Conditions: This symptom occurs shortly after the “ip sla schedule X start specific_start_time” command is issued multiple times on the same probe instance. Hence, when the configuration is synced to the standby management processor, a PRC error occurs. The PRC error causes a reload of the standby management processor.

  Workaround: Unschedule the probe before rescheduling for a specific start time.

- CSCtw94319

  Symptoms: Crash is seen at dhcpd_forward_request.

  Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.

  Workaround: Remove the **ip dhcp relay information option vpn** command, if possible. Otherwise, there is no workaround.

- CSCtw94598

  Symptoms: Web authentication does not work after an upgrade. NAS-Port-Type = Async.

  Conditions: The symptom is observed when you upgrade to Cisco IOS Release 12.2 (58)SE2 or later or to the Cisco IOS 15.0(1)SE train.

  Workaround: Change NAS-Port-Type on AAA Server to match the new value.

- CSCtw98456

  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

  For example, the IVRF routing table should show:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
  ```

  but instead it shows:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1
  ```

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

  Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

  Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

Workaround: Configure a static route to the remote network. For example:

```
ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtw99290

  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- CSCtw99989

  Symptoms: During normal operation a Cisco ASR 1000 Series Aggregation Services router may show the following traceback:

  ```
  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi
  ```

  Conditions: The symptom is observed during PPP renegotiation.

  Workaround: There is no workaround.

- CSCtx01604

  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.

  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.

  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- CSCtx18626

  Symptoms: IPv6 BFD hardware offloaded sessions do not come up when BFD session is formed.

  Conditions: The symptom is observed when an IPv6 BFD session is created between a Cisco 7600 (in one side) and third party vendor devices (on the other side).

  Workaround: There is no workaround.

- CSCtx21206

  Symptoms: BFDv6 hardware offloaded sessions do not come up with all IPv6 source addresses.

  Conditions: This symptom is observed with interface source IPv6 addresses that have some specific bits in the 6th byte set like 6001:1:C::1..

  Workaround: Reconfigure the source IPv6 addresses to some address that will not match the criteria mentioned in the above Conditions.

- CSCtx28483

  Symptoms: A router set up for Cisco Unified Border Element-Enterprise (CUBE- Ent) box-to-box redundancy will reload when certain configuration commands are deconfigured out of the recommended sequence.

  Conditions: The symptom is observed when deconfiguring CUBE-Ent box-to-box redundancy once it is already configured (for CUBE-Ent box-to-box redundancy) on the Cisco ASR platform. You cannot change the configuration under the “application redundancy group” submode without first

removing the redundancy-group association under “voice service voip” submode. If you do not remove this association first before changing the configuration under “application redundancy group”, the ASR will reload. You are not provided any other option.

Workaround: Always first remove the redundancy-group association under “voice service voip” submode first and then you can change the configuration under “application redundancy group”.

- CSCtx29543

  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the **show ip route** command.

  Conditions: This symptom occurs under the following conditions:

  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exists.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

  The router may now crash when doing **show ip route** command or when default route is updated.

  Workaround: There are two possible workarounds:

  1. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- CSCtx29557

  Symptoms: A standby crashes @ fib_fib_src_interface_sb_init.

  Conditions: All.

  Workaround: There is no workaround.

- CSCtx31175

  Symptoms: Framed-IP-Address added twice in PPP service-stop accounting record.

  Conditions: The symptom is observed with the following conditions:

  1. User session exists on ASR1001.
  2. Stop one user’s session by using **clear subscriber session username xxx** on ASR1001.
  3. ASR1001 sends double “Framed-IP-Address” in service-stop accounting for one user’s session.

  Workaround: Do not use **clear subscriber session** command to clear the session, instead use **clear pppoe**.

- CSCtx32628

  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

  Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

  - BGP full mesh is configured.
  - BGP cluster-id is configured.
  - **address family vpnv4** is enabled.
  - **address family ipv4 mdt** is enabled.

  - The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

  Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx35692

  Symptoms: On the Cisco ASR 1000 platform, while acting in a redundancy pair, when the standby ASR becomes active the dial-peers on the standby never change their state back to active causing all calls to fail. Calls that were active during the failover scenario will stay active in the new switchover. Only new calls are affected.

  Conditions: The symptom is observed on an ASR 1000 series router CUBE with a box-to-box redundancy configured that is using OOD option pings in the dial- peers. Global configuration of option pings under voice service VoIP is only for IN-Dialog option pings.

  Workaround: Disable option keepalives from the dial-peers.

- CSCtx39936

  Symptoms: A Cisco 7600 router configured for MPLS TE with tunnel load-sharing may punt traffic to MSFC when multiple TE paths to a given destination exist.

  Conditions: The symptom is observed with a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRE4, configured with multiple MPLS TE tunnels with load-sharing.

  Workaround 1: In some cases, clearing the router may trigger proper reprogramming of the prefix in the hardware.

  Workaround 2: Remove load-sharing from the TE tunnels.

- CSCtx47213

  Symptoms: The following symptoms are observed:

  1. Session flap when iBGP local-as is being used on RRs.
  2. Replace-as knob is not working in iBGP local-as case.

  Conditions:

  1. The session will flap when iBGP local-as is used on the RR client and RR sends an update.
  2. Replace-as knob even used is ignored and prefixes are appended with local-as.

  Workaround: Do not use iBGP local-as.

- CSCtx48010

  Symptoms: PIM neighbors on MDT tunnel continuously flap on a Cisco 7600 series router. Decapsulation path shows wrong rewrite index for flapping peers, instead of expected 7FFA recirculation index.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)S1. ES20 card as core-facing.

  Workaround: Identifying the adjacency of the flapping peer and changing the rewrite index to 7FFA manually stops the flap:

  ```
  test mls cef adj 180262 4055 9238 7ffa 2608 20 multicast 001e.f741.e28d 0.0.0 0 0x5fa
  ```

- CSCtx51935

  Symptoms: Router crashes after configuring “mpls traffic-eng tunnels”.

  Conditions: The symptom is observed with the following steps:

  ```
  interface gi1/2
  mpls traffic-eng tunnels
  no shut
  ```

```
router OSPF 1
mpls traffic-eng area 100
mpls traffic-eng router-id lo0
end
```

Workaround: There is no workaround.

- CSCtx55357

  Symptoms: Auto RP messages are permitted through “ip multicast boundary”.

  Conditions: The symptom is observed when the ACL associated with the multicast boundary matches 224.0.1.39 and 224.0.1.40. It is seen on the Cisco ASR 1000 platform.

  Workaround: Use “no ip pim autorp” which will disable Auto RP completely from this device.

- CSCtx67474

  Symptoms: Update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.

  Conditions: This can happen when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.

  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- CSCtx71618

  Symptoms: Router crash at process L2TP mgmt daemon.

  Conditions: The symptom is observed with a Cisco ASR 1006 (RP2) running Cisco IOS Release 15.1(2)S.

  Workaround: There is no workaround.

- CSCtx73452

  Symptoms: The following symptoms are observed:

  1. You send an ICMPv4 packet with IP option. It will be forwarded by ASR1001. IP options field includes “loose source routing” option.
  2. ASR 1001 receives the packet. ASR 1001 has “no ip source-route” setting in its configuration.
  3. ASR 1001 incorrectly overwrites the destination IP address of packet, which has source-route option set, and forwards it instead of dropping it.

  Conditions: The symptom is observed with the Cisco ASR 1001 (2.5G ESP).

  Workaround: There is no workaround.

- CSCtx73612

  Symptoms: A Cisco ASR 1000 may reload while reading IPsec MIBs via SNMP and write a crashfile.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: Do not poll or trap IPsec information via SNMP.

- CSCtx82775

  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.

  Conditions: The symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- CSCtx89018

  Symptoms: MLDP MVPN traffic over data MDTS is dropped.

  Conditions: The symptom is observed with the following conditions:

  - Multicast traffic is flowing on data MDTS.
  - The issue is seen after second switchover but sometimes on first switchover.
  - Multicast scale is 40 VRFs with 10000 mroutes distributed unequally among the 40 VRFs.

  Workaround: Using **clear ip mroute *** in all the VRFs will recreate all the mroutes and traffic will be resumed.

- CSCtx99544

  Symptoms: Exception occurs when using **no aaa accounting system default vrf** *VRF3* **start-stop group** *RADIUS-SG-VRF3*:

  ```
  router(config)# no ip vrf VRF3
  router(config)# no aaa accounting system default vrf VRF3 start-stop group
  RADIUS-SG-VRF3

  %Software-forced reload
  ```

  Conditions: The symptom is observed with the following conditions:

  - Hardware: Cisco ASR 1001.
  - Software: asr1001-universalk9.03.04.02.S.151-3.S2.

  Workaround: There is no workaround.

- CSCty02403

  Symptoms: EIGRP topo entry with bogus nexthop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus nexthop. So if you have a default route received from some neighbors, then that default route will also be flapped.

  Conditions: It can only occur when you have more then one attribute set in any route received from a neighbor.

  Workaround: Do not set more then one attribute in the route.

- CSCty16623

  Symptoms: Traffic getting black holed because the VPN corresponding to the tunnel secondary VLAN gets programmed with punt adjacency.

  Conditions: The symptom is observed with unconfiguring-reconfiguring the VRF. (The issue is independent of time gap between the configuration change.)

  Workaround: There is no workaround.

- CSCty34109

  Symptoms: Router crash at pm_port_set_vlan_state.

  Conditions: The symptom is observed with the following conditions:

  - 50 GRE-based MVPN intranet MVRFs with 100 mroutes in each, with PIM-SM having static-RP in core for 25 MDTs and auto-RP for 25 MDTs and PIM-SSM in VRF.
  - 50 MLDP-based intranet MVRFs with 100 mroutes in each, with PIM-SM having static-RP in 25 VRFs and auto-RP in 25 VRFs.
  - 100 P2MP-TE tunnels, with explicit paths. One branching point at nPE1, nPE2, nPE3, nPE4, uPE1, uPE2 and six branching points at nP with nP as bud node.
  - 900 unicast VRFs.

  - 5K mroutes in global context (plain multicast with PIM-SM having static RP for RP election).
  - IGP as OSPF.
  - P2P-TE tunnels in core, with link FRR protection.

  Workaround: There is no workaround.

- CSCty37445

  Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from hub and then advertises it back to the hub, bypassing split horizon.

  Conditions: The symptom is observed when on the spoke you have a **distribute list route-map** command setting tags.

  Workaround: Once you remove that command EIGRP works normally.

- CSCty41067

  Symptoms: Router crashes while doing an SSO without any configurations.

  Conditions: The symptom is observed while doing an SSO.

  Workaround: There is no workaround.

- CSCty58656

  Symptoms: A Cisco 7600 series router with ES+ module may crash.

  Conditions: The symptom is observed with the QoS policy map that has a name hash that is same as an existing policy used by the ES+ module and configuring a child policy or adding a child policy that is already in use.

  Workaround: Do not call a child policy map.

Resolved Caveats—Cisco IOS Release 15.1(3)S2

Cisco IOS Release 15.1(3)S2 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S2 but may be open in previous Cisco IOS releases.

- CSCsb53810

  Symptoms: A Cisco Catalyst 6500 series switch may not block traffic, which is supposed to be denied by an outbound ACL on a VLAN interface.

  Conditions: This issue is under investigation.

  Workaround: Reload the switch.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

- CSCsh39289

  Symptoms: A router may crash under a certain specific set of events.

  Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.

Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCta27728

  Symptoms: A Cisco router may crash.

  Conditions: This symptom is observed on a Cisco ASR1002 router running Cisco IOS Release 15.1(2)S1 with RSVP for MPLS TE tunnel signaling.

  Workaround: There is no workaround.

- CSCtc96631

  Symptoms: Packet drops occur in downstream devices every 4ms burst from shaper.

  Conditions: The symptom is observed when shaping at high rates on very fast interface types with low memory buffer devices downstream.

  Workaround: Use Cisco ASRs instead of Cisco ISRs.

- CSCti33159

  Symptoms: The PBR topology sometimes chooses a one-hop neighbor to reach a border, as opposed to using the directly-connected link.

  Conditions: This is seen when the border has multiple internal interfaces and one of the internal interfaces is directly connected to a neighbor and the other interface is one hop away.

  Workaround: There is no workaround.

- CSCtj30238

  Symptoms: WRED counters are wrongly updated. The default counter should be 0, but the counter is wrongly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there are no traffic matches in the class.

  Conditions: This issue is seen on the Cisco 7600 router with ES+ line card only. The Es+ line card does not support per WRED class based counters. There was a recent breakage due to the Transmit packets/bytes column that started showing up for the Es+ line card. This is wrong. As ES+ writes same value to WRED transmit count (not the per subclass base count, but total count), this value does not make sense.

  Workaround: Do not use WRED subclass Transmit packets/bytes counters for ES+ line card on the Cisco 7600 router.

- CSCtj33003

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

- CSCtk03371

  Symptoms: SVI-based EoMPLS/VPLS VC fails to forward traffic even when VC is up.

Conditions: This happens when the **ip cef accounting non-recursive** command is configured on the router. This command is documented as an unsupported command on the Cisco 7600 platform, but it should also generate an error message when configured on the Cisco 7600. Preferably it should not take any action, for example, it should not affect any other working features.

Workaround: Unconfigure the command by typing “no ip cef accounting non- recursive”.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- CSCtl50815

  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

  ```
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
  Non-OER, OOP Reason <reason>
  ```

  Conditions: The symptom is observed under the following conditions:

  - Use ECMP.
  - Use **mode monitor passive**.

  Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

  Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl83517

  Symptoms: The last switchover redundancy mode shows the configured mode.

  Conditions: This symptom occurs if DIVC ISSU results puts the system in RPR mode, and the last switchover redundancy mode still shows SSO. When a system tries to come out of RPR to SSO through either manual reset of standby or OIR, it will be stuck in RPR and will not progress to SSO as the last switchover flag shows SSO, and clients assume it is already in SSO.

  Workaround: There is no workaround.

- CSCtn04357

  Symptoms: When applying the following netflow configuration in the same sequence, the standby supervisor module continuously reloads:

  vlan configuration 161 ip flow monitor flowmonitor1 in ip flow monitor flowmonitor1 input

  Conditions: The symptom is observed on a Sup7-E that is running Cisco IOS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

  Workaround 1: Remove the flow monitor configuration.

Workaround 2: Use netflow-v9 export protocol.

Workaround 3: Use a record format exportable by netflow-v5.

- CSCtn07696

  Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the **show tech-support** command output using the **ftp** command due to TCP-2-INVALIDTCB.

  Conditions: This symptom is observed with the following CLI:

  ```
  show tech-support | redirect
  ftp://cisco:cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt
  ```

  During the FTP operation, if the interface fails or shuts down, it could trigger this crash.

  Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCtn31333

  Symptoms: High CPU utilization is observed on the Cisco CMTS router due to the Net Background process.

  Conditions: This symptom is observed on a router used for L2TP network server (LNS) with an L2TP application.

  Workaround: There is no workaround.

- CSCtn59075

  Symptoms: A router may crash.

  Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, 15.1(3)T1, and 15.1(4)M. Flexible Netflow needs to be running.

  Workaround: Disable Flexible NetFlow on all interfaces.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- CSCto81701

  Symptoms: The PfR MC and BR sessions flap.

  Conditions: The symptom is observed with a scale of more than 800 learned TCs.

  Workaround: Use the following configuration:

  pfr master keepalive 1000

- CSCto88393

  Symptoms: CPU hogs are observed on a master controller:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (0/0),process
  = OER Master Controller.
  ```

  Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.

  Workaround: There is no workaround.

- CSCtq29547

  Symptoms: The router crashes on watchdog timeout while processing the SNMP request for ciscoEigrpMIB.

  Conditions: This symptom occurs while processing the SNMP request for ciscoEigrpMIB.

  Workaround: Exclude ciscoEigrpMIB from being polled by using the following SNMP view:

  ```
  snmp-server view NOCRASH internet included
  snmp-server view NOCRASH ciscoEigrpMIB excluded
  ```

  Then, apply the view to your SNMP community string: snmp-server community test view NOCRASH

- CSCtq49325

  Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

  Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

  Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

  Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However if a particular path is threaded to be sent, in this case it is scheduled for a reply message, the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq60703

  Symptoms: The device crashes and traceback is seen when executing **write network**.

  Conditions: The symptom is observed when the command **write network** is used with no URL specified.

  Workaround: Specify a URL.

- CSCtq61128

  Symptom: Router is crashing with Segmentation fault (11).

  Conditions: This symptom is observed on routers acting as IPSEC hub using certificates.

  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 6.3/5.2:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2011-4231 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/en/US/products/products_security_vulnerability_policy.html

- CSCtq68778

  Symptoms: After an ISSU, the reload reason string is missing in the newly-active session.

  Conditions: The symptom is observed after an ISSU.

  Workaround: There is no workaround.

- CSCtq88777

  Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.

  Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.

  Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- CSCtq92940

  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

  Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

  Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

  Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtr04829

  Symptoms: A device configured with "ip helper-address" drops packets because of a zero hardware address check.

  Conditions: This symptom occurs when the hardware address is zero.

  Workaround: There is no workaround.

- CSCtr05686

  Symptoms: An error occurs when a policy-map with byte based queue-limit is not attachable to target.

```
policy-map p1
 class class-default
  bandwidth 200
  random-detect dscp-based
  random-detect dscp 8 10000 bytes 20000 bytes 10
  random-detect dscp 16 13500 bytes 20000 bytes 10
  random-detect dscp 24 16000 bytes 20000 bytes 10
  random-detect dscp 32 18000 bytes 20000 bytes 10
```

  The above configuration is not possible.

  Conditions: This issue occurs only when bytes based WRED is configured before byte based queue-limit.

Workaround: See the following:

```
policy-map p1
 class class-default
  bandwidth 200
  queue-limit 3000 bytes
  random-detect dscp-based
  random-detect dscp 8 10000 bytes 20000 bytes 10
  random-detect dscp 16 13500 bytes 20000 bytes 10
  random-detect dscp 24 16000 bytes 20000 bytes 10
  random-detect dscp 32 18000 bytes 20000 bytes 10
```

- CSCtr06926

  Symptoms: A CA server in auto grant mode goes into disabled state when it receives a client certificate enrolment request.

  Conditions: The symptom is observed when a client certificate enrolment request is received.

  Workaround: Do not place the CA server in auto grant mode.

- CSCtr25386

  Symptoms: BFDv6 static route association fails after reenabling interfaces.

  Conditions: This symptom is observed after interfaces are reenabled.

  Workaround: There is no workaround.

- CSCtr31496

  Symptoms: The line card crashes after switchover with the multilink configurations.

  Conditions: This symptom occurs after switchover with the multilink configurations.

  Workaround: There is no workaround.

- CSCtr33918

  Symptoms: Convergence is observed in the order of 1-6 seconds of multicast/video traffic on a Cisco 7600 router that is running Cisco IOS Release 15.0(1)S3a.

  Conditions: This symptom is observed with failure or restoration of a link carrying multicast/video traffic at the head-end or receiver-end.

  Workaround: There is no workaround.

- CSCtr34960

  Symptoms: A router that is running Cisco IOS may run out of IO memory.

  The **show buffers** command shows that the count reaches 0 in free list.

```
Router#sh buffers
...
Interface buffer pools:
....
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
     273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
```

```
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

Conditions: This issue is seen post bootup. The Cisco 7600 in HA is required to hit the issue. The **show buffers old** command shows some buffers hanging on EOBC buffers list for a long time, weeks or more. The issue is a corner case, and buffer leak rate is slow.

This DDTS fixes leaks for the **mls cef maximum-routes** and **mls cef adjacency-mcast** commands.

See the output from the **show buffers old pack**:

```
F340.08.04-6500-2-dfc1#show buf old packet

Buffer information for EOBC0/0 buffer at 0x275A0B00
  data_area 0x275A0FB8, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:36.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A100C, datagramsize 50, maximum size 1680
  mac_start 0x275A0FFE, addr_start 0x275A0FFE, info_start 0x0
  network_start 0x275A100C, transport_start 0x0, caller_pc 0x205DF718

275A100C: 00200000 02010000 00010006 01000000  . ..............
275A101C: 00350001 00101608 00000053 000000A6  .5.........S...&
275A102C: 000603E7 01170000 00000000 00000000  ...g............
          --------
275A103C: 000000                               ...

Buffer information for EOBC0/0 buffer at 0x275A5B48
  data_area 0x275A6000, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:41.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A6054, datagramsize 80, maximum size 1680
  mac_start 0x275A6046, addr_start 0x275A6046, info_start 0x0
  network_start 0x275A6054, transport_start 0x0, caller_pc 0x205DF718



275A6054:          00200000 02010000 02150007      . ..........
275A6060: 01000000 000A0001 00301608 00000052  .........0.....R
275A6070: 000000A4 00480002 01047FFF 00000001  ...$.H..........
                   --------
275A6080: 00000000 00000000 00000000 00000000  ................
275A6090: 00000001 00000000 00000000 00000000  ................
275A60A0: 00000000 00
```

```
F340.08.04-6500-2-dfc1#
```

The **show buffers old packet** command output will be either 000603E7 OR 00480002.

Workaround: Reload the supervisor to clear the leaked buffers.

- CSCtr35740

  Symptoms: QoS queuing hierarchy not moved to current active link when the previously active link goes down.

  Conditions: The symptom is observed when the DMVPN tunnel active link goes down.

  Workaround: There is no workaround.

- CSCtr49064

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

  The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this 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-ssh

- CSCtr51926

  Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

  Conditions: The symptom is observed when a service-policy is applied on the main interface.

  Workaround 1: Enable IPv6 explicitly on the main interface:

  ```
  interface x/y
    ipv6 enable
  ```

  Workaround 2: Reconfigure the IPv6 address on the subinterface:

  ```
  interface x/y.z
    no ipv6 address
    ipv6 address ...
  ```

- CSCtr56174

  Symptoms: The MPLS-TE link count reaches a large value (4 billion+) on the Cisco ASR 1000 series router and negative value on the Cisco 7600 series router. This issue is seen in the **show mpls tr link sum** and **show mpls tr link int** command output.

  Conditions: This symptom occurs if MPLS-TE tunnels are deleted using the **no int tunX** command and if the number of TE tunnels deleted are more than the TE links on the box. Even if they are not, with every TE tunnel deleted, the link count is affected and gets reduced.

  Workaround: Do not delete MPLS-TE tunnels using the **no int tuX** command. If a TE tunnel is not required, shut it down. If these symptoms are observed, the only way is to reboot.

- CSCtr58140

  Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.

Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

Workaround: There is no workaround.

- CSCtr79347

  Symptoms: A Cisco ASR1006 crashes without a BGP configuration change or BGP neighbor up/down event.

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
  Traceback summary
  % 0x80e7b6 : __be_bgp_tx_walker_process
  % 0x80e3bc : __be_bgp_tx_generate_updates_task
  % 0x7f8891 : __be_bgp_task_scheduler
  ```

  Conditions: No conditions but this is a rarely observed issue.

  Workaround: There is no workaround.

- CSCtr81559

  Symptoms: The PPP session fails to come up occasionally on LNS due to a matching magic number.

  Conditions: This symptom is observed during LCP negotiation, when the random magic number generated on the client matches the magic number generated on the LNS. PPP assumes it to be a loopback and disconnects the PPP session. This condition occurs rarely.

  Workaround: To avoid this, renegotiate the LCP. Configure the client using the **retry** command. This may cause the next session to come up correctly.

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCtr91890

  Symptoms: An RP crashes sometimes when the router is having PPPoX sessions.

  Conditions: If a PPPoX session is terminated in the middle of session establishment and ip local pool is configured to pick the IP address for the peer and the version that the router is running has the fix for CSCtr91890.

  Workaround: There is no known workaround.

- CSCtr92285

  Symptoms: The following log is seen, and VCs cannot be configured.

  ```
  SSM CM: SSM switch id 0 [0x0] allocated
  ACLIB [Gi9/1/0.3830, 3830]: Failed to setup switching for VLAN interface ...
  ```

Conditions: This symptom is observed with the access circuit interface shut and core flaps occurring, along with pseudowire redundancy. Also, leaks occur per flap.

Workaround: There is no workaround. If VCs can be removed, do so to release some IDs. Otherwise, try a redundancy switchover.

- CSCtr94545

  Symptoms: Standby crashes at fm_global_feature_add_for_vrf.

  Conditions: The system crashes when virtual servers are deleted.

  Workaround: There is no workaround.

- CSCts06929

  Symptoms: Disposition traffic gets dropped after SSO as the new local labels allocated by AToM do not get programmed on the line cards.

  Conditions: This symptom occurs when pseudowires are configured on the setup without graceful restart configured. Then, SSO is performed and two local labels have the same disposition information. This really manifests as a traffic drop issue when the scale is high.

  Workaround: Configuring graceful restart resolves this issue.

- CSCts11594

  Symptoms: A mediatrace session is scheduled with an attached session- parameter. The session is unscheduled and the session-parameters removed so that the default session parameters should be used.

  On the first schedule, traceback is seen. The session is again unscheduled and scheduled for second time and a crash is seen.

  Conditions: The symptom is observed when using custom session-parameters for a session and then removing it. Then using the default session-parameters followed by scheduled and unscheduled twice.

  Workaround: Use either the default session-parameters or custom session- parameters. Do not toggle between both.

- CSCts16013

  Symptoms: Longevity testing session churn causes RP crash on the Cisco ASR1K router. RP crash occurs due to memory leak by the QOS Accounting feature.

  Conditions: This symptom is observed during testing with the QOS Accounting feature PAC2. This issue is seen when there are a large number of sessions and churns with “aaa-accounting” in the QOS policy-map.

  Workaround: There is no workaround.

- CSCts16285

  Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

  Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

  Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts20246

  Symptoms: The DR for the receiver segment forwards IPv6 multicast packets on the Accepting Interface of S,G.

Conditions: This symptom occurs while multicast stream is running and the RPF interface towards the source and RP goes down on the DR and the interface connected to the receiver (oif in S,G before interface goes down) becomes the RPF interface for the source and RP and hence iif for S,G.

Workaround: There is no workaround.

- CSCts27042

  Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.

  Conditions: The symptom is observed with several hundred streams combined with a routing change (interface shutdown/no shutdown or metric increment/decrement).

  Workaround: There is no workaround.

- CSCts32920

  Symptoms: Traffic gets punted to the RP.

  Conditions: This symptom occurs when there are multiple P2P-GRE tunnels in a particular VRF. Remove one particular P2P-GRE tunnel from that VRF.

  Workaround: Shut/no shut P2P-GRE tunnels in that particular VRF, for which traffic is getting punted to the RP.

- CSCts34693

  Symptoms: A Cisco router may crash with the following error message:

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

Exception to IOS Thread:
Frame pointer 0x30CF1428, PC = 0x148FDF84

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EEM ED Syslog
-Traceback=
1#07279b80de945124c720ef5414c32a90  :10000000+48FDF84 :10000000+48FE400 :10000
000+4B819C8 :10000000+4B81964 :10000000+F5FAD8 :10000000+F5FD10 :10000000+F5FE
F0 :10000000+F5FF94 :10000000+F60608
```

  Conditions: This symptom is observed in a Cisco ASR 1004 router that is running Cisco IOS Release 15.0(1)S. This problem appears to be related to an EEM script that executes on a syslog event.

```
event manager applet BGP-MON
 event tag BGP-DOWN syslog pattern "BGP-5-ADJCHANGE.*Down"
 event tag BGP-UP syslog pattern "BGP-5-ADJCHANGE.*Up"
trigger
  correlate event BGP-DOWN or event BGP-UP
 action 02 cli command "enable"
 action 03 cli command "sh log"
 action 04 mail server "$_email_server" to "$_email_to" from
"$_info_routername@mcen.usmc.mil" subject "Problems on $_info_routername,
BGP neighbor Change" body "$_cli_result"
```

  Workaround: There is no workaround at this time.

- CSCts38429

  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

- CSCts41217

  Symptoms: Memory leak occurs in const_mfib_lc_* processes.

  Conditions: This symptom is observed during deletion and addition of VRFs. Multicast needs to be enabled in the VRF and the P2P tunnels should be present in the VRF. VRF should be removed before deleting the P2P tunnels for this to happen.

  Workaround: Delete all the P2P tunnels before removing the VRF

- CSCts42154

  Symptoms: After the Cisco IOS ASR 1006 router is reloaded, it fails to reregister to the key server. From the debugs, it is observed that the attempt to register is generated too early before the GDOI is ON. This registration attempt is made before the interface, through which GDOI registration traffic with the key server passes, goes to the UP state.

  Conditions: This symptom is observed on a Cisco IOS ASR 1006 router that runs Cisco IOS Release 15.0(1)S2 and Cisco IOS Release 15.0(1)S3.

  Workaround: Use the **clear crypto gdoi** command to fix this issue.

- CSCts47566

  Symptoms: During standby RP bootup, an incorrect ICMP punt entry for MPLS interfaces gets programmed. This entry appears even if the interface has no ACL applied in the input/output direction.

```
2037#show tcam inter gi4/0/3 acl in ip

* Global Defaults shared


Entries from Bank 0

    punt          icmp any any eq 11 <<<<<<<<<<<<<<<<
    permit        ip any any (1895 matches)

Entries from Bank 1
```

  Conditions: This symptom is observed with the ICMP punt entry, which is required to allow trace route across MPLS cloud. This is a workaround for a hardware problem with Tycho. The feature is called “FM_FEATURE_MPLS_ICMP_BRIDGE”. This workaround is required only if there are aggregate labels programmed in the superman VPN cam, but can get set incorrectly even when there is no VRF configuration on the box.

  Workaround: To clear the entry set unnecessarily, disable/enable MPLS on the interface for which it appears.

- CSCts49032

  Symptoms: Data traffic is getting block-holed.

Conditions: This symptom occurs with the removal/addition of default MDT address in VRF, with time gap of 30 minutes.

Workaround: Deletion/addition of VRF.

- CSCts55322

  Symptoms: More traffic is sent out because of stale MET entries.

  Conditions: This symptom occurs in a scale condition when the route towards the core on the source PE is changed.

  Workaround: There is no workaround.

- CSCts57115

  Symptoms: After the following procedure is executed, multicast traffic on several VRFs is not forwarded to the outbound tunnel interface for MDT.

  The procedure is as follows:

  1. Reload the router.
  2. Perform RP switchover.
  3. Perform active ESP(F0) hardware reload.
  4. Perform active ESP(F1) hardware reload.

  Conditions: This symptom is observed when MVPN sends out multicast traffic on a lot of VRFs.

  Workaround: Use the **ip pim sparse-mode** command to reconfigure the loopback0(global) interface.

- CSCts58394

  Symptoms: The SNMP graph traffic rate (collected from the port-channel subinterface) does not match the 5-minute offered rate from “show policy-map inter port-channel x.x”.

  Conditions: This symptom occurs on the Cisco 7600-S running Cisco IOS Release 15.0(1)S4 with the port-channel subinterface on 76-ES+XC-40G3CXL. This issue is seen only when there is EARL recirculation of packets and affects only the ingress traffic rate.

  Workaround: There is no workaround.

- CSCts62082

  Symptoms: Router generates the following message:

  ```
  %NHRP-3-QOS_POLICY_APPLY_FAILED: Failed to apply QoS policy 10M-shape mapped to NHRP
  group xx on interface Tunnelxx, to tunnel x.x.x.x due to policy installation failure
  ```

  Conditions: The symptom is observed when “per-tunnel” QoS is applied and there are more than nine DMVPN spokes. (Up to eight spokes, with QoS applied is fine.)

  Workaround: There is no workaround.

- CSCts64539

  Symptoms: The BGP next hop is inaccessible. The **show ip route** command output in the global and VRF routing tables shows that the next hop is reachable. The **show ip bgp vpnv4 all attr next-hop** command output shows max metric for the next hop.

  Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

  Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.

  Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

Workaround 3: If “neighbor x.x.x.x diable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCts69204

  Symptoms: PPPoE sessions do not get recreated on the standby RP.

  Conditions: This symptom occurs on the standby RP.

  Workaround: There is no workaround.

- CSCts76410

  Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

  Conditions: The symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

  Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts80643

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate this 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-rsvp

- CSCts81427

  Symptoms: With a scaled dLFIoATM configuration on FlexWAN, after issuing SSO, some of the interfaces stop pinging.

  Conditions: This symptom is observed after doing SSO.

  Workaround: Shut/no shut of the ATM interface helps to resolve the problem.

- CSCts85694

  Symptoms: The following error message is displayed:

  ```
  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi  (0x104C2E4)
  ```

  Conditions: This symptom is seen when clearing the sessions after a long time, and the memory leak is increasing incrementally. Leak is very slow.

  Workaround 1: Do not bring down all sessions together.

  Workaround 2: Do not tear down the sessions (scale numbers: 4k and above) together from different sources (say clearing PPP sessions and ISG sessions in lab; in field, clearing might happen via other triggers) simultaneously with no time gap between them.

  Workaround 3: Do not have accounting accuracy configured.

  Workaround 4: In this case, ISG Features are applied on TC and Session both. If we do not apply the features on the TCs, chances of this happening are less.

- CSCts86788

  Symptoms: CPU Hog messages start to appear followed by a crash.

  Conditions: This symptom is observed when the **show mpls traffic-eng fast-reroute database interface** *name* **detail** command is issued on an interface where there are no MPLS-TE tunnels.

  Workaround: Do not issue this command on an interface where there are no MPLS-TE tunnels.

  Further Problem Description: The trigger is simple, that is, issuing the FRR **show display** command on an interface on which there are no MPLS-TE tunnels.

- CSCts88467

  Symptoms: The drops happen earlier than expected.

  Conditions: This symptom occurs if the queue-limit is incorrectly calculated.

  Workaround: Configure a queue-limit explicitly to fix this issue.

- CSCts90734

  Symptoms: IKEA message trace entry memory leak is seen.

  Conditions: This symptom occurs when there is an IPsec session.

  Workaround: There is no workaround.

- CSCts97803

  Symptoms: When a policy-map is configured with two RTP class-maps and two RTP encapsulated MDI class-maps, flows are monitored on them. Changing one of the RTP class-maps to MDI will lead to the crash. Also when a policy-map is configured with both RTP and MDI class-maps, and if the flow being monitored by them is RTP encapsulated MDI flows, then RTP monitoring will not work.

  Conditions: This symptom is seen when policy-map is configured with both RTP and MDI class-maps. The RTP flow to be monitored should be RTP encapsulated MDI flow.

  Workaround: There is no workaround.

- CSCtt03485

  Symptoms: ES40: IDBMAN crash is seen with “no ip flow-export destination <> vrf <>”.

  Conditions: This symptom occurs when “ip flow-export destination 10.21.1.1 3000 vrf vrf_1120” is removed.

```
PE2(config)#no ip flow-export destination 10.21.1.1 3000 vrf vrf_1120

PE2#show vlan internal usage | i NDE      both NDE internal VLANs 1013, 1015
are cleared  from 'internal VLAN table'

PE2#show monitor event-trace idbman all | i NDE
*Sep 28 00:21:58.523: clear NDE_1013 vlan 1013
*Sep 28 00:21:58.527: clear NDE_1013 vlan 1013  mapping 1013 is cleared, but
 1015  is not cleared from idbman mapping

PE2#test platform debugger callfn name idbman_dump_vlans 0
Calling address (0x0AF46AFC) 1: Vl1 : 1
1015: NDE_1015 : 1015    mapping 1015 is still present in IDBMAN, eventhough
1015 is a free VLAN, so, it can be allocated to any new interface
```

Now, 1015 can be allocated for any other new interface, as it is cleared from “internal VLAN table”, whereas it is not cleared from IDBMAN mapping. Thus, you can reproduce the IDBMAN inconsistency with NDE interfaces.

When a new interface comes UP, the IDBMAN set will fail, as there is already an old mapping existing (NDE_1015). When you try to delete this new interface, it will try to clear the mapping in IDBMAN. But, it finds the old mapping (NDE_1015); hence, you must perform forced crash in idbman_if_clear_vlan_id and configure “ip flow-export destination 10.21.1.1 3000 vrf vrf_1120”.

```
PE2#show vlan internal usage | i NDE
1013 NDE
1015 NDE_vrf_0

PE2#show monitor event-trace idbman all | i NDE
*Sep 28 00:08:39.387: set NDE_1013 vlan 1013
*Sep 28 00:08:39.395: set NDE_1015 vlan 1015

                              PE2#test platform debugger callfn name
idbman_dump_vlans 0
                             Calling address (0x0AF46AFC) 1: Vl1 : 1
                              1013: NDE_1013 : 1013
                              1015: NDE_1015 : 1015
```

Workaround: Reload.

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt16487

  Symptoms: High CPU is seen when changes are made to the Cisco WCCP Access Control List (ACL).

  Conditions: This symptom is observed in a Cisco WCCP ACL.

  Workaround: There is no workaround.

- CSCtt18020

  Symptoms: A router that is running Cisco IOS may reload unexpectedly.

  Conditions: This symptom may be seen with active SSH sessions to or from the router. Only SSH is affected.

  Workaround: Use Telnet.

- CSCtt19442

  Symptoms: Cisco 7600 subinterface that is configured for bridging after router reload sends traffic even when being shutdown. This traffic is sent from physical interface to which subinterface correspond and further received on the other side of the link.

Conditions: This symptom is seen when bridging is configured on subinterface.

Workaround:

- Doing a **no shutdown**, then **shutdown** on the subinterface clears the issue.
- Remove bridging configuration from subinterface.

Deleting subinterface, and then recreating it does not fix the issue.

- CSCtt23367

  Symptoms: The status on active PoA is A/U. The status on standby PoA is S/A.

  Conditions: This symptom is seen after HA switchover. When configuring a new mLACP port-channel on new ACTIVE RP, it may get stuck in A/U state.

  Workaround: Remove the port-channel and RG configuration and add back again.

- CSCtt26532

  Symptoms: With QoS policy-map configured on a BFD interface, modifying the QoS policy-map flaps the BFD session.

  Conditions: This symptom is observed when BFD and QoS policy-maps are configured on the same interface.

  Workaround: There is no workaround.

  Further Problem Description: QoS and BFD use a common flag that gets reset and set during QoS policy-map update, causing the BFD session to flap. BFD session flap leads to the OSPF session also going down.

- CSCtt26643

  Symptoms: A Cisco ASR 1006 router running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.

  Conditions: This symptom is observed on a Cisco ASR 1006 router running the asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin image. The **show version** command causes the “Last reload reason: Critical software exception” error.

  Workaround: There is no workaround.

- CSCtt28703

  Symptoms: VPN client with RSA-SIG can access a profile where his CA trustpoint is not anchored.

  Conditions: This symptom is seen with the use of RSA-SIG.

  Workaround: Restrict access by using a certificate-map matching the right issuer.

  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 3.5/3:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:N/A:N/E:POC/RL:W/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/en/US/products/products_security_vulnerability_policy.html

- CSCtt32165

  Symptoms: The Cisco Unified Border Element Enterprise on the Cisco ASR 1000 series router can fail a call with cause 47 immediately after the call connects.

Conditions: This symptom is observed with a sufficient call volume and a call flow that redirects many calls. The Cisco ASR router can fail to provision the forwarding plane for the new call due a race condition where a prior call is not completely cleaned up on the forwarding plane before trying to use the same structure again.

The **show voice fpi stats** command output indicates that a failure has occurred if the last column is greater than zero. For example:

```
show voip fpi stats | include provisn rsp


provisn rsp          0      32790        15
```

Workaround: There is no workaround. However, Cisco IOS Release 3.4.1 is less impacted by these call failures due to a resolution of defect CSCts20058. Upgrade to Cisco IOS Release 3.4.1 until such time as this defect is resolved. In a fully redundant Cisco ASR 1006 router, you can failover the ESP slots to clear the hung entries in the forwarding plane. Other platforms will require a reload.

- CSCtt33158

  Symptoms: If WRED is already present and the queue limit is configured in packets then WRED thresholds become 0.

  Conditions: The symptom is observed if WRED is already present and the queue limit is configured in packets.

  Workaround: Remove WRED and reattach it.

- CSCtt35936

  Symptoms: EIGRP route updates are not sent to DMVPN spokes. The **show ip eigrp inter** command output shows pending routes in interface Q, which remains constant. The **show ip eigrp int deta** command output shows that the next sequence number of the interface remains the same (does not advance).

  Conditions: This symptom occurs when EIGRP session flapped, resulting in routes being withdrawn and restored.

  Workaround: Add a static route on any spoke that kicks out EIGRP learned routes from the RIB table; this will again kick the interface on the HUB.

- CSCtt46873

  Symptoms: In an MVPN setup, when the **mdt default** command is removed from under the VRF, unicast packets coming from the core, such as LDP and BGP, get dropped, leading to router isolation.

  Conditions: This issue is primarily seen when mls mpls tunnel-recir is not configured on the box (or does not get enabled due to the absence of a sip10g device). In such a case, MDT tunnel VLAN gets allocated, but is never released, until the **mdt default** command is removed. Since the decap adjacency handling the unicast packets is a GRE decap, with an MDT tunnel VLAN allocated, removal/re-add of **mdt default** command will program the adjacency with the MDT tunnel VLAN. Another removal along with a race condition might leave the adjacency with the tunnel VLAN (now deallocated), thereby causing the unicast packets to be dropped.

  Workaround: Configure mls mpls tunnel-recir on the box and remove/re-add the **mdt default** command or reload with mls mpls tunnel-recir configured to be safe.

- CSCtt69984

  Symptoms: The Cisco ASR 1000 series router does not initialize GDOI registration for the second GDOI group after reload.

Conditions: This symptom is observed with the following conditions:

1. Image version: Cisco IOS Release 15.1(3)S
2. Platform: Cisco ASR 1000 series router
3. Two GDOI groups need to be configured.

Workaround 1: Issue the **clear crypto gdoi** after the router reloads, or remove the crypto map from the WAN interface and reapply it.

Workaround 2: If you are using the same local address for different GDOI groups, have the two groups use a different local address.

- CSCtt90672

  Symptoms: CFM MEP enters the INACTIVE state on deleting the subinterface.

  Conditions: This symptom is observed under the following conditions:

  1. Create a subinterface (vlan 104) for EOAM communication. Check “CC-Status” = Enabled.
  2. Create a QinQ subinterface (vlan tags: 104 128) for subscriber on the same physical interface. Check “CC-Status” = Enabled.
  3. Later, delete the QinQ subinterface from the step 2 above (DT’s provisioning system does it, for example, for a new policy change). The “CC-Status” goes to inactive.

  Workaround: Unconfigure and reconfigure the **continuity check** command under the corresponding Ethernet CFM domain/service global configuration for this CFM MEP.

- CSCtu01172

  Symptoms: The Cisco ASR 1000 series router without an actual redundant router may crash when configured for CUBE HA based on the document “Cisco Unified Border Element High Availability(HA) on ASR platform Configuration Example.”

  Conditions: This symptom is observed with the Cisco ASR 1000 series router.

  Workaround: Remove the application configuration, that is, “no application redundancy”.

- CSCtu08608

  Symptoms: The standby RP crashes due to VoIP HA Session App.

  Conditions: The Cisco ASR 1000 platform with redundant RPs and Cisco Unified Border Element Enterprise. The signature in the crashinfo is as follows:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Voip HA Session App
  ```

  Workaround: There is no workaround.

- CSCtu12574

  Symptoms: The **show buffers** command output displays:

  1. Increased missed counters on EOBC buffers.
  2. Medium buffer leak.

  ```
  Router#sh buffers
  Buffer elements:
       779 in free list (500 max allowed)
       1582067902 hits, 0 misses, 619 created

  Interface buffer pools:
  ....
  ```

```
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
     273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

This DDTS tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```
0A9C4ED8: 00200000 02150000 0202080B 01000000  . .............. --> IPC Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A  .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000    .R.............  --> ICC Header
            --  --
```

And, if we look at the ICC header at the underscored items 00520002:

```
0052   (represents the class name)             ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)          ----> L3_MGR_MLS_REQ
```

Workaround: Reload the system.

- CSCtu30649

  Symptoms: Standby is reset.

  Conditions: This issue is seen when the ISSU standby is reset because of MCL failure.

  Workaround: There is no workaround.

- CSCtu31340

  Symptoms: The **show sip call called-number** crashes the router.

  Conditions: This symptom is observed when the call SIP state is DISCONNECT.

  Workaround: There is no workaround.

- CSCtu33956

  Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.

  Conditions: This symptom is observed under the following conditions:

  – The PPPoE dialer client needs to be configured on the physical SHDSL interface.
  – The GRE tunnel destination interface should point to the dialer interface.
  – The MPLS pseudowire should go over the tunnel interface.
  – After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.

  Workaround: There is no workaround.

- CSCtu36562

  Symptoms: cikeFailureReason and cipsecFailureReason from CISCO-IPSEC-FLOW- MONITOR MIB do not report the proper failure reasons for failed IKE negotiations (ph1 or ph2).

  Conditions: The symptom is observed with failed IKE negotiations (ph1 or ph2).

  Workaround: There is no workaround.

- CSCtu92289

  Symptoms: VCCV BFD on PW HE (routed pseudowire) is not working.

  Conditions: VCCV BFD is not working on routed pseudowire but works fine on scalable EoMPLS.

  Workaround: There is no workaround.

- CSCtv19529

  Symptoms: Router crashes on unconfiguring the last available DHCP pool. Crash will also be seen on running the **no service dhcp**.

  Conditions: This crash can happen only if “DHCP Client” process is running on the router along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).

  The client process can be started:

  1. from an DHCP autoinstall attempt during router startup (with no nvram config).
  2. if the **ip address dhcp** is run on one of the interfaces.
  3. if the router was used for DHCP proxy client operations.

  The relay processes are started when a DHCP pool is created by the **ip dhcp pool** *pool* command.

  Workaround: Have a dummy DHCP pool created using the **ip dhcp pool** *dummy_pool* command, and never delete this pool. Other pools can be created and removed at will, the *dummy_pool* should not be removed. In addition, do not execute the **no service dhcp** command.

- CSCtw45168

  Symptoms: DTMF interworking fails when MTP is used to convert OOB---RFC2833 and vice versa.

  Conditions: This symptom is observed when MTP is used to convert OOB---RFC2833 and vice versa.

  Workaround: This issue is seen starting from Cisco IOS XE Release 3.2. Cisco IOS XE Release 3.1 should work fine.

- CSCtw73551

  Symptoms: Standby RP can crash due to a memory leak processing calls. The crashinfo file identifies the process as follows:

  ```
  UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps
  ```

  Conditions: This symptom is seen on CUBE enterprise on the Cisco ASR 1000 series router with redundant RPs and approximately 2.4 million calls processed from last start of the standby RP.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(3)S1

Cisco IOS Release 15.1(3)S1 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S1 but may be open in previous Cisco IOS releases.

- CSCso88042

  Symptoms: The VLANs allowed on the trunk to WiSM are lost on every reload.

  Conditions: This symptom occurs when the number of entries in the allowed-VLAN statement exceeds five.

  Workaround: Limit the number of entries to five or less, using ranges instead of single VLANs.

  Further Problem Description: When the entries in the VLAN-allowed statement are more than five, two WiSM module allowed-VLAN statements are seen, even though one line was allowed during configuration. When reloaded, only one WiSM module allowed-statement is taken and the first statement is lost.

- CSCsq45560

  Symptoms: The port-channel member link stays as a standalone port with LACP.

  Conditions: This symptom is observed only with the “vlan dot1q tag native” feature enabled.

  Workaround: There is no workaround.

- CSCtd15853

  Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.

  Conditions:

  - mVPN is configured on the PE router.
  - Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.

  Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

  Workaround: There is no workaround.

- CSCti83542

  Symptoms: MPLS LDP flapping is seen with T3 SATOP CEM interface configurations.

  Conditions: This issue is seen with T3/E3 SATOP TDM configurations.

  Workaround: There is no workaround.

- CSCtj56551

  Symptoms: The Cisco 7600 crashes in a very rare case.

  Conditions: This symptom is observed very rarely when route-churn/sessions come up.

  Workaround: There is no workaround.

- CSCtk18404

  Symptoms: Per-user route is not installed after IPCP renegotiation.

Conditions: The symptom is observed with the following conditions:

1. PPP session comes up, NAS installs static routes which are sent as attribute from RADIUS server.
2. After a while, if CPE asks for IPCP renegotiation, IPCP is renegotiated but the static routes are lost.

Workaround: There is no workaround.

- CSCtn65116

  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

  Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Release 12.2(33)SRB and later. Earlier versions are not affected.

  Workaround: Advertise and withdraw or withdraw and re-advertise a more specific prefix. That will force the re-evaluation of the prefix not being imported, for import again.

- CSCtn67034

  Symptoms: The username attribute is missing in the accounting stop record even though the user is authenticated.

  Conditions: This symptom is observed when accounting is enabled for an unauthenticated session, and the start record does not have the username (as expected). After authenticating the session, the first accounting packet that goes out does not have the username, that is:

  1. The first interim packet, if interim is enabled.
  2. The stop record, if interim is not enabled or if the stop record is sent before the interim period expires.

  Workaround: Enable the interim so that the stop record will have the username information.

- CSCto16196

  Symptoms: Performing al **no wccp version2** on the WAAS device connected to the WAN link and then reconfiguring **wccp version 2** results in tracebacks on a Cisco ASR 1000 router configured with WCCP. Traffic loss is also observed.

  Conditions: This symptom is observed when WCCP is configured on a Cisco ASR 1000 router and the WCCP tunnels are up before **wccp version 2** is removed and reapplied on the WAAS devices.

  Workaround: There is no workaround.

- CSCto70633

  Symptoms: Packets get punted to the RP because the default ACL does not get programmed on the Distributed Feature line card (DFC), which causes high RP CPU.

  Conditions: This symptom is observed upon removal and reinsertion of the line card when there are VRF-scale configurations on the ES+ card as given below: More than 800 subinterfaces with VRF configurations

  Workaround: Reload the router.

- CSCto76700

  Symptoms: Multihop BFD session goes down with TE-FRR cutover.

  Conditions: The symptom may be observed with single hop, VCCV BFD and multihop BFD sessions. But after the TE-FRR cutover, the VCCV BF session comes back up whereas multihop BFD session goes down.

  Workaround: The workaround is to perform a “no shut” the port-channel interface.

- CSCto99343

  Symptoms: Linecards do not forward packets which causes a failure on the neighborship.

  Conditions: The symptom is observed on VSL-enabled linecards on a VSS system.

  Workaround: There is no workaround.

- CSCtq08864

  Symptoms: Scalable EoMPLS VC imposition traffic drop.

  Conditions: This is seen with a scaled configuration of scalable EoMPLS VC with access facing as LACP etherchannel with dual member links spread across the ES40 NP modules. Upon flapping one of the member links followed by port- channel bundle flap, a random VC stops flowing traffic on the imposition side.

  Workaround: Trigger the reprogramming of the VC using **clear xconnect all**.

- CSCtq17082

  Symptoms: Router reloads.

  Conditions: The symptom is observed with at least 2000 IPSec tunnel sessions by automatic script to remove a QoS configuration from Virtual Template.

  Workaround: Session teardown before you remove the QoS configuration.

- CSCtq21234

  Symptoms: Label is not freed.

  Conditions: The symptom is observed after shutting down the link.

  Workaround: There is no workaround.

- CSCtq24614

  Symptoms: The commands to ignore S1 bytes are not supported on an ATM interface.

  Conditions: The symptom is observed with an ATM SPA.

  Workaround: There is no workaround.

- CSCtq58383

  Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.

  Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

  Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq80648

  Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.

  For example:

```
interface Ethernet1/0
  vrf forwarding vpn1
   ipv6 address 1::1/64
!
 router bgp 65000
  address-family ipv6 vrf vpn1
```

```
neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
```

If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

Conditions: This symptom occurs when a user changes the VRF assignment.

Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq82715

  Symptoms: When the VPLS VC goes up/down, the DHCP snooping LTL has not been updated, resulting in DHCP packet drop.

  Conditions: This symptom occurs when the VPLS VC goes up/down, indicating that the DHCP snooping LTL has not been updated.

  Workaround 1: Enable/disable snooping.

  Workaround 2: Clear the xconnect peer for the newly elected peer.

  Further Problem Description: In such an event, the GPI is now passed onto DHCP snooping code to program its LTL.

- CSCtq86515

  Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.

  Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.

  Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- CSCtq91643

  Symptoms: Basic IP session with dot1q encapsulation and IP initiator may not come up.

  Conditions: The symptom is observed on an ES40.

  Workaround: Reconfigure the dot1q encapsulation (which has same VLAN ID as the outer VLAN ID of the QinQ subinterface) after an OIR.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when bgp deterministic-med is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr07704

  Symptoms: While using scripts to delete non-existent class map filter from a class, the router sometimes crashes (c2600XM) or returns traceback spurious memory access (c2801nm).

  Conditions: This symptom occurs when trying to delete a non-existent classmap filter, the classmap will be NULL, and passed to match_class_params_same. This results in referencing a null pointer.

  Workaround: Do null check in match_class_command and match_class_params_same. To keep existing behavior, do not print out a message like “the class does not exist” when deleting a non-existent class map from a class.

- CSCtr14675

  Symptoms: The line card crashes after removing the child policy in traffic.

  Conditions: This symptom occurs after the child policy is removed in traffic.

  Workaround: There is no workaround.

- CSCtr14852

  Symptoms: A Cisco 7600 router may experience the following error conditions:

  1. The router starts displaying ICC WATERMARK messages. (This is expected if it happens for a short duration and is not associated with the second symptom mentioned below).

     For example:

```
%ICC-SP-5-WATERMARK: 1375 multicast tx pkts for class L2-DRV(FC) are waiting to be
processed
-Traceback= 81757BC 85FB874 85FC09C 85E5684 85E7CC8 85F18DC 85F1C7C 85F2050 84436A4
8443EA4 835C958 8356C34
```

  2. The above symptom would trigger a situation where the flow control mechanism is turned "ON" by the communication infra (ICC). As a result, the communication infra will fail to carry application data from one point to another within the router. This in turn would lead to failure of multiple features that are dependent on the ICC.

     For example: The ICC flow control can be verified by the following command:

```
BFW01#sh icc flowcontrol
Class Name              FC state                    FC Counts (on/off)
                                          [ Local ]   [ Remote ]  [ IPC ]
=============================================================================
   37 EARL_NDE(FC)      [ OFF ]             0/0         0/0         0/0
   71 ACE_REQUESTS      [ OFF ]             0/0         0/0         0/0
   77 ICC_FC_TEST_REQU  [ OFF ]             0/0        0/0         0/0
   78 L3-MGR-QM(FC)     [ OFF ]             0/0         0/0         0/0
   79 L3-MGR-FM         [ OFF ]             0/0         0/0         0/0
   80 L3-MGR-INTF(FC)   [ OFF ]             1/0         0/0         0/0
```

  As shown above, the flow control is turned ON on L3-MGR-INTF, but never turned OFF.

  The ICC flow control mechanism is required to manage the ICC. If the flow control is turned on for a genuine reason, it will be turned OFF in a short while. This is expected.

  However, in this case, because of a bug in accounting, the flow control is turned ON (when not required), and never gets turned OFF, leading to the above situation.

Conditions: This symptom occurs during “ICC MULTICAST” (not IP multicast) usage. This issue may be caused by heavy route flaps or interface flaps.

Workaround: There is no workaround.

- CSCtr19286

  Symptoms: A “no shut” on an administratively down interface may result in overruns on other interfaces that are forwarding traffic. This occurs on ports being no shut for the first time in the same ASIC group. Subsequent shut/no shut on the same port does not cause this issue.

  Conditions: This symptom occurs under the following conditions:

  – This issue has been seen on Rohini ASIC-based DFC LAN cards such as WS-X6748-GE-TX.
  – The ports belong to the same port ASIC.
  – This issue is seen only the first time you no shut an interface

  Workaround: No shut all the ports in the ASIC group after bootup. Subsequent shut/no shut will not cause the overrun issue.

- CSCtr19922

  Symptoms: Lots of output printed by **show adjacency** *[key of adj] internal dependents* followed by a crash.

  Conditions: The symptom is observed with the existence of midchain adjacencies, which will be created by IP tunnels, MPLS TE tunnels, LISP, and similar tunneling technologies.

  Workaround: Do not use the **show adjacency** *[key of adj] internal dependents* command. Specifically, it is the “dependents” keyword which is the problem. If the dependents keyword is not used there is no problem.

- CSCtr22007

  Symptoms: A Cisco 7600 router that is configured with RSVP crashes.

  Conditions: MPLS-TE Tunnel Flap.

  Workaround: There is no workaround.

- CSCtr27674

  Symptoms: A SIP-200 linecard crashes.

  Conditions: The symptom is observed with a POS SPA on SIP-200 linecard after performing an ISSU upgrade on a Cisco 7600 Series router.

  Workaround: There is no workaround.

- CSCtr28527

  Symptoms: After a few minutes of HA cutover, DHCP snooping on a VLAN stops.

  Conditions: This symptom occurs after a few minutes of HA cutover.

  Workaround: Shut/no shut the port-channel interface.

  Further Problem Description: After SSO, the LTL consistency checker starts recomputing fpoe for each LTL. For those from the sw-mcast region, the LTL cc makes a callback to retrieve the gpid list to program the fpoe for the LTL. In this case, the DHCP snooping feature provides an incomplete list because the VPLS VC programming is done directly by the cwan_atom code and the feature is unaware of this gpid list. The VPLS VC gpid programming to LTL is now redirected to the feature itself.

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

- CSCtr30621

  Symptoms: When working and protect LSPs are over different IMs, an OIR of one will bring down both.

  Conditions: The symptom is observed when you OIR the link for one LSP.

  Workaround: Shut/no shut the TP tunnel interface.

- CSCtr34793

  Symptoms: The router cannot establish mVPN PIM adjacencies over an MDT tunnel. The core PIM still works normally.

  Conditions: This symptom may occur after router reload when mVPN with PIM is configured and PIM-hellos from the neighbors are coming to the line card with DFC. Another possible trigger could be removal/recreation of the MDT in a VRF definition.

  Workaround: Reload the line card.

- CSCtr37073

  Symptoms: WS-X6196-RJ-21 and WS-X6148X2-RJ-45 may fail to come online on the Cisco 7600 router when running SRC or higher images.

  Conditions: This symptom occurs when SRC or higher images are run on a Cisco 7600 router.

  Workaround: There is no workaround.

  Further Problem Description: This issue occurs due to a timing problem in the module initialization routine of the Cisco IOS.

- CSCtr45608

  Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

  Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.

  Workaround: Configure “ipv4 vrf” along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

- CSCtr45633

  Symptoms: A BGP dynamic neighbor configured under VPNv4 address-family does not work correctly.

  Conditions: The symptom is observed when a BGP dynamic neighbor is configured under a VPNv4 address-family.

  Workaround: Add “dynamic neighbor peer-group” under “ipv4 unicast address- family”.

- CSCtr51786

  Symptoms: The command **passive-interface** for a VNET auto- created subinterface x/y.z may remove the derived interface configuration command **ip ospf** *process id* **area** *number*. Consequently, putting back **no passive-interface** command will not form the lost OSPF ADJ.

  Conditions: The symptom is observed only with interfaces associated with the OSPF process using the command **ip ospf vnet area** *number*.

  Workaround: Associate the interface with the OSPF process using a network statement or using the interface command **ip ospf** *process id* **area** *number*.

  Further Problem Description: Interfaces associated with a process using a network statement under "router ospf" or interfaces configured with the command **ip ospf** *process id* **area** *number* are not affected.

- CSCtr53118

  Symptoms: The command **show mls cef ip lookup** *prefix* and **show mls cef ipv6 lookup** *prefix* returns IPv4 FIB Miss and IPv6 FIB Miss errors respectively.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 15.1(3)S.

  Workaround: Use **show mls cef ip** *prefix* and **show mls cef ipv6** *prefix* instead.

- CSCtr53677

  Symptoms: ARP failure is seen with the following **show** command:

  show arp vrf *vrf name*

  Conditions: This symptom occurs during deletion and readdition of the VRF with the multicast MDT configured and P2P tunnels as the access-facing interface, along with Gigabit subinterfaces.

  This issue is seen under the following conditions:

  1. Configure the mcast VRF with P2P tunnels as access-facing, along with Gigabit subinterfaces. Use a sip400 line card as the access-facing line card.
  2. Delete the VRF, P2P tunnel, and Gigabit subinterface.
  3. Add the same VRF again after a 60-second interval.
  4. Observe the ARP failure on the Gigabit subinterface.

  Workaround: There is no workaround.

- CSCtr53739

  Symptoms: The tunnel-encap entry is wrongly programmed. The following **show** command is used:

  show platform software multicast ip cmfib vrf *vrf- name* **tunnel-encap verbose**

  Conditions: This symptom occurs during deletion and readdition of the VRF with the multicast MDT configured and P2P tunnels as the access-facing interface, along with Gigabit subinterfaces.

  This issue is seen under the following conditions:

  1. Configure the mcast VRF with P2P tunnels as access-facing, along with Gigabit subinterfaces. Use a sip400 line card as the access-facing line card.
  2. Delete the VRF, P2P tunnel, and Gigabit subinterface.
  3. Add the same VRF again after a 60-second interval.
  4. Observe the tunnel-encap entry wrong programmed on the SP, with corrupt values.

  Workaround: There is no workaround.

- CSCtr69937

  Symptoms: The POS link flap in the core breaks the IPv4 PIC Core functionality.

  Conditions: This symptom occurs on Cisco 7600 routers running Cisco IOS Release 15.1(03)S.

  Workaround: Execute the **clear ip route** command for the affected prefix.

- CSCtr74529

  Symptoms: The following error messages are displayed:

  ```
  %ENVM-DFC3-4-LONGBUSYREAD: C2W Interface busy for long time reading temperature sensor
  1 %ENVM-DFC2-4-LONGBUSYREAD: C2W Interface busy for long time reading temperature
  sensor 2
  ```

  Conditions: This symptom is not caused by any specific conditions.

  Workaround: There is no workaround.

- CSCtr80366

  Symptoms: Relay miscalculates the giaddr from the OFFER packet, and hence cannot find the binding.

  Conditions: This symptom occurs while configuring multiple pools on the server and multiple secondary IP addresses on the relay loopback IP address.

  Workaround: There is no workaround.

- CSCtr89882

  Symptoms: Platform-related error messages are seen during an LDP flap in an ECM scenario.

  Conditions: This symptom is observed with LDP with ECMP paths and during flapping of LDP sessions.

  Workaround: There is no workaround.

- CSCtr92067

  Symptoms: A Cisco 7609 that is running Cisco IOS Release 15.1(2)S1 may have CHUNKSIBLINGSEXCEED messages in the log/syslog. The following maybe seen from the supervisor:

  ```
  %SYS-SP-STDBY-4-CHUNKSIBLINGSEXCEED: Number of siblings in a chunk has gone above the
  threshold. Threshold:10000 Sibling-Count:12036 Chunk:0x1DC6D820 Name:Const IPv6 ADJ
  -Process= "Const2 IPv6 Process", ipl= 5, pid= 435 -Traceback= <snip>
  ```

  Or from a linecard:

  ```
  %SYS-DFC9-4-CHUNKSIBLINGSEXCEED: Number of siblings in a chunk has gone above the
  threshold. Threshold:10000 Sibling-Count:12008 Chunk:0x29B01260 Name:Const IPv6 ADJ
  -Process= "Const2 IPv6 Process", ipl= 5, pid= 303 -Traceback= <snip>
  ```

  Conditions: The symptom is observed on a Cisco 7609 that is running Cisco IOS Release 15.1(2)S1.

  Workaround: There is no workaround.

- CSCts15072

  Symptoms: Multicast traffic in the MVPN solution is dropped.

  Conditions: This symptom is observed on the Cisco 7600 series routers after deletion and (re)creation of a VRF.

  Workaround: Do not delete VRFs. All configuration related to a VRF can safely be removed. Only the VRF name should be retained in the configuration.

- CSCts39240

  Symptoms: The **advertise** command is not available in BGP peer-policy templates.

Conditions: This symptom is observed on Cisco router running Cisco IOS Release 15.2(01.05)T, Cisco IOS Release 15.2(00.16)S, Cisco IOS Release 15.1 (03)S0.3, or later releases.

Workaround: The keyword and functionality is still available to be configured in the BGP neighbor command.

- CSCts39535

  Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.

  Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

  Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

  Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

  Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCts47605

  Symptoms: For ECMP on the Cisco ASR1k router, RSVP does not select the right outgoing interface.

  Conditions: This symptom is observed with RSVP configuration with ECMP.

  Workaround: There is no workaround.

- CSCts51980

  Symptoms: STM1-SMI PAs of version 3.0 do not come up.

  Conditions: This symptom is observed when the new version of PAs do not come up with enhanced flexwan.

  Workaround: There is no workaround. Without the PA, flexwan will come up.

- CSCts67423

  Symptoms: On the Cisco ASR1k and ISR G2 only, call failures occur in the CUBE enterprise with interoperability to third-party SIP devices due to a trailing comma in the Server and User-Agent fields. For example:

  User-Agent: Cisco-SIPGateway/IOS-15.1(3)S,

  Server: Cisco-SIPGateway/IOS-15.1(3)S,

  You might see this with Cisco IOS Release 15.2(1)T or other versions. If the trailing comma is present it can cause interoperability issues. If there is no trailing comma, then this defect is not applicable.

  Conditions: This symptom is observed when there is an interoperability problem between the CUBE enterprise and a third-party SIP device. The trailing comma is invalid against RFC 2616 and the third-party SIP device ignores SIP messages from the CUBE.

Workaround: On both inbound and outbound dial peers, apply a SIP profile similar to the one below, or add the four lines to an existing SIP profile in use.

```
voice class sip-profile 1
 request ANY sip-header User-Agent modify "-15.*," ""
 response ANY sip-header User-Agent modify "-15.*," ""
 request ANY sip-header Server modify "-15.*," ""
 response ANY sip-header Server modify "-15.*," ""

dial-peer voice 1 voip
 voice-class sip profiles 1
```

Resolved Caveats—Cisco IOS Release 15.1(3)S0a

Cisco IOS Release 15.1(3)S0a is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S0a but may be open in previous Cisco IOS releases.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes, when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when “bgp deterministic-med” is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

Open Caveats—Cisco IOS Release 15.1(3)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(3)S. All the caveats listed in this section are open in Cisco IOS Release 15.1(3)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCto16377

  Symptoms: DPD deletes only IPSec SAs. It does not delete IKE SAs.

  Conditions: This issue is observed when DPD is enabled and the peer is down.

Workaround: There is no workaround.

- CSCto45782

  Symptoms: When a tunnel interface in a DMVPN environment flaps, about 10 percent of the original number of tunnels do not get re-established automatically.

  Conditions: This issue is observed when all the following conditions are met:

  - RP2 and ESP20 are installed on the router.
  - The DMVPN hub has a large number (for example, 4000) of spokes connected to traffic.
  - IKEv1 and EIGRP are configured on the DMVPN hub.

  Workaround: Re-establish the tunnels by manually clearing them using the **clear crypto sa peer** command or the **clear crypto isakmp** command.

- CSCto56161

  Symptoms: Memory leaks are observed when 8000 ISGv6 PPP sessions out of 32000 ISGv6 PPP sessions with three TCs where one TC starts flapping.

  Conditions: This issue is observed when ISGv6 PPP sessions start flapping.

  Workaround: Reload the router.

- CSCto91593

  Symptoms: A packet loss is seen after an RPSO.

  Conditions: This issue is observed after an RPSO.

  Workaround: Run the **ip multicast redundancy routeflush maxtime** *300* command.

  There is no workaround.

- CSCtq08864

  Symptoms: Scalable EoMPLS VC imposition traffic drops.

  Conditions: This symptom is seen with scaled configuration of scalable EoMPLS VC with access facing as LACP EtherChannel with dual member links spread across the ES40 NP modules. Upon flapping one of the member links followed by port-channel bundle flap, some random VC stops flowing traffic in imposition side.

  Workaround: Trigger the reprogramming of the VC by using the **clear xconnect all** command.

- CSCtq14556

  Symptoms: If the active channel flaps while the standby channel is down, the multilinks do not come up.

  Conditions: This issue is observed if the active channel flaps while the standby channel is down. The MLP bundles remain inactive because the interfaces are down due to the LRDI error.

  Workaround: Bring up the standby channel.

- CSCtq15058

  Symptoms: A policy does not get attached to the LC after the policy map is modified and an OIR is performed.

  Conditions: This issue is observed after the policy map is modified and an OIR is performed.

  Workaround: There is no workaround.

- CSCtq17082

  Symptoms: Crash is observed with VTEMPLATE Background Manager when removing QoS configurations from Virtual-Template.

  Conditions: This scale issue happens with at least 2000 IPSec tunnel sessions by automatic script to remove QoS configuration from Virtual-Template.

  Workaround: There is no workaround.

- CSCtq31954

  Symptoms: High CPU utilization is observed during the AAA per-user process.

  Conditions: This issue is observed when there is a large number (for example, 15000) of TAL sessions.

  Workaround: There is no workaround.

- CSCtq40115

  Symptoms: Offset-list is not incrementing the metric by the correct value in EIGRP classic mode.

  Conditions: This symptom is seen only in classic mode and not in named mode.

  Workaround: Use EIGRP in named mode.

  Further Problem Description: When using offset-list in classic mode, the metric does not increase at all for small values like 10 or 20. For larger values, the metric increases by some random smaller value with no relation.

  This issue is not seen in EIGRP named mode since EIGRP named mode supports wide metrics.

- CSCtq56659

  Symptoms: Incorrect LC programming is seen with CEM interface.

  Conditions: This symptom is seen after the initial configuration of HSPWs.

  Workaround: Soft OIR.

- CSCtq57630

  Symptoms: Packets are lost due to high CPU utilization that occurs when a large number of data MDTs are configured at the same time.

  Conditions: This issue is observed when a large number of data MDTs are configured at the same time.

  Workaround: Configure a small number of data MDTs at a time.

- CSCtq67680

  Symptoms: When the SPA reloads, the event triggers a silent reload of the LC.

  Conditions: This issue is observed when a QoS policy is applied on the multilink bundle of the serial SPA.

  Workaround: There is no workaround.

- CSCtq67717

  Symptoms: Standby SUP is getting reset due to RF Client: IOS Config ARCHIVE after SSO while sync is happening.

  Conditions: This symptom occurs when archive is configured and performing SSO.

  Workaround: There is no workaround.

- CSCtq71477

  Symptoms: The **redistribute connected metric** *20000000 2 255 255 1500* command sets a bandwidth of 4294967295 Kbit.

  Workaround: There is no workaround.

  Further Problem Description: the **redistribute connected metric** *20000000 2 255 255 1500* sets a bandwidth of 4294967295 Kbit. All bandwidth values above 10000001 show the same value of 4294967295.

- CSCtq74691

  Symptoms: A buffer leak is observed at radius_getbuffer.

  Conditions: This symptom is observed when a DHCP request is initiated from the client. A DHCP address is allocated from the server, and a session comes up in the authentication state. A buffer leak occurs at radius_getbuffer and may increase with each new session.

  Workaround: There is no workaround.

- CSCtq79350

  Symptoms: Rekey fails in the GM after the ACL is changed in the key server a few times.

  Conditions: This issue is observed after the ACL is added to or removed from the key server.

  Workaround: Use the **clear crypto gdoi** command.

- CSCtq80074

  Symptoms: A router crashes when the **no ip trigger-authentication timeout** *90* **port** *1* command is executed.

  Conditions: This symptom is seen under the following conditions:

  – Configure “ip trigger-authentication timeout 90 port 1”

  – Configure “ethernet mac-tunnel virtual 4094”

  – Execute **no ip trigger-authentication timeout** *90* **port** *1* command.

  Workaround: There is no workaround.

- CSCtq80351

  Symptoms: SP crashes during a switchover in RPR mode.

  Conditions: This symptom is observed after the following failures and tracebacks with mcast scale configurations:

```
%SYS-SP-2-MALLOCFAIL: Memory allocation of 1708 bytes failed from 0x82148C4,
alignment 32
Pool: I/O  Free: 2064  Cause: Memory fragmentation
Alternate Pool: None  Free: 0  Cause: No Alternate pool
 -Process= "Pool Manager", ipl= 0, pid= 8
-Traceback= 81BA4D8z 8345490z 834ACB0z 82148C8z 835FC38z 835FF9Cz 83A301Cz 839D288z
CMD: 'sh redundancy state |  inc peer state' 18:21:22 IST Tue Jun 7 2011
Jun  7 18:21:22.575 IST: %SYS-SP-3-CPUHOG: Task is running for (2000)msecs, more than
(2000)msecs (27/2),process = SP Error Detection Process.
-Traceback= 0x8367AACz 0x821E7BCz 0x821EA94z 0x8E01830z 0x8BDDD60z 0x8E01A08z
0x96ED980z 0x96EBB34z 0x83A301Cz 0x839D288z
```

  Workaround: There is no workaround.

- CSCtq88437

  Symptoms: An IKEv2 memory leak results in RP reload. The memory leak speed depends on the session scale numbers. Session flapping will increase the leak.

  Conditions: This symptom is observed when tested with 4000 crypto map.

  Workaround: There is no workaround.

- CSCtq95291

  Symptoms: The router crashes.

  Conditions: This issue is observed when the saved configuration is copied to the startup configuration.

  Workaround: There is no workaround.

- CSCtq95873

  Symptoms: Some IPSec tunnels (DMVPN spokes) fail after the first IKE rekey.

  Conditions: This issue is observed when all the following conditions are met:

  - RP2 and ESP20 are installed on the router.
  - The DMVPN hub has a large number (for example, 4000) of spokes connected to traffic.
  - IKEv1 and EIGRP are configured on the DMVPN hub.

  Workaround: Reduce the number of tunnels (spokes) to 2000 or a smaller number.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when “bgp deterministic-med” is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr01431

  Symptoms: An error is encountered during configuration synchronization.

  Conditions: This issue is observed when the following sequence of steps is performed:

  1. A loopback interface is created
  2. The macro interface range is configured for the loopback interface.
  3. The loopback interface is deleted.

4. SSO is performed.

Workaround: There is no workaround.

- CSCtr06338

  Symptoms: IDSM2 service module does not come up.

  Conditions: This symptom occurs when IDSM2 service module heavy variant with RSP720-10GE.

  Workaround: There is no workaround.

- CSCtr12618

  Symptoms: With crypto map configured on a Cisco ASR 1000 series router with asr1000rp1-advipservicesk9.03.02.00.S.151-1.S.bin, if the crypto map ACL is changed, all IPSec traffic stops forwarding until tunnels rekey.

  Conditions: This symptom is seen in Cisco IOS Release 15.1(1)S.

  Workaround: Use the **clear crypto session** command to get crypto traffic to forward.

- CSCtr14867

  Symptoms: Static VTI tunnels terminating on a Cisco ASR 1000 series router that is using NAT-T due to a NAT rule in between the endpoints will fail to decapsulate traffic. The tunnel will build phase 1 and phase 2, the remote peer will show IPsec encaps and decaps, but the Cisco ASR 1000 series router will only show encaps with no decaps. This causes one-way outgoing traffic from the Cisco ASR 1000 series router side of the tunnel.

```
ASR1000#sh cry ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.12.1
protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.168.15.1 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1008, #pkts encrypt: 1008, #pkts digest: 1008
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

The Drop reason from the ASR is IpsecInput.

ASR1000#show platform hardware qfp active statistics drop all
-----------------------------------------------------------------------------
Global Drop Stats                          Packets                 Octets
-----------------------------------------------------------------------------
IpsecDenyDrop                                  0                      0
IpsecIkeIndicate                               0                      0
IpsecInput                                  1228                 233320
IpsecInvalidSa                                 0                      0
IpsecOutput                                    0                      0
IpsecTailDrop                                  0                      0
IpsecTedIndicate                               0                      0
```

Conditions: This symptom is observed on a Cisco ASR 1000 series router that is running Cisco IOS Release XE 3.3.1S with NAT-T tunnels using udp/4500 for encrypted traffic and static VTIs are in use.

Workaround: Remove NAT and use ESP for encapsulating encrypted packets. Downgrade to Cisco IOS Release 15.1(2)S. Use dynamic VTIs.

Resolved Caveats—Cisco IOS Release 15.1(3)S

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(3)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsd55997

  Symptoms: When the **archive tar/xtract tftp://***TFTP_ADDRESS***/tarball.tar flash:** command is used to unpack the contents of a TAR file to the flash: filesystem, the extraction process may cease right after the first “large file” is unpacked. All files in the TAR file which follow this “large file” will not be unpacked.

  Conditions: This behavior may be observed on Cisco IOS router platforms where the target flash: filesystem is Class B (LEFS). The source path of the TAR file may be TFTP or FTP. All Cisco IOS releases are affected.

  There is no problem unpacking all the contents of the TAR file when the target flash: filesystem is Class C (DOSFS).

  Workarounds:

  1. If possible format the target flash: filesystem as DOSFS (**format flash:**) as opposed to LEFS (**erase flash:**).
  2. If there is a second target media available (say slot0:), copy the TAR file there first and then unpack the TAR file to flash: **archive tar/xtract slot0:tarball.tar flash:**.
  3. If you are preparing your own TAR files, order all the “large files” at the end of the TAR file, with the largest “large file” as the last file in the archive.

- CSCsl74976

  Symptoms: When MPLS-tagged packets are punted to MSFC CPU at a high rate, incoming interface hold-queue can fill up, and interface will be throttled. No packets are processed from throttled interfaces (until interface is unthrottled). If control plane protocols are running on throttled interfaces (especially with aggressive short timeouts), frequent throttling can lead to instabilities (such as BGP session loss, OSPF adjacency flaps, HSRP failovers, BFD neighbor less, etc.).

  Conditions: This symptom occurs when MPLS-tagged packets are punted to MSFC CPU at a high rate, incoming interface hold-queue can fill up, and interface will be throttled.

  Workaround: A certain level of stability can be gained by increasing hold queues on interfaces in questions. Also reducing the rates and duration of the traffic punting to MSFC CPU will help.

- CSCsx64858

  Symptoms: A router may crash after the **show ip cef vrf** *VRF* **platform** command is issued.

  Conditions: This symptom occurs when BGP routes are learned via two equal paths within a VRF. If an update occurs so that only one path remains while the **show ip cef vrf** *VRF* **platform** command is issued, the router may crash.

  Workaround: There is no workaround.

- CSCsz53809

  Symptoms: There is an infinite reload of a VSS member due to configuration mismatch between peers.

  Conditions: This symptom is due to the use of double quotes in VLAN name configuration, which causes the rejection of that name during the initialization of a member after its reload.

  Workaround: There is no workaround.

- CSCta10402

  Symptoms: Continuous packet send by BFD causes a CPU hog.

  Conditions: The symptom is observed when BFD is enabled in the router.

  Workaround: Disable BFD.

- CSCtd10712

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtf39056

  Symptoms: RRI route will not be deleted even after IPSec SA has been deleted.

  Conditions: This symptom was first observed on the Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.

  Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the syntax may vary depending on the versions used):

```
############
configure terminal
!
event manager applet SR_000000526
event timer cron name SR_000000526 cron-entry  "0 3 * * *"
action 1 cli command "en"
action 2 cli command "reload"
!
end
############
```

- CSCth69364

  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://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml.

- CSCti10828

  Symptoms: In Cisco IOS Release 12.4T, there is no response to SNMP queries of:

  ```
  1.3.6.1.4.1.9.9.276.1.1.2.1.11 cieIfSpeedReceive
  1.3.6.1.4.1.9.9.276.1.1.2.1.12 cieIfHighSpeedReceive
  ```

  within the CISCO-IF-EXTENSION-MIB although supported at the CLI:

  ```
  interface GigabitEthernet0/3
   bandwidth receive 100 <<<<<

  ==> , BW 100000 Kbit/sec, RxBW 100 Kbit/sec
  ```

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCti48483

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCti16649

  Symptoms: GETVPN GM reregisters.

  Conditions: This symptom is seen when any ACL is added or removed from the key server.

  Workaround: There is no workaround.

- CSCti23324

  Symptoms: With some L2 DEC configurations, recirculation may be added during packet forwarding.

  Conditions: This symptom is seen with L2 DEC and PFC3B configurations.

  Workaround: This is not a forwarding issue. Remove L2 DEC or use PFC3C in the L2 DEC.

- CSCti87194

  Symptoms: The last fragment causes a crash because of an invalid zone value.

  Conditions: This symptom occurs when a Big IPC message is fragmented. Then, the last fragment causes the crash because of an invalid zone value.

  Workaround: There is no workaround.

- CSCti98219

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

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)

  - H.323 protocol

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtj04672

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtj14921

  Symptoms: During the stress test of EzVPN, many messages are observed on the console like the following:

  ```
  "%PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT: IOS thread disabled interrupt for 11 msec"
  ```

  The EzVPN server is configured for dVTI and dynamic crypto maps. The stress test consists of bringing up and tearing down close to 1700 EzVPN clients (1250 dVTI and 450 dynamic cmap) clients.

  Conditions: This symptom is seen on a Cisco ASR 1006 router with RP2/FP20 combo with EzVPN clients coming in on GigE interfaces and on the latest XE3.2 throttle build. Many messages are seen on the console followed by tracebacks.

  Workaround: There is no workaround.

- CSCtj65692

  Symptoms: The service policy applied to a service instance stops forwarding any traffic. The output of the **show policy-map interface** *x/y* command indicates that all packets are hitting the violation queue. The conform counter does not increase at all and all traffic is dropped.

  Conditions: This symptom is observed in Cisco 7600 with policers/LLQ on ES+ interfaces. This issue is applicable for the service policy (policing or LLQ) applied for ingress or egress traffic.

  Workaround: There is no workaround.

  Removing and reapplying service-policy may clear the condition for temporarily, but it can reappear. The issue is specific to policers. If possible, shapers can be used instead of policers to avoid the issue.

- CSCtj84234

  Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBR'd in hardware. This symptom is observed with route-map configuration, as given below:

route-map *RM name*

match ip address *acl*

set ip next-hop *NH1 NH2*

Workaround: There is no workaround.

- CSCtj94510

  Symptoms: When sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and 4 SA dual per session, a crash happens on Crypto_SS_process.

  Conditions: This symptom occurs when sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and four SA dual per session.

  Workaround: There is no workaround.

- CSCtj94589

  Symptoms: With the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF and four SA dual per session, in unconfigured testbed after end of the IXIA traffic, crash happens at "no vrf" under "crypto isakmp profile".

  Conditions: This symptom is seen with the configuration of 1000 VRFs (fvrf! =ivrf), with one IKE session per VRF and four SA dual per session.

  Workaround: There is no workaround.

- CSCtk31401

  Symptoms: A Cisco router crashes when the SSH session from it is exited.

  Conditions: This symptom is observed when "aaa authentication banner" is configured on the router.

  Workaround: There is no workaround.

- CSCtk67073

  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipsla.shtml.

- CSCtk74660

  Symptoms: The Network Time Protocol (NTP) tries to re-sync after the server clock changes its time and after the NTP falls back to the local clock.

  Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

  Workaround: There is no workaround.

- CSCtk99699

  Symptoms: Rekey functionality is broken if you remove and add crypto key again.

  Conditions: This symptom occurs when removing the key and adding again. The rekey is not working.

Workaround: Use the **clear crypto gdoi** command.

- CSCtl49917

  Symptoms: Minor diagnostic error is seen on SIP-400.

  Conditions: This symptom occurs when scaled configurations are applied to ES+ and SIP-400. The BusConnectivity test fails on SIP-400 during boot-up.

  Workaround: Power enable SIP-400 after all the line cards have come up in the test bed. Or, after a couple of retries, reload SIP-400, and it automatically comes up.

- CSCtl90292

  Symptoms: The following error messages are displayed:

  ```
  an 18 08:00:16.577 MET: %SYS-2-MALLOCFAIL: Memory allocation of 9420 bytes
  failed from 0x42446470, alignment 32
  Pool: I/O  Free: 11331600  Cause: Memory fragmentation Alternate Pool: None
  Free: 0  Cause: No Alternate pool  -Process= "BGP I/O", ipl= 0, pid= 564
   -Traceback= 417E8BEC 4180FA6C 42446478 42446B64 42443984 40FC18C8 40FCCB4C
  40FD1964 403BDBFC 403BCC34 40344508 403668AC
  ```

  Conditions: This symptom is observed when several hits and failures are seen for medium buffers. All are linktype IPC. For example:

  ```
  Buffer information for Medium buffer at 0x4660E964
  ...
    linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
    if_input 0x481DEA50 (EOBC0/0), if_output 0x0 (None)
  ```

  Workaround: There is no workaround.

- CSCtl90570

  Symptoms: PIM neighborship is lost on one of the PEs (source node).

  Conditions: This symptom occurs when reloading all the routers simultaneously.

  Workaround: Use the **clear mpls mldp neighbor *** command.

- CSCtn22961

  Symptoms: With the pseudowire redundancy, after performing “clear xconnect all” on the remote primary peer, the VCs that switchover to the backup PWs are now in the standby state on the primary peer. However, they are in down state on the local node instead of standby state.

  Conditions: This symptom occurs when performing “clear xconnect all” on the remote primary peer where initially all the VCs are in UP state.

  Workaround: There is no workaround.

- CSCtn36227

  Symptoms: Alignment errors are seen at ipv6_checksum.

  Conditions: This symptom is seen when the GRE tunnel is configured with IPv6 ping sweep going across.

  Workaround: There is no workaround.

- CSCtn51058

  Symptoms: Traffic drops cause long multicast reconvergence times.

  Conditions: This symptom occurs when performing Stateful Switchover (SSO).

Workaround: There is no workaround.

- CSCtn52270

  Symptoms: CWMP is not coming up.

  Conditions: This symptom is seen because of the “alcdsl_get_wan_dsl_link_config” function.

  Workaround: There is no workaround.

- CSCtn55847

  Symptoms: A memory leak is seen in crypto IKMP.

  Conditions: This symptom is observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(1)S2 that is acting as an IPSEC Hub based on DVTI. This happens when IPSEC spokes are flapping.

  Workaround: There is no workaround.

- CSCtn61834

  Symptoms: NAT-T keepalive cannot send out cause NAT translation timeout.

  Conditions: This symptom is seen when the NAT translation table is getting timeout since no NAT keep alive message is received.

  Workaround: There is no workaround.

- CSCtn62287

  Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.

  Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.

  Workaround: There is no workaround.

- CSCtn64879

  Symptoms: After configuring service group, traffic will go through both of the memberlinks of Ethernet Virtual Connection (EVC) point of contact (PoC) with xconnect.

  Conditions: This symptom is seen when defaulting the PoC configuration and adding it back.

  Workaround: Reset line card.

- CSCtn67577

  Symptoms: SIP-400 crashes while modifying the cell-packing values.

  Conditions: This symptom occurs when cell-packing values are modified at PE2 side.

  Workaround: There is no workaround.

- CSCtn67637

  Symptoms: Traffic is not forwarded from the DECAP PE in the egress replication mode.

  Conditions: This symptom occurs when the ingress LC on the DECAP PE is a CFC LC like 6748/SIP400 and the egress replication mode is used on the DECAP PE in a mVPN setup.

  Workaround: Switch to the ingress replication mode on the DECAP PE. Then, the traffic will start flowing.

- CSCtn68643

  Symptoms: OSPFv3 hellos are not processed and neighbors fail to form.

  Conditions: This symptom occurs when configuring OSPFv3 IPSec authentication or encryption.

```
ipv6 ospf encryption ipsec spi 500 esp null sha1
12341234123412341234123412341234123412341234
```

or

```
ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcd
```

Workaround: There is no workaround.

- CSCtn93891

  Symptoms: Multicast traffic is getting blocked.

  Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

  Workaround: There is no workaround.

- CSCtn95344

  Symptoms: After RPR downgrade from SRE2 CCO to SRE1 CCO, the standby RSP gets stuck in cold bulk and reboots every 50 minutes.

  Conditions: This symptom occurs after RPR downgrade from SRE2 CCO to SRE1 CCO.

  Workaround: Perform reload on the router.

- CSCtn95395

  Symptoms: VTEMPLATE Background Mgr crashes on DVTI server after using the **clear crypto session** command on DVTI client.

  Conditions: This symptom is seen on DVTI server when sessions are setting up with the IPSec DVTI configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. We might run into VTEMPLATE Background Mgr process crashing after executing the **clear crypto session** command a couple of times on DVTI client.

  Workaround: There is no workaround.

- CSCtn99858

  Symptoms: Crashinfo is seen.

  Conditions: This symptom is observed during an 8k session.

  Workaround: There is no workaround.

- CSCto00318

  Symptoms: SSH session that is initiated from a router that is running Cisco IOS Release 15.x may cause the router to reboot.

  For now, consider not initiating a SSH session from the Cisco router that is running a Cisco IOS Release 15.x train.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.x.

  Workaround: There is no workaround.

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload

  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCto09059

  Symptoms: CPUHOG at IPC Check Queue Time Process results in IOSD crash.

  Conditions: This symptom occurs with multiple RP switchovers with ISG PPPoE sessions.

  Workaround: There is no workaround.

- CSCto10336

  Symptoms: The LNS router hangs up at the interrupt level and goes into an infinite loop.

  Conditions: This symptom occurs during control channel cleanup.

  Workaround: There is no workaround. This symptom can be only removed through power cycle.

- CSCto11025

  Symptoms: When traffic streams are classified into multiple classes included with LLQ with qos-preclassify on the tunnel interface and the crypto map applied to an interface, packets are dropped on crypto engine on the Cisco 890 series router with buffers unavailable.

  Conditions: This symptom is observed when IPSec and QoS are used when qos-preclassify is on the tunnel interface and a crypto map is on the main interface.

  Workaround: Use tunnel protection or VTI instead of the crypto map on the interface.

- CSCto11957

  Symptoms: PPPoE is terminated on port-channel with ES+ session limit error occurring incorrectly.

```
%CWAN_RP-6-SESS_LIMITS_PORT_GROUP: Exceeded max number of sessions supported
on
port-group
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
[ADJ:PPPoE:5789] - hardware platform error.

Mismatch in sessions on RP and ES+:
BRAS#sh pppoe summary
    PTA  : Locally terminated sessions
    FWDED: Forwarded sessions
    TRANS: All other sessions (in transient state)

                                TOTAL     PTA   FWDED   TRANS
TOTAL                              57      56       0       1
Port-channel100                    57      56       0       1

BRAS#show platform isg session-count 4
 ES+ line card
 Sessions on a port-channel are instantiated on all member ports
 Port-group          Sess-instance   Max Sess-instance
 ----------          -------------   -----------------
 Gig4/11-Gig4/15              2936                4000 <<<<<<< INCORRECT
```

Conditions: This symptom is seen when scaled PPPoE sessions are terminated on port-channel with ES+ ports. Sessions negotiate, disconnect and attempt to renegotiate port-channel number other than port-channel 2.

Workaround: Change port-channel number to port-channel 2. Configure sessions to terminate on stand-alone ports.

- CSCto15278

  Symptoms: Tracebacks are seen at managed_chunk_low.

  Conditions: This symptom occurs when sending multicast traffic and using the **show memory debug leaks chunks** command.

  Workaround: There is no workaround.

- CSCto29720

  Symptoms: Packets drop in the LLQ queue without any congestion on the link when the line card is SIP-400.

  Conditions: This symptom occurs when LLQ is configured under Shaper on the physical interface and the line card is SIP-400.

  Workaround: There is no workaround.

- CSCto47524

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs responder.

  A **show process memory sorted** command may initially show “MallocLite” growing. By disabling malloclite with the following:

  ```
  config t
  no memory lite
  end
  ```

  One may start to see process “IP SLAs Responder” growing. In at least one specific case, the leak rate was 80mb per day.

  Conditions: This symptom is observed on a Cisco ASR 1002 router.

  Workaround: Disable IP SLA on affected router, if possible.

- CSCto50255

  Symptoms: Memory leak occurs while running UDP echo operation.

  Conditions: This symptom is observed when an UDP echo operation successfully runs. Leak is seen on every 100th run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way is monitoring and decoding the PC via the **show processes memory** *pid* command.

  Workaround: There is no workaround.

- CSCto53332

  Symptoms: A router configured for IPSEC accounting may display the following error message:

  ```
  %AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
  ```

  This does not seem to result in any impact apart from intermittently lost accounting messages.

  Conditions: This symptom occurs when ipsec accounting is active.

  Workaround: There is no workaround.

- CSCto55567

  Symptoms: The ES+ card goes to a major error state because of fabric CRC errors.

  Conditions: This symptom occurs after SSO with multicast traffic flowing through the line card.

  Workaround: Soft reload the line card.

- CSCto55606

  Symptoms: When same remote unicast neighbor is configured and received on different interfaces, the two neighbors keep flapping.

  Conditions: This symptom is seen when the same EIGRP neighbor is coming up on different interfaces.

  Workaround: This may not be a recommended configuration since having the same neighbor on different interfaces is not allowed in classic mode. This option is provided only for certain migration scenarios.

- CSCto55708

  Symptoms: There is a build error due to a missing “ " “ in a printf statement, only in dsgs, due to compiler-specific issues.

  Conditions: This symptom occurs due to a missing “ " “ in a printf statement only in dsgs due to compiler-specific issues.

  Workaround: There is no workaround.

- CSCto55812

  Symptoms: The router may crash.

  Conditions: This symptom occurs on entering vlan mode from a different mode, for example vfi, without exiting from the previous command mode.

  Workaround: Always exit from the current command mode while entering into another command mode.

- CSCto57723

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6

- CSCto60216

  Symptoms: Cisco IOS crashes in ospfv3_write.

  Conditions: This symptom occurs when the **issu runversion** command is entered multiple times within a short period of time.

  Workaround: Wait for the newly active router processor to completely initialize.

- CSCto61485

  Symptoms: High CPU utilization is seen after session disconnect.

  Conditions: This symptom is observed with scaling test cases with 10K to 24K sessions.

  Workaround: There is no workaround.

- CSCto63720

  Symptoms: No traffic passes after a link flap if port-security is configured on the Gigabit Ethernet interface on 6748 LC.

  Conditions: This symptom occurs when the Cisco IOS version running is Cisco IOS Release 12.2(33)SRE2. This issue is seen when port-security is configured on a 6748 port and the link flap occurs on this interface.

  Workaround: Reconfiguring port-security fixes the problem.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

  Conditions: This symptom is seen with GETVPN related configurations with fail-close feature activated.

  Workaround: There is no workaround.

- CSCto70972

  Symptoms: Multicast traffic drops and does not reach the corresponding entries like (*,G/m) or (*,G).

  Conditions: This symptom occurs when multicast traffic drops and does not reach the corresponding entries like (*,G/m) or (*,G).

  Workaround: There is no workaround.

- CSCto71075

  Symptoms: High CPU usage is seen on changing root node multiple times in an MLDP setup. Loss of pim neighborship is also seen when changing path in a P2MP setup.

  Conditions: This symptom occurs when ptcam redirection being enabled for Lspvif can cause unexpected results. By default, Lspvif ptcam redirection is disabled. This fix ensures that this is taken care of in scenarios of pim state change.

  Workaround: There is no workaround.

- CSCto74038

  Symptoms: After an upgrade to SRE3, the CESoPSN (clock) pseudowire stays down due to payload size value mismatch.

  Conditions: This symptom occurs when, before the upgrade to SRE3, the payload size is configured to 80 and dejitter value is the default (5). After the upgrade, the payload size 80 and dejitter 5 combination is not accepted anymore as it is not the recommended value, so the payload size is removed from the configuration. The pseudowire is therefore configured with the default payload size. The default value is not accepted by the remote end of the pseudowire, thus leading to payload size mismatch.

  Workaround: Configure an acceptable dejitter value, and then reconfigure the payload size.

- CSCto76009

  Symptoms: Crypto SS crashes on DVTI server after using the **clear crypto session** command on DVTI client after all SAs have been established.

  Conditions: This symptom occurs when sessions are set up with the configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session.

  Workaround: There is no workaround.

- CSCto77225

  Symptoms: The states for VCs with MTP configurations remain up and on standby on standby POA.

Conditions: This symptom is seen when SSO is followed by a pmLACP/mLACP switchover.

Workaround: There is no workaround.

- CSCto77233

  Symptoms: The supervisor module on the Cisco 7600 router resets.

  Conditions: This symptom is observed when you use the **show ip cef** *prefix* platform internal command on the SP CPU and let it allow to hang on the --more-- prompt for long. When the underlying data gets changed or cleaned up due to waiting for long on --more-- prompt, the CLI can end up referencing wrong data resulting in router reset.

  Workaround: There is no workaround.

- CSCto77352

  Symptoms: Standby cannot reach HOT sync state with active. Standby RP will keep resetting. The following messages are printed:

  ```
  %SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1),process
  = IPC Dynamic Cache.
  ```

  Conditions: This symptom occurs with SSO mode when a Cisco ASR 1000 series router is configured with ISG as DHCP server and with low DHCP lease timer.

  Workaround: There is no workaround.

- CSCto77504

  Symptoms: With shape configured on port-shaper and bandwidth-percent configured on groups in the EVC, on dynamic configuration of port-shaper value, the groups do not get the updated shape values based on bandwidth percent.

  Conditions: This symptom is seen when bandwidth-percent is configured on group or EVC with port-shaper.

  Workaround: There is no workaround.

- CSCto79174

  Symptoms: A Cisco 7600 router crashes with the following logs:

  ```
  Frames of RPC pm-cp process (pid 325) on 6 (proc|slot) after blocking rpc
  call failed: 8331CD0 855F3F4 8546A58 85E3F98 85E4910 86009E4 86BF18C 86BC44C
  86BDE8C 8601090 8601394 835B498 8355774

  Failed to send card online to CP, slot 2

  %Software-forced reload


  Unexpected exception to CPU: vector 1500, PC = 0xAF8765C , LR
  = 0xAF87620
  ```

  Conditions: Conditions are not known.

  Workaround: There is no workaround.

- CSCto80714

  Symptoms: Prowler SPA goes out of service with heartbeat failures when traffic flows through the MLPPP (multilink) interface. This issue is seen only in the Cisco IOS Release 12.2SRE throttle and not in mcp_dev. Some optimizations and a microcode reload-related fix is also included as part of this DDTS.

  Conditions: This symptom is observed when traffic flows through the MLPPP interface on Prowler. Microcode and SPA reload is required to recover.

  Workaround: There is no workaround.

- CSCto81530

  Symptoms: Task hung errors are seen in hal_dist_commit from cmfi code.

  Conditions: This symptom occurs when mldp configurations are loaded in a scaled environment.

  Workaround: There is no workaround.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- CSCto93880

  Symptoms: Enable authentication fails when user is configured with TACACS server group.

  Conditions: This symptom occurs when TACACS server is configured with user defined group and configured for enable authentication. User is unable to authenticate when he tries to switch to privilege executive mode (enable) and gets an error that indicates that there is no address for defined servers.

  %TAC+: no address for get_server

  %TAC+: no address for get_server

  Workaround: Configure the TACACS server group with the default group name.

- CSCto95591

  Symptoms: ES+ crash occurs.

  Conditions: This symptom is observed when vpls over the gre tunnel is configured and shut/no shut of the tunnel interface is done.

  Workaround: There is no workaround.

- CSCto99226

  Symptoms: Multicast packets are not forwarded.

  Conditions: This symptom occurs when the physical interface in the outgoing interface list (olist) of S,G has local join.

  Workaround: There is no workaround.

- CSCtq01136

  Symptoms: There is a ping failure over tunnel interface.

  Conditions: This symptom is seen during 6VPE basic configuration.

  Workaround: There is no workaround.

- CSCtq06105

  Symptoms: In an IP-FRR setup, after shut and unshut of the primary interface, traffic continues to flow along the backup interface, which is wrong. Traffic should flow along the primary path once the primary path is restored.

  Conditions: This symptom occurs with an IP-FRR setup. The primary interface should be shut and unshut to see the issue.

  Workaround: Shut and unshut the backup interface. This will reprogram the FRR, but this will cause a traffic drop.

- CSCtq09088

  Symptoms: The router crashes while trying to unconfigure “ip rsvp sender-host 10.0.0.5 10.0.0.1 UDP 11 11 10 10 identity bogusID”.

  Conditions: This symptom is observed on the Cisco 7200 router that is running the c7200-adventerprisek9-mz.122-33.3.13.SRE image.

  Workaround: There is no workaround.

- CSCtq09206

  Symptoms: Traffic flowing via MPLS TE tunnels gets blackholed after FRR-protected primary link flaps initiate an FRR cutover. CEF Backwalk failure messages may be observed on the SP/DFC console.

  Conditions: This symptom is observed with TE/FRR configuration with node protection.

  Workaround: There is no workaround.

- CSCtq10019

  Symptoms: After router reload, rate-limiters for multicast do not come into effect and packets are punted.

  Conditions: This symptom occurs during high CPU load when mfib is unable to distribute into lc and SP.

  Workaround: There is no workaround.

- CSCtq12230

  Symptoms: When overhead accounting command “hw-module slot 1 account np 0 out 4” is configured on the ES+ LC, show policy-map interface counters do not get updated.

  Conditions: This symptom is seen with QoS on any ES+ interface with overhead accounting feature enabled.

  Workaround: There is no workaround.

- CSCtq14829

  Symptoms: Traffic drops are seen in a DMVPN ph3 hierarchical setup. Traffic is flowing through spoke-hub-spoke path. Dynamic tunnel is not building between spokes.

  Conditions: This symptom occurs when traffic drops are seen at rhub1 when the number of tunnels is 50 or more.

  Workaround: There is no workaround.

- CSCtq21258

  Symptoms: When a user uses a password larger than 32 bytes in size, the authentication for COA will pass if the password matches the settings on the RADIUS server. When this password is reduced in size to exactly 32 bytes, including the setting on the RADIUS server, the authentication for the COA will fail as the ISG appends excess data to the password sent to the RADIUS for authentication.

  Conditions: This symptom is seen when the user password is larger then 32 bytes and is being reduced to exactly 32 bytes.

  Workaround: Do not use 32 bytes as the size for the user password. In case the error occurs, the only method to solve the issue is to reload the device.

- CSCtq21435

  Symptoms: Some specific s,g entries do not pass traffic with mldp during root node redundancy switchover.

  Conditions: This symptom occurs in case of mldp + RNR. This issue is seen when Accept Vlan is programmed as zero in the platform.

  Workaround: Clear the mroute.

- CSCtq21785

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS-XE Release 15.1(2) S may crash upon performing a CRL check on an invalid certificate.

  Conditions: The conditions are unknown.

  Workaround: Turning off CRL check should stop the crash. It should be configured as:

  “revocation-check none”

  This will stop the CRL check of the peer certificate but should not be a long term solution.

- CSCtq23038

  Symptoms: With “platform control-packets use-priority-q disable” configured on the port-channel main interface, after shut/no shut on the port-channel or member-link, port-channel subinterfaces do not inherit the “platform control-packets use-priority-q disable” feature.

  Conditions: This symptom occurs when you perform shut/no shut on a member-link or link flaps with port-channel subinterfaces and “platform control-packets use-priority-q disable” configured on the port-channel.

  Workaround: A possible workaround is to remove and reconfigure the subinterfaces.

- CSCtq23158

  Symptoms: The dlfi o atm fails to come up on sip400 with Cisco IOS Release 15.0(1)S images onwards if an ES+ card is present.

  Conditions: This symptom occurs when you cannot bring up dlfi o atm.

  Workaround: A possible workaround is to power down all ES+ cards.

- CSCtq23793

  Symptoms: After reloading PE router in mVPN network, multicast traffic stops on one of the VRFs randomly.

  Condition: This symptom occurs under the following conditions:

  -When reloading a PE in mVPN network. -When PE has many VRFs and scaled mVPN configuration.

Workaround: Remove and add MDT configuration.

- CSCtq29554

  Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the **show ipc port | in MRIB** command on a failed line card does not display a port.

  Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.

  Workaround: Reload the failing line card to recover it.

- CSCtq30686

  Symptoms: A Cisco router crashes in a Secure Device Provisioning (SDP) environment.

  Conditions: This symptom is seen when the Registrar router crashes when a client router submits an enrollment request that was previously stuck in “granted” status with the same fingerprint.

  Workaround: There is no workaround.

- CSCtq31338

  Symptoms: ESM20 crashes with MLDP intranet test.

  Conditions: This symptom occurs with access interface flapping a couple of times.

  Workaround: There is no workaround.

- CSCtq32896

  Symptoms: LSM entries stop forwarding traffic.

  Conditions: This symptom is observed after Stateful Switchover (SSO).

  Workaround: There is no workaround.

- CSCtq33102

  Symptoms: A Cisco router that is acting as an RA crashes in an SDP environment with CVO setup.

  Conditions: This symptom occurs during CVO enrollment request.

  Workaround: There is no workaround.

- CSCtq34807

  Symptoms: Service group does not take effect on EVC Xconnect on a port channel.

  Conditions: This symptom is observed with a service group configuration on EVC Xconnect existing on a port channel. This issue is seen when EVC is removed and the configuration is reapplied.

  Workaround: Remove and reapply the service group.

- CSCtq36726

  Symptoms: Configuring the **ip nat inside** command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned Virtual- access interface. The NAT functionality is thus broken, because the V-access interface does not get this command cloned from its respective VTEMP.

  Conditions: This symptom is observed on Cisco ASR1006 (RP2/FP20) routers with ikev2 dVTI. This issue may be service impacting and is easily reproducible.

  Workaround: Reconfigure the Virtual-template interface such that the **ip nat inside** command is applied first, followed by other commands.

- CSCtq37538

  Symptoms: Duplicate traffic is seen during route changes with p2mp te for multicast or mldp.

  Conditions: This symptom occurs during LSM configuration and route changes.

  Workaround: Clear the problematic mroute using the **clear ip mroute** command.

- CSCtq38303

  Symptoms: A policy is rejected with an insufficient bandwidth percent guarantee.

  Conditions: This symptom is observed with bandwidth percentage guarantees.

  Workaround: Do not configure bandwidth in percentages.

- CSCtq43480

  Symptoms: A Cisco router crashes.

  Conditions: This symptom occurs when a session starts with PBHK and accounting features while the method list is not provisioned for the accounting features.

  Workaround: There is no workaround.

- CSCtq50674

  Symptoms: Total traffic drop is seen for 6PE/6VPE when IPFRR is configured in the core.

  Conditions: This symptom occurs when BGP/6PE peer is protected by IPFRR in core.

  Workaround: There is no workaround.

- CSCtq52345

  Symptoms: IPv6 sessions sync to standby. IPv6 sessions are up on standby. After switchover the IPv6 sessions drop traffic.

  Conditions: This symptom is seen with switchover of IPv6 sessions.

  Workaround: Clear sessions and start reestablishment.

- CSCtq55723

  Symptoms: With Transport Control Protocol (TCP) and User Datagram Protocol (UDP), operations with VPN Routing and Forwarding (VRF) are not working.

  Conditions: This symptom occurs only with VRF.

  Workaround: Works without VRF.

- CSCtq56845

  Symptoms: Static PW over P2MP TE traffic might not pass through access facing SIP-400.

  Conditions: This symptom is seen with static PW with P2MP TE. On the SIP-400 drops are seen with MTU exceeded in “show plat drop detail” on the access facing SIP-400.

  Workaround: There is no workaround.

- CSCtq56948

  Symptoms: The default route attribute is used by features like uRPF and if it is missed out, it may cause uRPF to allow packets whose source addresses match against the default route.

  Conditions: This symptom occurs because some prefixes in the FIB are sourced by non-RIB features, such as CTS, or are used to represent next hops for recursive paths. Such prefixes inherit the forwarding information from their covers, but the default route attribute is not inherited.

  Workaround: There is no workaround.

- CSCtq57054

  Symptoms: ISSU between Cisco IOS Release XE 3.3.0S and Cisco IOS Release XE 3.4.0S is affected due to config sync issue.

  Conditions: A newly introduced CLI in Cisco IOS Release XE 3.4 is not phrased properly to support the backward compatibility.

  Workaround: There is no workaround.

- CSCtq59827

  Symptoms: MLDP and traffic are not passing at bud node.

  Conditions: This symptom is seen when MLDP/LSM and traffic are not passing at bud node. Some stale adjacencies will be seen for label entry programming in the hardware.

  Workaround: Remove the OIF and add it back. (Do a shut/no shut).

- CSCtq60383

  Symptoms: Traffic outage is observed after TEFRR cutover in an MLDP setup.

  Conditions: This symptom is observed when “mpls ldp explicit-null” is configured on all the provider boxes.

  Workaround: Unconfigure “mpls ldp explicit-null”.

- CSCtq62600

  Symptoms: Double LSM entries are seen.

  Conditions: This symptom is observed while changing the configurations from a same slot FRR to a different slot FRR.

  Workaround: Reload the router.

- CSCtq62759

  Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.

  Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq63744

  Symptoms: MAC withdrawal is not sent to the core VCs on reception of STP TCN for MST.

  Conditions: This symptom is seen when access has switchport only.

  Workaround: There is no workaround.

- CSCtq67970

  Symptoms: Inter-AS IPv4 multicast streams do not resume if the source of the multicast stream is stopped. The s,g state expires in the transit AS, and traffic source is started again.

  Conditions: This symptom occurs when BGP PIC CORE/EDGE is configured in the system.

  Workaround: There is no workaround.

- CSCtq71011

  Symptoms: The router crashes, or in some cases a traceback is seen.

  Conditions: This symptom is seen when IPv6 routes with diverse paths are enabled.

Workaround: There is no workaround.

- CSCtq79767

  Symptoms: IPSEC key engine crashes after using the **clear crypto session** command on CES.

  Conditions: This symptom occurs under the following conditions:

  1. Topology:

     IXIA --> CES (DVTI Client) --> UUT (DVTI Server)-->

  2. Configuration:

     1000 vrf x 1 IKE session x 4 IPsec SA dual

  3. The crash on UUT is seen after using the **clear crypto session** command on CES after all SAs have been established.

  Workaround: There is no workaround.

- CSCtq80603

  Symptoms: Newly created SVIs are in down/down state.

  Conditions: This symptom occurs when SW VLAN RP process is stuck.

  Workaround: The following workarounds may work:

  1. Set the memory location of l2vlanifmib_access_count to zero after warm restart of snmp-sever.
  2. Perform SSO and/or LC OIR.
  3. Perform an active reload.

- CSCtq83677

  Symptoms: High traffic loss (around 15 sec) is seen for receivers on MVR receiver ports during SSO.

  Conditions: This symptom is seen during SSO.

  Workaround: There is no workaround.

- CSCtq85564

  Symptoms: The fix of CSCto77352 may cause a data corruption problem.

  Conditions: This symptom is seen when two processes are calling the same function that is raising the race condition.

  Workaround: There is no workaround.

- CSCtq86216

  Symptoms: Multicast traffic flows over both primary and backup interfaces during TEFRR reopt.

  Conditions: This symptom occurs when multicast traffic flows over an MLDP core with TEFRR link protection.

  Workaround: Duplicate traffic flows only for a short period of time (20 seconds). So, the issue gets automatically resolved after 20 seconds.

- CSCtq91305

  Symptoms: Standby cannot reach HOT sync state with active. The standby RP keeps resetting. The following message is displayed:

  ```
  %SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1),process
  = IPC Dynamic Cache.
  ```

Conditions: This symptom occurs with SSO mode, when the Cisco ASR 1000 series router is configured with ISG as dhcp server and with a low dhcp lease timer.

Workaround: There is no workaround.

- CSCtq91403

  Symptoms: High CPU can be seen during reloads under the MVPN topology.

  Conditions: This symptom occurs in an MVPN network with an S,G with an incoming interface over the MDT tunnel, when there are no forwarding interfaces for that S,G.

  Workaround: A possible workaround is to create a static join for that S,G to protect the RP CPU. Also, in some case multicast rate-limiters will be useful.

- CSCtq92182

  Symptoms: An eBGP session will not be established.

  Conditions: This issue is seen when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtq93823

  Symptoms: Ping drops with fragment size of 256.

  Conditions: This symptom occurs when doing a sweep ping with sizes 500 to 1000.

  Workaround: Flap the interfaces.

- CSCtq94418

  Symptoms: Adding, deleting, and re-adding an access subinterface may sometimes lead to loss of data path.

  Conditions: The symptom is observed when the configuration sequence involves an add-delete-add sequence.

  Workaround: Create dummy access subinterfaces belonging to a new vrf. Do not remove the interface.

- CSCtq97646

  Symptoms: A Cisco 7600 ES+ and SIP-400 card may crash when Dynamic Ethernet Services Activation (DESA) is configured, and certain attributes are downloaded from a radius server.

  Conditions: This symptom is seen when DESA is configured, and the radius profile that it downloads for an EVC contains an idle-timeout and dot1q range for the “stag-vlan-id” attribute. The card will crash.

  The ES+ card will crash as soon as the attributes are downloaded while a SIP- 400 may crash when the idle-timer expires.

  Radius Example:

```
simulator radius subscriber 25029
# [28] idle-timeout
 attribute 28 numeric 60
 vsa cisco generic 1 string "subscriber:sss-service=vpws"
 vsa cisco generic 1 string "l2vpn:service-
id=atom_from_agg22_to_dist2_int1_cfg1_1_of_1000"
 vsa cisco generic 1 string "l2vpn:redundancy-group=2"
 vsa cisco generic 1 string "ethernet-service-instance:service-instance-
```

```
description=... Dynamic EFP on Po2, stag:2000-2009, CFG_SEQ:1306963076"
 vsa cisco generic 1 string "l2vpn:redundancy-priority=2"
 vsa cisco generic 1 string "cdp:l2protocol-pdu-action=forward"
 vsa cisco generic 1 string "accounting-list=ACCT11"
 vsa cisco generic 1 string "ethernet-service-instance:stag-vlan-id=2000-
2009"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress=1"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-tag-
operation=Push1"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-stag-
type=0x8100"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-stag-
vlanid=1100"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-
symmetric=TRUE"
!
```

The card will not crash if either dot1q range or IDLE-Timeout is absent from the downloaded configuration.

Workaround: Configure radius to either not send an idle-timeout value or to not send a dot1q range.

- CSCtr06867

  Symptoms: There is no response to SNMP queries of the MIB objects:

  ```
  1.3.6.1.4.1.9.9.276.1.1.2.1.11 cieIfSpeedReceive
  1.3.6.1.4.1.9.9.276.1.1.2.1.12 cieIfHighSpeedReceive
  ```

  The OID is incorrect in the MIB definition.

  Conditions: This symptom is observed when SNMP walk is not returning any data for the following OIDs:

  ```
  "cieIfSpeedReceive"            "1.3.6.1.4.1.9.9.276.1.1.2.1.11"
  "cieIfHighSpeedReceive"        "1.3.6.1.4.1.9.9.276.1.1.2.1.12"
  ```

  Workaround: There is no workaround.

- CSCtr37182

  Symptoms: XAUI coding errors are seen on the console.

  Conditions: This symptom is observed on a Cisco 7600 series router.

  Workaround: There is no workaround.

Caveats for Cisco IOS Release 15.1(2)S

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section consists of the following subsections:

Resolved Caveats—Cisco IOS Release 15.1(2)S2

Cisco IOS Release 15.1(2)S2 is a rebuild release for Cisco IOS Release 15.1(2)S. The caveats in this section are resolved in Cisco IOS Release 15.1(2)S2 but may be open in previous Cisco IOS releases.

- CSCti42671

  Symptoms: The state of MLP bundles on active RP and standby RP is not in sync. Some of the bundles that are active on active RP, show up as inactive on standby RP. This may result in the bundles going to down state after switchover.

  Conditions: This symptom occurs under the following conditions:

  1. Configure scaled number of MLP bundles on 1xCHOC12 SPA.
  2. Reload the SPA.

  Workaround: Reload the standby RP.

- CSCti48483

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

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

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

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCti83542

  Symptoms: MPLS LDP flapping is seen with T3 SATOP CEM interface configurations.

  Conditions: This issue is seen with T3/E3 SATOP TDM configurations.

  Workaround: There is no workaround.

- CSCti98219

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtj04672

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtj14525

  Symptoms: Standby is not synced to active after attaching a new policy.

  Conditions: This symptom happens when dynamic policy is used such as RADIUS CoA.

  Workaround: There is no workaround.

- CSCtk67768

  Symptoms: RP crash is observed in DHCPD receive process.

  Conditions: This symptom occurs on the DHCP server that is used on Cisco ASR routers and acting as ISG.

  Workaround: There is no workaround.

- CSCtk69114

  Symptoms: RP resets while doing ESP reload with crypto configuration.

Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.

Workaround: There is no workaround.

- CSCtl00995

  Symptoms: Cisco ASR 1000 series routers with 1000 or more DVTIs may reboot when a shut/no shut operation is performed on the tunnel interfaces or the tunnel source interfaces.

  Conditions: This symptom occurs when all the DVTIs have a single physical interface as tunnel source.

  Workaround: Use different tunnel source for each of the DVTIs. You can configure multiple loopback interfaces and use them as tunnel source.

- CSCtl49917

  Symptoms: Minor diagnostic error is seen on SIP-400.

  Conditions: This symptom occurs when scaled configurations are applied to ES+ and SIP-400. The BusConnectivity test fails on SIP-400 during boot-up.

  Workaround: Power enable SIP-400 after all the line cards have come up in the test bed. Or, after a couple of retries, reload SIP-400, and it automatically comes up.

- CSCtn15317

  Symptoms: Traffic on MPLS VPN is dropped. When you check LFIB information on the P router, the entry has an instruction to TAG all packets that are destined to the PE router instead of a POP instruction which is expected on a directly connected P.

  Conditions: This symptom occurs with the following conditions:

  - The ISIS protocol is running as IGP on MPLS infrastructure.
  - ISIS on the PE router is summarizing network that includes BGP vpnv4 update-source.
  - The P router is running an MFI-based image.

  Workaround 1: Remove the **summary-address** command in ISIS on PE.

  Workaround 2: Change the BGP update source.

- CSCtn18784

  Symptoms: Interface Tunnel 0 constantly sends high-bandwidth alarms.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn19027

  Symptoms: The **show mediatrace responder sessions brief** command crashes the router.

  Conditions: This symptom is observed on Mediatrace Responder when showing a stale session.

  Workaround: There is no workaround. Avoid issuing this impacted **show** command.

- CSCtn40571

  Symptoms: Issuing the **crypto pki server** *name* **rollover cancel** command can result in multiple rollover certificates installed on Sub-CA router.

  Conditions: This symptom is seen when the rollover certificate is already installed.

  Workaround:

  - Copy startup-configuration from router.

  - Remove the older rollover certificate from configuration under the **crypto pki cert chain** *ca* command.
  - Copy the new configuration back to startup-configuration and reload the router.

- CSCtn44232

  Symptoms: With multiple RP switchovers, both RPs become unusable.

  Conditions: This symptom is observed with multiple RP switchovers.

  Workaround: There is no workaround.

- CSCtn58128

  Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

  Conditions: The issue may be triggered by route-flaps in scaled scenario where the route reflector may have 4000 route reflector clients and processing one million+ routes.

  Workaround: Ensure “no logging console” is configured.

- CSCtn64879

  Symptoms: After configuring service group, traffic will go through both of the memberlinks of Ethernet Virtual Connection (EVC) point of contact (PoC) with xconnect.

  Conditions: This symptom is seen when defaulting the PoC configuration and adding it back.

  Workaround: Reset line card.

- CSCtn67637

  Symptoms: Traffic is not forwarded from the DECAP PE in the egress replication mode.

  Conditions: This symptom occurs when the ingress LC on the DECAP PE is a CFC LC like 6748/SIP400 and the egress replication mode is used on the DECAP PE in a mVPN setup.

  Workaround: Switch to the ingress replication mode on the DECAP PE. Then, the traffic will start flowing.

- CSCtn68117

  Symptoms: The **session** command does not work on Cisco 3000 series routers that have become the master after a mastership change.

  Conditions: This symptom is seen when fail-over to slave occurs.

  Workaround: There is no workaround.

- CSCtn96521

  Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.

  Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.

  Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- CSCtn97451

  Symptoms: The BGP peer router crashes after executing the **clear bgp ipv4 unicast** *peer* command on the router.

  Conditions: This symptom occurs with the following conditions:

  Router3 ---ebgp--- Router1 ---ibgp--- Router2

Router1:

```
--------
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-mode
!

router ospf 100
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 10.1.1.2 remote-as 1
 neighbor 10.1.1.3 remote-as 11
!
```

Router 2:

```
--------
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 100
 redistribute static
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
 bgp log-neighbor-changes
 network 0.0.0.0
 redistribute static
 neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

Router 3:

```
-------
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip pim sparse-mode
!

router bgp 11
bgp log-neighbor-changes
 network 0.0.0.0
```

```
 network 0.0.0.0 mask 255.255.255.0
 redistribute static
 neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

Reproduce crash with the following steps:

1. Traffic travel from router 3 to router 2.
2. “clear bgp ipv4 unicast 10.1.1.1” on router 2.

Workaround: There is no workaround.

- CSCto00796

  Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

  Conditions: This symptom occurs when a new interface is provisioned inside a vrf and the configuration such that the connected routes are redistributed in the vrf. This redistributed route fails to tag itself with the RT when it reaches the peering PE(+RR)

  Workaround: Soft clear the peer that missed getting the RT.

- CSCto07586

  Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

  Conditions: This symptom occurs with the following conditions:

  – Create an IOS image that does not IPV6 enabled.
  – Enable BFD on an interface.
  – Configure an IPV4 static route with BFD routing through the above interface.

  The IPV4 BFD session does not get established, so the static route does not get installed.

  Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCto11957

  Symptoms: PPPoE is terminated on port-channel with ES+ session limit error occurring incorrectly.

  ```
  %CWAN_RP-6-SESS_LIMITS_PORT_GROUP: Exceeded max number of sessions supported
  on
  ```

```
port-group
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
[ADJ:PPPoE:5789] - hardware platform error.

Mismatch in sessions on RP and ES+:
BRAS#sh pppoe summary
    PTA  : Locally terminated sessions
    FWDED: Forwarded sessions
    TRANS: All other sessions (in transient state)

                                TOTAL     PTA   FWDED   TRANS
TOTAL                              57      56       0       1
Port-channel100                    57      56       0       1

BRAS#show platform isg session-count 4
 ES+ line card
 Sessions on a port-channel are instantiated on all member ports
 Port-group          Sess-instance   Max Sess-instance
 ----------          -------------   -----------------
 Gig4/11-Gig4/15              2936                4000 <<<<<<< INCORRECT
```

Conditions: This symptom is seen when scaled PPPoE sessions are terminated on port-channel with ES+ ports. Sessions negotiate, disconnect and attempt to renegotiate port-channel number other than port-channel 2.

Workaround: Change port-channel number to port-channel 2. Configure sessions to terminate on stand-alone ports.

- CSCto16106

  Symptoms: Address not assigned when “ip dhcp use class aaa” is configured.

  Conditions: When the DHCP server is configured to download a class name from the radius using “ip dhcp use class aaa” and lease an IP address from that class, the IP address is not assigned to the client.

  Workaround: There is no workaround.

- CSCto31265

  Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.

  Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

  Workaround 1: Delete/re-add the static route that generates Type7.

  Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

  Workaround 3: Execute the **clear ipv6 ospf redistribution** command on ASBR.

- CSCto35160

  Symptoms: After switchover, traffic drops are seen in CARRIER-Ethernet testcase for about 15 seconds. This issue is not seen consistently.

  Conditions: This symptom is seen after switchover.

Workaround: Will auto restore after 15 seconds.

- CSCto41165

  Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit|deny** command, and then the **no ip extcommunity-list 55 permit|deny** command.

  Conditions: This symptom occurs when the standby router is configured.

  Workaround: There is no workaround.

- CSCto41223

  Symptoms: Standby IOSD crashes when standby RP reload is executed.

  Conditions: This symptom is observed in a scaled configuration with 8000 EoMPLS and 8000 EVC sessions while the traffic is flowing. On issuing standby RP reload, IOSd crashes at the process “Standby service handler”.

  Workaround: There is no workaround.

- CSCto46716

  Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.

  Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In “debug ip ospf spf”, when the SPF process link for the TE tunnel is in its own RTR LSA, the “Add path fails: no output interface” message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

  Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto55643

  Symptoms: High CPU loading conditions can result in delayed download of multicast routes to line cards, resulting in multicast forwarding (MFIB) state on line cards out of sync with the RP. The **show mfib linecard** command shows line cards in sync fail state with many in LOADED state.

  Conditions: This symptom occurs during high CPU loading due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted processed switched packets, before HW forwarding can be programmed.

  Workaround: There is no workaround. Ensure that mls rate limits are properly configured.

  Further Problem Description: IPC errors may be reported in the MRIB Proxy communications channel that downloads multicast routes to line cards.

- CSCto55983

  Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.

  Conditions: This symptom occurs during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in sync.

  Workaround: There is no workaround.

- CSCto63720

  Symptoms: No traffic passes after a link flap if port-security is configured on the Gigabit Ethernet interface on 6748 LC.

Conditions: This symptom occurs when the Cisco IOS version running is Cisco IOS Release 12.2(33)SRE2. This issue is seen when port-security is configured on a 6748 port and the link flap occurs on this interface.

Workaround: Reconfiguring port-security fixes the problem.

- CSCto69071

  Symptoms: Metrics collection fails due to invalid DVMC runtime object handle.

  Conditions: This symptom occurs when the transport layer is not passing up an interface type that is acceptable to DVMC.

  Workaround: There is no workaround.

- CSCto71004

  Symptoms: Router crashes with high scale and a lot of BGP routes. This crash is seen in the box when core links flap.

  Conditions: This symptom is seen when scaled box with a lot of BGP routes crashes the box when some of the core links flap.

  Workaround: There is no workaround.

- CSCto72480

  Symptoms: The output of the **show mfib linecard** command shows that line cards are in “sync fail” state.

  Conditions: This symptom occurs usually when the last reload context displayed in the **show mfib linecard internal** command output is “epoch change”. This indicates that an IPC timeout error has occurred in the MRIB communications channel that downloads multicast routing entries to the multicast forwarding information base (MFIB). In this condition, multicast routing changes are not communicated to the failed line cards and they are not in sync with the RP.

  Workaround: If this issue is seen, using the **clear mfib linecard** *slot* command may clear the problem. If the problem occurs on a Cisco 7600 SP, an RP switchover is required after clearing the problem on any affected line cards. The workaround may not completely work if high CPU loading continues to be present and IPC errors are reported.

  Further Problem Description: The IPC timeout errors could result from high CPU loading conditions caused by high rates of processed switched packets. High rates of multicast processed switched packets can be avoided if rate limits are applied after each router boot, especially after using the **mls rate-limit multicast ipv4 fib-miss** command.

- CSCto75643

  Symptoms: Few ISIS packets get subjected to QoS. In case of congestion, this may cause ISIS protocol flaps.

  Conditions: This symptom occurs only when “isis network point-to-point” is configured.

  Workaround: Add a class-map to classify ISIS control packets and allot bandwidth for it.

- CSCto76018

  Symptoms: Cisco ASR1000-WATCHDOG process crashes on DVTI Server after clearing crypto session on DVTI Client.

  Conditions: This symptom occurs for sessions with the configuration of 1000 vrf, 1 IKE session per vrf, and 4 IPSec SA dual per session. The ASR1000- WATCHDOG process crashes on DVTI Server during clear crypto session on DVTI client, after all the SAs have been established.

  Workaround: There is no workaround.

- CSCto77504

  Symptoms: With shape configured on port-shaper and bandwidth-percent configured on groups in the EVC, on dynamic configuration of port-shaper value, the groups do not get the updated shape values based on bandwidth percent.

  Conditions: This symptom is seen when bandwidth-percent is configured on group or EVC with port-shaper.

  Workaround: There is no workaround.

- CSCto80714

  Symptoms: Prowler SPA goes out of service with heartbeat failures when traffic flows through the MLPPP (multilink) interface. This issue is seen only in the Cisco IOS Release 12.2SRE throttle and not in mcp_dev. Some optimizations and a microcode reload-related fix is also included as part of this DDTS.

  Conditions: This symptom is observed when traffic flows through the MLPPP interface on Prowler. Microcode and SPA reload is required to recover.

  Workaround: There is no workaround.

- CSCto88581

  Symptoms: The standby RP crashes following an interface configuration change.

  Conditions: This symptom is observed only when “ospf non-stop routing” is configured.

  Workaround: There is no workaround.

- CSCto88660

  Symptoms: Command failure on RP is causing both protecting and working APS to go to active.

  Conditions: This symptom may be caused by switchover during scaled conditions.

  Workaround: There is no workaround.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

- This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml. CSCto90252

  Symptoms: A standby route processor (RP) is stuck to “init, standby” for about 10 hours.

  Conditions: This symptom occurs after reloading five or six times on a Cisco ASR 1000 series router.

  Workaround: Disable NSR.

- CSCto98212

  Symptoms: The IPv6 address and prefix 2001:DB8:1:104::/64 at 25 Aug 2011 00:01 25 Jul 2011 00:01 are lost after a router reload.

  Conditions: This command checks for the clock validity. When the router reloads the clock validity is displayed as “not yet valid”. This causes the command to not be applied.

Workaround: There is no workaround.

- CSCto99523

  Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

  Conditions: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

  Workaround: There is no workaround.

- CSCtq04117

  Symptoms: DUT and RTRA have IBGP-VPNv4 connection that is established via loop back. OSPF provides reachability to BGP next hop, and BFD is running.

  Conditions: This symptom occurs under the following conditions:

  1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
  2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

  Workaround: Use the **clear ip route vrf x *** command.

- CSCtq06538

  Symptoms: RP crashes due to bad chunk in MallocLite.

  Conditions: This symptom occurs while executing testcase number 4883. The test case 4883 sends an incorrect BGP update to the router to test whether the router is able to handle the problematic update. The incorrect BGP update has the local preference attribute length incorrect:

```
LOCAL_PREF
        Header
          AttributeFlags
            Optional: 0b0
            Transitive: 0b1
            Partial: 0b0
            ExtendedLength: 0b0
            Unused: 0b0 0b0 0b0 0b0
          TypeCode: 0x05
          Length: 0x01    <----- should be 0x04 instead
        Value: 0xff 0xff 0xff 0xff
    NetworkLayerReachabilityInfo: 0x08 0x0a <snip>
```

  Workaround: There is no workaround.

- CSCtq10019

  Symptoms: After router reload, rate-limiters for multicast do not come into effect and packets are punted.

  Conditions: This symptom occurs during high CPU load when mfib is unable to distribute into lc and SP.

  Workaround: There is no workaround.

- CSCtq21785

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(2)S may crash upon performing a CRL check on an invalid certificate.

  Conditions: The conditions are unknown.

  Workaround: Turning off CRL check should stop the crash. It should be configured as:

  “revocation-check none”

  This will stop the CRL check of the peer certificate but should not be a long term solution.

- CSCtq22873

  Symptoms: Router may show the following traceback (error message) after receiving certain IPv6 packets:

  ```
  TB:%SCHED-2-EDISMSCRIT:process=PuntInject Keepalive Process
  ```

  Conditions: This symptom is seen when router is configured for IPv6 routing.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq23038

  Symptoms: With “platform control-packets use-priority-q disable” configured on the port-channel main interface, after shut/no shut on the port-channel or member-link, port-channel subinterfaces do not inherit the “platform control-packets use-priority-q disable” feature.

  Conditions: This symptom occurs when you perform shut/no shut on a member-link or link flaps with port-channel subinterfaces and “platform control-packets use-priority-q disable” configured on the port-channel.

  Workaround: A possible workaround is to remove and reconfigure the subinterfaces.

- CSCtq23158

  Symptoms: The dlfi o atm fails to come up on sip400 with Cisco IOS Release 15.0(1)S images onwards if an ES+ card is present.

  Conditions: This symptom occurs when you cannot bring up dlfi o atm.

  Workaround: A possible workaround is to power down all ES+ cards.

- CSCtq23793

  Symptoms: After reloading PE router in mVPN network, multicast traffic stops on one of the VRFs randomly.

  Condition: This symptom occurs under the following conditions:

  -When reloading a PE in mVPN network. -When PE has many VRFs and scaled mVPN configuration.

  Workaround: Remove and add MDT configuration.

- CSCtq30686

  Symptoms: A Cisco router crashes in a Secure Device Provisioning (SDP) environment.

Conditions: This symptom is seen when the Registrar router crashes when a client router submits an enrollment request that was previously stuck in “granted” status with the same fingerprint.

Workaround: There is no workaround.

- CSCtq32896

  Symptoms: LSM entries stop forwarding traffic.

  Conditions: This symptom is observed after Stateful Switchover (SSO).

  Workaround: There is no workaround.

- CSCtq34807

  Symptoms: Service group does not take effect on EVC Xconnect on a port channel.

  Conditions: This symptom is observed with a service group configuration on EVC Xconnect existing on a port channel. This issue is seen when EVC is removed and the configuration is reapplied.

  Workaround: Remove and reapply the service group.

- CSCtq43480

  Symptoms: A Cisco router crashes.

  Conditions: This symptom occurs when a session starts with PBHK and accounting features while the method list is not provisioned for the accounting features.

  Workaround: There is no workaround.

- CSCtq46745

  Symptoms: Custom configured default sip profiles (option/method/header) are lost during a router reload.

  Conditions: This symptom occurs during reload.

  Workaround: Use non-default profiles for each adjacency.

- CSCtq46760

  Symptoms: When doing ISSU subpackage upgrade from Cisco IOS XE Release 3.2.2 to Cisco IOS XE Release 3.4.0 with the Cisco IOS XE Release 2.3 feature set, both FPs crash and multiple core files are seen after the last ISSU step, active RP loadversion.

  Conditions: This symptom only occurs on Cisco ASR1006 subpackage upgrade with dual RPs.

  Workaround: Reload the standby RP before switchover.

- CSCtq50674

  Symptoms: Total traffic drop is seen for 6PE/6VPE when IPFRR is configured in the core.

  Conditions: This symptom occurs when BGP/6PE peer is protected by IPFRR in core.

  Workaround: There is no workaround.

- CSCtq62759

  Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.

  Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq63744

  Symptoms: MAC withdrawal is not sent to the core VCs on reception of STP TCN for MST.

  Conditions: This symptom is seen when access has switchport only.

  Workaround: There is no workaround.

- CSCtq67680

  Symptoms: An SPA reload triggers silent LC reload under the following steps:

  1. Configure policy-maps as shown below:

     ```
     policy-map mul1
     class GOLD
     priority 1000
     class SILVER
     bandwidth 1000
     policy-map mul2
     class GOLD
     priority 7000
     class SILVER
     bandwidth 7000
     class class-default
     random-detect
     ```

  2. Apply it on multilink interfaces - multilink1 and multilink2.
  3. Reload the SPA.

  Conditions: This issue is seen only with QoS policy applied on multilink bundle on serial SPA.

  Workaround: There is no workaround.

- CSCtq67970

  Symptoms: Inter-AS IPv4 multicast streams do not resume if the source of the multicast stream is stopped. The s,g state expires in the transit AS, and traffic source is started again.

  Conditions: This symptom occurs when BGP PIC CORE/EDGE is configured in the system.

  Workaround: There is no workaround.

- CSCtq77363

  Symptoms: License images are not working properly.

  Conditions: This symptom is seen when the license image is loaded. There is a traceback due to access of uninitialized variables.

  Workaround: There are no workarounds.

- CSCtq83629

  Symptoms: The error message is associated with a loss in multicast forwarding state on line cards under scaled conditions when an IPC error has occurred.

  Conditions: This symptom is observed during router boot or high CPU loading, which can cause IPC timeout errors. This issue is seen on line cards during recovery from an IPC error in the MRIB channel.

  Workaround: Line card reload is required to resolve the problem.

- CSCtq92182

  Symptoms: An eBGP session is not established.

  Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtq93823

  Symptoms: Ping drops with fragment size of 256.

  Conditions: This symptom occurs when doing a sweep ping with sizes 500 to 1000.

  Workaround: Flap the interfaces.

- CSCtq94418

  Symptoms: Adding, deleting, and re-adding an access subinterface may sometimes lead to loss of data path.

  Conditions: The symptom is observed when the configuration sequence involves an add-delete-add sequence.

  Workaround: Create dummy access subinterfaces belonging to a new vrf. Do not remove the interface.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when bgp deterministic-med is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtq97646

  Symptoms: A Cisco 7600 ES+ and SIP-400 card may crash when Dynamic Ethernet Services Activation (DESA) is configured, and certain attributes are downloaded from a radius server.

  Conditions: This symptom is seen when DESA is configured, and the radius profile that it downloads for an EVC contains an idle-timeout and dot1q range for the “stag-vlan-id” attribute. The card will crash.

  The ES+ card will crash as soon as the attributes are downloaded while a SIP- 400 may crash when the idle-timer expires.

  Radius Example:

```
simulator radius subscriber 25029
 <b># [28] idle-timeout
 attribute 28 numeric 60</b>
 vsa cisco generic 1 string "subscriber:sss-service=vpws"
 vsa cisco generic 1 string "l2vpn:service-
id=atom_from_agg22_to_dist2_int1_cfg1_1_of_1000"
 vsa cisco generic 1 string "l2vpn:redundancy-group=2"
 vsa cisco generic 1 string "ethernet-service-instance:service-instance-
description=... Dynamic EFP on Po2, stag:2000-2009, CFG_SEQ:1306963076"
 vsa cisco generic 1 string "l2vpn:redundancy-priority=2"
 vsa cisco generic 1 string "cdp:l2protocol-pdu-action=forward"
 vsa cisco generic 1 string "accounting-list=ACCT11"
 vsa cisco generic 1 string "ethernet-service-instance:stag-vlan-id=<b>2000-
2009</b>"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress=1"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-tag-
operation=Push1"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-stag-
type=0x8100"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-stag-
vlanid=1100"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-
symmetric=TRUE"
!
```

The card will not crash if either dot1q range or IDLE-Timeout is absent from the downloaded configuration.

Workaround: Configure radius to either not send an idle-timeout value or to not send a dot1q range.

- CSCtr07704

  Symptoms: While using scripts to delete non-existent class map filter from a class, the router sometimes crashes (c2600XM) or returns traceback spurious memory access (c2801nm).

  Conditions: This symptom occurs when trying to delete a non-existent classmap filter, the classmap will be NULL, and passed to match_class_params_same. This results in referencing a null pointer.

  Workaround: Do null check in match_class_command and match_class_params_same. To keep existing behavior, do not print out a message like “the class does not exist” when deleting a non-existent class map from a class.

- CSCtr22007

  Symptoms: A Cisco 7600 router that is configured with RSVP crashes.

  Conditions: The condition is unknown.

  Workaround: There is no workaround.

- CSCtr30820

  Symptoms: IP address is not assigned to the client after a DHCP request.

  Conditions: The problem is observed while verifying the VRF-aware-DHCP functionality in Cisco IOS relay and server in an MPLS setup.

Workaround: There is no work around.

Resolved Caveats—Cisco IOS Release 15.1(2)S1

Cisco IOS Release 15.1(2)S1 is a rebuild release for Cisco IOS Release 15.1(2)S. The caveats in this section are resolved in Cisco IOS Release 15.1(2)S1 but may be open in previous Cisco IOS releases.

- CSCtd10712

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtd23069

  Symptoms: A crash occurs because of a SegV exception after configuring the **ip virtual-reassembly** command.

  Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 and Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCth52252

  Symptoms: Two EzVPN clients behind the same NAT device initiate sessions to dVTI EzVPN Server. When the first client connects, traffic is successful. When the second client also connects, traffic is successful for the second client, but fails for the first client.

  Conditions: This symptom is observed when two EzVPN clients behind the same NAT device initiate sessions to dVTI EzVPN Server.

  The drop reason is

  sh pl ha qf ac fe ipsec data drop

  Drop Type Name Packets

  ---

  30 IN_V4_POST_INPUT_POLICY_FAIL 8

  The same scenario is supported with dynamic crypto map configuration.

  Workaround: Use legacy EZVPN and RRI. Only partial functionality of DVTI is achieved.

- CSCth69364

  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://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml.

- CSCti64685

  Symptoms: User may not be able to configure SLA MPLS configuration.

  Conditions: This symptom occurs when the router is booted up and may be random.

  Workaround: There is no workaround.

- CSCti92812

  Symptoms: After physical interface flap, GRE tunnel for VRF does not come up correctly.

  Conditions: This symptom occurs when GRE tunnel is configured for default (global) routing table.

  Workaround: There is no workaround.

- CSCtj46670

  Symptoms:

  IPCP cannot complete after dialer interface is moved out of Standby mode CONFREJ is seen while negotiating IPCP

  Conditions: The symptom is observed when a dialer interface has moved out from standby mode.

  Workaround: Reload the router.

- CSCtj55624

  Symptoms: A router crashes upon entering the **show crypto ruleset** command.

  Conditions: This symptom is seen when version 6 crypto maps are configured.

  Workaround: Do not run the **show** command.

- CSCtj65692

  Symptoms: The service policy applied to a service instance stops forwarding any traffic. The output of the **show policy-map interface** *x/y* command indicates that all packets are hitting the violation queue. The conform counter does not increase at all and all traffic is dropped.

  Conditions: This symptom is observed in Cisco 7600 running Cisco IOS Release 12.2SRD. This issue is applicable for the service policy applied for ingress or egress traffic.

  Workaround: There is no workaround. To restore the services, the service policy has to be removed from the service instance, and then the condition clears. The service policy can then be reapplied and will work normally.

- CSCtj78966

  Symptoms: A Cisco ASR 1000 router crashes with thousands of IKEv2 sessions, after many operations on IKEv2 session.

  Conditions: This symptom is seen when IKEv2 SA DB WAVL tree is getting corrupted if we fail to insert the SA due to some error, for example, PSH duplication.

  Workaround: There is no workaround.

- CSCtj87846

  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

  Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

  Workaround: Do shut/no shut on PfR master or PfR border.

- CSCtj91149

  Symptoms: A delay of approximately 30 seconds is observed in dynamic xconnect- based ISG session that comes up on standby, after it is up on active.

  Conditions: This symptom occurs on switchover.

  Workaround: There is no workaround.

- CSCtj94510

  Symptoms: When sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and 4 SA dual per session, a crash happens on Crypto_SS_process.

  Conditions: This symptom occurs when sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and four SA dual per session.

  Workaround: There is no workaround.

- CSCtk12122

  Symptoms: A Cisco 7200 router may crash after clearing the SAs while using the IKE keepalive feature.

  Conditions: This symptom occurs when the IKE keepalive feature is turned on, and the user executes a **clear crypto session** command or a **clear crypto sa** command.

  Workaround: There is no workaround.

- CSCtk46381

  Symptoms: Service Policy installation on L2transport PVP fails when shaping rate is changed.

  Conditions: This symptom is seen when the PVP shape rate is changed.

  Workaround: Remove the service-policy and add again.

- CSCtk76697

  Symptoms: Service instances on the line card go to the down state for the approximately first 100 service instances of 4000 service instances after a test crash on the line card, resulting in a complete traffic drop on these service instances.

  Conditions: This symptom occurs only during the first test crash on the LC after booting up the router.

  Workaround: A shut/no shut on the service instance/interface will resolve this issue.

- CSCtk83638

  Symptoms: Client gets assigned an IP address from an incorrect pool when it reconnects with a different profile.

  Conditions: This symptom is been observed in a setup where two clients are behind a NAT router. When one client connection is broken and the server is not made aware of this, and the client reconnects with a different group, the IP address assigned is not from the correct pool.

  Workaround: There is no workaround.

- CSCtk95106

  Symptoms: CPU 1 of SPA 8XT1E1 goes into a forced reload followed by a software forced reload of line card SIP-200 when a multilink PPP with interleave enabled having fragment size 42 is disabled and enabled. One member of the link is removed.

  Conditions: This issue is noticed when traffic is pumped onto the DUT from remote end. Size could be as low as 800 bytes. Interleave is disabled and enabled on the mulilink interface, and one of the members of the MP is detached from the bundle using the **no ppp multlink group** <> command.

Workaround: There is no workaround.

- CSCtl70143

  Symptoms: LAC does not forward a PPP CHAP-SUCCESS message from LNS to client sometimes.

  Condition: This symptom is seen when T1/PRI is used between the client and LAC.

  Workaround: There is no workaround.

- CSCtl78285

  Symptoms: In VRF configuration, we are not able to add rd after deleting rd configuration once:

```
A-SUP5-6509E#sho run | be vrf
ip vrf CUST1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 239.39.39.39



A-SUP5-6509E(config)#ip vrf CUST1
A-SUP5-6509E(config-vrf)#no rd 1:1
% "rd 1:1" for VRF CUST1 scheduled for deletion

wait for some time and try to add rd again (waited for more than 2 hrs)

A-SUP5-6509E(config)#ip vrf CUST1
A-SUP5-6509E(config-vrf)#rd 1:1
% Deletion of "rd" in progress; wait for it to complete
A-SUP5-6509E(config-vrf)#
```

  Conditions: This symptom is seen in a VRF configuration with rd.

  Workaround: Remove VRF configuration and add again.

- CSCtl82517

  Symptoms: For the Cisco ME3600 and Cisco ME3800, the following licensing errors are seen, leading to license manager failure at bootup:

```
%SCHED-7-WATCH: Attempt to lock uninitialized watched semaphore (address 0).
-Process= "Init", ipl= 4, pid=
```

  Conditions: This symptom is seen when a Cisco ME3600 or Cisco ME3800 license-based image is loaded off mcp_dev_nile.

  Workaround: Use whales-universal-mz.

- CSCtl84797

  Symptoms: SBC traceback occurs.

  Conditions: This issue is observed when LI is enabled and there are multiple media sessions in a single call (that is, SDP contains information about multiple media sessions).

  Workaround: There is no workaround.

- CSCtl92210

  Symptoms: A router may crash when trying to show the sessions on responder while the session queue is being managed (removal).

  Conditions: This symptom occurs while new sessions are being provisioned or removed from Mediatrace initiator side. The router can crash when trying to show the session objects on the responder while the session queue is being managed (removal) by first disabling the initiator using the **no mediatrace initiator force** command and then disabling responder with the **no mediatrace responder** command.

  Workaround: Do not disable initiator with the **no mediatrace initiator force** command and responder with the **no mediatrace responder** command in quick succession while the **show mediatrace responder session [brief | details]** command is not finished with output or in pause mode.

- CSCtl99266

  Symptoms:

  1. CoA service logon is not synced to standby.
  2. CoA multiservice logon/logoff is not synced to standby.

  Conditions:

  For issue 1:

  - Do CoA service logoff of a service that was not installed via CoA service logon (i.e. installed through a rule or as an auto service). This gets synced to standby.
  - Do CoA service logon of the same service. This is not synced.

  For issue 2:

  - Do CoA multiservice logon/logoff of more than 1 service. The services are applied/unapplied on active, but not on standby.

  Workaround:

  For issue 1:

  - After the CoA service logon is not synced, reboot the standby.
  - After the standby comes up, a bulk sync from the active is initiated, which will sync the service logon.

  For issue 2: There is no workaround.

- CSCtn11326

  Symptoms: The Structure-agnostic TDM over Packet (SAToP) PW remains down when the AC is down.

  Conditions: This problem is seen if the xconnect configuration is applied on a CEM AC, which is in down state.

  Workaround: There is no workaround.

- CSCtn16840

  Symptoms: VPLS imposition traffic does not go through for some of the VCs when the core is a port channel on ES20.

  Conditions: This symptom is observed when core facing is a port channel on ES20.

  Workaround: Do a shut/no shut on the port channel.

- CSCtn17680

  Symptoms: When performing an OIR on a Cisco WS-X6708 module, the router may crash. When inserting the card, the following message is displayed:

  ```
  %EARL_L2_ASIC-SP-4-DBUS_HDR_ERR: EARL L2 ASIC #0: Dbus Hdr. Error occurred. Ctrl1
  0xB88D0E3D
  ```

  Then, the following message is displayed:

  ```
  %CPU_MONITOR-SP-2-NOT_RUNNING: CPU_MONITOR messages have not been sent for 60 seconds
  [*Sched* 41%/0% (00:01:00.244 99%/99%)]
  ```

  Finally, a timeout occurs, followed by the crash:

  ```
  %CPU_MONITOR-SP-3-TIMED_OUT: CPU_MONITOR messages have failed, resetting system
  (self) [5/0]
  ```

  Conditions: This symptom is observed on Cisco IOS 7600 series routers with either a single or dual RSP720 supervisor. In the case of dual supervisors, both supervisors crash. The cause of the crash is unknown. However, after the router reloads, the affected module has been installed again without further issue in a couple of instances.

  Workaround: There is no workaround.

- CSCtn19178

  Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working VRF “A” and a new local label will not be reassigned.

  Conditions: This symptom occurs on the MPLS Edge LSR when you remove the configuration of an unused VRF “B”, including:

  - The VRF interface, for example, **no interface Gi1/0/1.430**
  - The same VRF process, for example, **no router ospf** *process id* **vrf** *vrf name*

  Run the following commands to verify whether you are facing this issue:

  - **show ip bgp vpnv4 vrf A** *subnet* (this is for the working VRF)
  - **show mpls forwarding-table labels** *local label*

  Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using either of the following commands:

  - **clear ip bgp** *mp-bgp neighbor* **soft in**
  - **clear ip bgp** *mp-bgp neighbor* **soft out**

- CSCtn19444

  Symptoms: mLACP memberlinks may be bundled on an isolated PoA with a core failure, resulting in both PoAs becoming active.

  Conditions: This symptom occurs when running mLACP. The ICRM connection between the PoAs is lost. The PoAs are in a split brain situation and both PoAs attempt to become active. If the interface configured as “backbone interface” goes down on one of the PoAs, that PoA may keep the port-channel memberlinks bundled. The end result is that both PoAs are in mLACP active state, and both have their port-channel memberlinks bundled. After the fix the PoA with the backbone interface failure will unbundle its port-channel memberlinks, leaving only one PoA as active.

  Workaround: Configure shared control by configuring “lacp max-bundle” on the Dual Homed Device (DHD) if the device supports it. This would prevent the DHD from bundling the memberlinks to both PoAs at the same time.

- CSCtn37743

  Symptoms: Egress interface is not correct as observed by Mediatrace responder. This can impact monitoring on perf-traffic and system profiles.

  Conditions: This symptom is seen on a node where it has both initiator and responder. When the responder has both high and low cost routes and when the interface is changed, the change is detected, but the egress is not reflected.

  Workaround: Remove the original session and add it again.

- CSCtn38996

  Symptoms: All MVPN traffic is getting blackholed when peer is reachable using a TE Tunnel, and an interface flap is done so that secondary path can be selected. The multicast route does not contain a native path using the physical interface.

  Conditions: This symptom is seen when **mpls traffic-eng multicast-intact** is configured under OSPF.

  Workaround: Issue the **clear ip ospf process** command on the core router.

- CSCtn39632

  Symptoms: RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.

  Conditions: This occurs on a Cisco ASR 1000 series router configured for RSA key encryption with a keyring name having more than 8 characters.

  Workaround: Modify the keyring name to be less than 8 characters.

- CSCtn41653

  Symptoms: When a user attempts to configure CFMoXC dynamic sessions, the standby router will reload.

  Conditions: This symptom is seen when setting up CFMoXC PEI dynamic sessions. It is observed during a large number of dynamic sessions.

  Workaround: There is no workaround.

- CSCtn42601

  Symptoms: A Cisco router may unexpectedly reload when OSPF event debugging is enabled.

  Conditions: This symptom occurs under the following conditions:

  1. OSPF router configured to redistribute another protocol and redistribution is being controlled by a route-map.
  2. The **debug ip ospf events** command is enabled.

  Workaround: Do not reconfigure route maps while OSPF event debugging is on. Disable OSPF event debugging before making route-map configuration changes.

- CSCtn43223

  Symptoms: The idle timer is not working with traffic flowing with backup PW.

  Conditions: This symptom is seen when primary VC is down in PW redundancy setup.

  Workaround: There is no workaround.

- CSCtn45777

  Symptoms: Align messages are seen when enabling the **debug cwan atom** debug command.

Conditions: This symptom is observed when the **cwan atom** debug command is enabled. Spurious memory access messages are seen on the router console.

Workaround: There is no workaround.

- CSCtn46263

  Symptoms: Memory leaks are seen in ikev2_packet_enqueue and ikev2_hash.

  Conditions: This symptom is observed during retransmissions and window throttling of requests.

  Workaround: There is no workaround.

- CSCtn48744

  Symptoms: Memory leaks on OER border router while running PfR-IPSLA configuration.

  Conditions: This symptom is seen on a Cisco 7200 router that is running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCtn51058

  Symptoms: Traffic drops cause long multicast reconvergence times.

  Conditions: This symptom occurs when performing Stateful Switchover (SSO).

  Workaround: There is no workaround.

- CSCtn51740

  Symptoms: Memory leak is seen in EzVPN process.

  Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.

  Workaround: There is no workaround.

- CSCtn53094

  Symptoms: The router crashes or generates the following error:

  ```
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 8796350.
  -Process= "Mwheel Process", ipl= 2, pid= 315
  ```

  Conditions: This symptom is observed when toggling very fast between the **ip pim** *mode* and **no ip pim** commands on an interface when that interface is the only one where PIM is being enabled. The most common way this can happen in a production network is through the use of “config replace”, which results in the toggling of the command from ON to OFF and then ON on a different interface.

  Workaround: Avoid fast toggling of the **ip pim** *mode* command if possible when it is only present on a single interface.

- CSCtn53222

  Symptoms: The REALs are stuck in READY_TO_TEST state, and they never come to OPERATIONAL state. The only way to make them operational is to make them OUTOFSERVICE and INSERVICE again.

  Conditions: This symptom occurs when the REAL moves to FAILED state because of real failure that is detected by the inband failure mechanism. After the retry timeout, the REAL will be moved to READY_TO_TEST state.

  Workaround: There is no workaround.

- CSCtn54985

  Symptoms: The status of a LSP health monitor with LSP discovery is shown as unknown.

Conditions: This symptom is observed when PE routers in an MPLS VPN scenario are configured with LSP health monitors.

Workaround: There is no workaround.

- CSCtn55187

  Symptoms: Memory leaks are seen at ikev2_ipsec_add_proxy_to_list, ikev2_skeyseed_create, and ikev2_ios_get_ipv6_pak on the Cisco 2900 and Cisco 3900 platform routers respectively.

  Conditions: This symptom is seen after the test has been completed and while trying to check for the memory leaks when testing the Tunnel Protection for IPv6 feature.

  Workaround: There is no workaround.

- CSCtn59698

  Symptoms: When MLP bundle comes up on LNS with conditional debugging based on username enabled, certain attributes like IDB description and IP-VRF are not applied on the MLP bundle Virtual-Access.

  Conditions: This symptom is observed with the following conditions:

  1. Only for MLP sessions on LNS.
  2. When you configure per-user attributes in the user Radius profile such as “ip:vrf-id” and “ip:description”.
  3. When you bring up the session.
  4. When you run **show interfaces virtual-access** *intf* configuration for both the member-link VA and bundle VA.
  5. When the VRF and IDB description sent by Radius is applied only on member link VA and not on bundle VA.

  Workaround: Do not enable conditional debugs like **debug condition username** *user-name*.

- CSCtn61834

  Symptoms: NAT-T keepalive cannot send out cause NAT translation timeout.

  Conditions: This symptom is seen when the NAT translation table is getting timeout since no NAT keep alive message is received.

  Workaround: There is no workaround.

- CSCtn62250

  Symptoms: After upgrade on the Cisco 7600 router from Cisco IOS Release 12.2(33)SRD5 to Cisco IOS Release 12.2(33)SRE3, there may be a problem with pim mdt neighbors, which do not get brought up, though the configuration is not changed. Conditions: This symptom is observed after upgrade on the Cisco 7600 router from Cisco IOS Release 12.2(33)SRD5 to Cisco IOS Release 12.2(33)SRE3. Workaround: Remove/reinsert the **mdt default** command in ip vrf configuration mode.

- CSCtn64500

  Symptoms: Multicast traffic does not pass through an ATM point to a multipoint subinterface.

  Conditions: This issue is caused by an incomplete inject p2mp multicast adjacency on ATM P2MP interface. The output of the **show adjacency ATM interface detail** command shows that the Inject P2MP multicast adjacency is in incomplete state.

  Workaround: Run the **clear adjacency** command to force repopulating the incomplete adjacency. Note that you should be aware of the impact of this system-wide command. As an alternative, use unicast commutation if it is possible to do so.

- CSCtn73941

  Symptoms: After doing an OIR for an ES+ card having EVC configuration with the **module clear-config** command enabled, restoring the old configuration does not work anymore, indicating that traffic will not be forwarded over those service instances. The VLANS used in the previous config cannot be effectively used on those ports, not even by changing the service instance numbers. It is observed that the IOS still believes that the port is configured though there is no configuration yet.

```
Router#sh bridge-domain 10
Bridge-domain 10 (3 ports in all)
State: UP                    Mac learning: Enabled
    TenGigabitEthernet4/1 service instance 10

Router#sh run int ten4/1
Building configuration...

Current configuration : 64 bytes
!
interface TenGigabitEthernet4/1
 no ip address
 shutdown
end
```

  Conditions: This symptom occurs only with **module clear-config** configured.

  Workaround: There is no workaround. A complete reload would probably resolve this issue.

- CSCtn74169

  Symptoms: Crash by memory corruption occurs in the “EzVPN Web-intercept daemon” process

  Conditions: This symptom is observed when EzVPN server pushes a long banner to the client after HTTP authentication using HTTP intercept

  Workaround: Do not use long banner in HTTP intercept.

- CSCtn74673

  Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the CPU rate being high, the line cards are stuck in a continual loop of failing to complete MFIB download.

  Conditions: This symptom is observed when high CPU utilization is caused by multicast traffic and the **show mfib linecard** does not show cards in sync and tables are in “connecting” state. The **clear mfib linecard** command does not correct the line card table states.

  Workaround: There is no workaround other than line card reload.

- CSCtn80120

  Symptoms: VLAN translation in ES+ line cards is not working when ports are configured as Layer 2 switch ports (as in LAN cards).

  Conditions: This symptom is observed when you configure VLAN translation in ES+ line cards.

  Workaround: There is no workaround

- CSCtn80993

  Symptoms: An IOSD crash is found when doing two SPA IORs back-to-back on the same SPA.

Conditions: This symptom is observed on a router that has scaled L2VPN configuration, for example, Cisco 7000 EoMPLS, 1500 TE tunnels, 6000 EVCs, and 3000 L2TPv3 sessions. IOSD crash is seen consistently on the second SPA OIR when there is traffic through the sessions, and when the second SPA OIR is attempted immediately after the first SPA OIR of the same SPA.

Workaround: Once the SPA comes up after the first OIR, wait about one minute before issuing the second SPA OIR.

- CSCtn81186

  Symptoms: BFD hardware offload subsystem has some memory leaks in the error paths.

  Conditions: This symptom is seen when BFD sessions are offloaded to ES+ line cards in bulk and when some errors occur.

  Workaround: There is no workaround.

- CSCtn81231

  Symptoms: Multicast traffic is not forwarded out of the RBE interface due to incomplete multicast adjacency.

  Conditions: This symptom is seen on an ATM DCHP host that is running IGMPv2 is established over RBE interface to router. Multicast group join is successful. However, multicast adjacency is incomplete and therefore cannot forward multicast traffic.

  Workaround: Use the **shutdown** command followed by the **no shutdown** command on the ATM main interface.

- CSCtn87155

  Symptoms: CoA sessions are not coming up.

  Conditions: This symptom is observed when some CLI commands that are called within shell function might fail if the shell programmatic APIs are used.

  Workaround: Manually use shell functions on the console.

- CSCtn89179

  Symptoms: Output drops are observed when traffic is sent beyond 64k rate with single E1 when E1 is configured as unframed. Issue is seen rarely with using time-slots 1-31. After LC OIR, this symptom is not observed. If the channel is removed and attached, this issue reappears.

  Conditions: This symptom occurs on the following hardware and software:

  Hardware: SIP: 7600-SIP-400, SPA: 7/1 8xCHT1/E1 SPA

  Software: Cisco IOS 12.2(33)SRD or later releases, c7600rsp72043-adventerprisek9-mz.

  Workaround:

  1. Apply a service policy similar to below:

     ```
     policy-map test1
     class class-default
     queue-limit 496 --> (this number is a interface bandwidth(in kbps)*1000 / (8
     * 250 * 2) value for the correct behavior.)
     ```

  2. Or reload the line card.

- CSCtn93158

  Symptoms: When per flow load balancing is configured on a port-channel with EVC connect and Xconnect, sometimes egress traffic on EVC connect or Xconnect may get dropped.

Conditions: This symptom occurs when one of the port channel member links is shut.

Workaround: Use the **shutdown** command followed by the **no shutdown** command on the port channel.

- CSCtn95344

  Symptoms: After RPR downgrade from Cisco IOS Release 12.2(33)SRE2 to Cisco IOS Release 12.2(33)SRE1, the standby RSP gets stuck in cold bulk and reboots every 50 minutes.

  Conditions: This symptom occurs after RPR downgrade from Cisco IOS Release 12.2(33)SRE2 to Cisco IOS Release 12.2(33)SRE1.

  Workaround: Perform reload on the router.

- CSCtn98521

  Symptoms: After the CLI is enabled on ES+ for the control packets hitting on ES+ to not go into special queue, CLI does not reflect in the running configuration on RP sometimes.

  Conditions: This symptom occurs after enabling the **platform control- packet use-priority-q disable** command on ES+ for the control packets hitting on ES+ to not go into special queue. CLI does not reflect in the running configuration on RP.

  Workaround: There is no workaround.

- CSCtn98966

  Symptoms: In the following topology, the port-channel link on the standby PoA may forward packets unexpected to DHD. The issue is observed in both Cu's environment and the test lab:

```
Topology:
 ------------------POA-1(active)
|                          |
DHD                  |(L3  ICC link and L2 Trunk)
|                          |
 ------------------POA-2(standby)
```

  In Cu's environment: When DHD sends an arp request to ask for MAC of an HSRP virtual IP, it will receive the arp reply from the standby PoA, causing MAC flapping on DHD.

  In the lab test environment: When you configure static arp on PoAs to bind an IP address with a nonexistent MAC address, ping this IP, so it will do unicast flooding within vlan. When you ping, POA-2(standby) also sends out the unicast packet to DHD via its port-channel link.

  Conditions: This symptom occurs both on Cisco IOS Release 12.2(33)SRE2 and Cisco IOS Release 12.2(33)SRE3 with MLACP deployment.

  Workaround: There is no workaround.

- CSCto00318

  Symptoms: SSH session that is initiated from a router that is running Cisco IOS Release 15.x may cause the router to reboot.

  For now, consider not initiating a SSH session from the Cisco router that is running a Cisco IOS Release 15.x train.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.x.

  Workaround: There is no workaround.

- CSCto02448

  Symptoms: On doing an inbound route refresh, the AS-PATH attribute is lost.

Conditions: This symptom is observed with the following conditions:

1. The neighbor is configured with soft-reconfiguration inbound.
2. The inbound routemap is not configured for the neighbor
3. The non-routemap inbound policy (filter-list) allows the path.

Workaround: Instead of using the non-routemap inbound policy, use the routemap inbound policy to filter the prefixes.

- CSCto04593

  Symptoms: Statid leak in line card is observed while churning PPPoE sessions when using "show plat npc xlif 0 statid-usage". The statid leak results in high LC CPU, when it runs out of stat ids.

  Conditions: This symptom is seen only with scale.

  Workaround: There is no workaround.

- CSCto10958

  Symptoms: One of the OIFS starts dropping traffic in MLDP/LSM scenario.

  Conditions: This symptom is seen within MLDP/LSM configuration on a midpoint node or bud node.

  Workaround: Flap the interface where the OIF is going.

- CSCto11076

  Symptoms: Flood traffic does not work post TE FRR cutover for VPLS VCs.

  Conditions: This symptom is seen when VPLS VCs are going over TE/FRR and FRR cutover.

  Workaround: Have bidirectional traffic.

- CSCto13029

  Symptoms: When the Cisco 7600 router is running Cisco IOS Release 15.1(3)S, under rare conditions, the service instance configuration may not be downloaded to SP.

  Conditions: This symptom occurs if a large number of service instances are configured on the router.

  Workaround: There is no workaround.

- CSCto43154

  Symptoms: A Cisco device that is running Cisco IOS may reload unexpectedly with the following message:

  ```
  %SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count, chunk <address> data <address>
  refcount FFFFFFFF alloc pc <address>
  ```

  Conditions: This symptom is observed on Cisco device that is running Cisco IOS.

  Workaround: There is no workaround.

- CSCto44396

  Symptoms: If flow is learned as ip-cbr flow and later MDI metric configuration is added to the class-map, and when the flow is updated as MDI, the MDI metrics will not be updated to SNMP.

  Conditions: This symptom occurs only if the flow is learned as ip-cbr and then later updated as MDI flow also.

  Workaround: Removing and reattaching the policy-map.

- CSCto44585

  Symptoms: Packets with DF-bit set across the l2tpv3 tunnel are punted/dropped on the CPU.

Conditions: This symptom occurs when PMTU in pseudowire-class configuration is enabled.

Workaround: Reduce MTU on client side.

- CSCto47524

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs responder.

  A **show process memory sorted** command may initially show "MallocLite" growing. By disabling malloclite with the following:

  ```
  config t
  no memory lite
  end
  ```

  one may start to see process "IP SLAs Responder" growing. In at least one specific case, the leak rate was 80mb per day.

  Conditions: This symptom is observed on a Cisco ASR 1002 router.

  Workaround: Disable IP SLA on affected router, if possible.

- CSCto48592

  Symptoms: With IPFRR/MPLS-TE FRR enable, IOSd crashes during a switchover.

  Conditions: This symptom occurs under the following conditions:

  1. Enable IPFRR/MPLS-TE FRR
  2. . Enable BFD on the protected interface
  3. Switchover
  4. Independent with protocol being used, whether OSPF or ISIS

  Workaround: There is no workaround.

- CSCto50204

  Symptoms: Selective traffic denied by an inbound WCCP redirect list is being software switched due to incorrect TCAM programming. This issue is seen on the Cisco 7600/RSP720 that is running Cisco IOS Release 15.1(1)S1.

  Conditions: This symptom is seen under the following conditions:

  - WCCP redirect list should be applied inbound.
  - Only certain traffic may be software switched.
  - Cisco 7600/RSP720 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: There is no workaround.

- CSCto50255

  Symptoms: Memory leak occurs while running UDP echo operation.

  Conditions: This symptom is observed when an UDP echo operation successfully runs. Leak is seen on every 100th run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way is monitoring and decoding the PC via the **show processes memory** *pid* command.

  Workaround: There is no workaround.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

Conditions: This symptom is seen with GETVPN related configurations with fail-close feature activated.

Workaround: There is no workaround.

- CSCto64240

  Symptoms: Unable to configure port-channel access sub-interface with three memberlinks.

  Conditions: This symptom occurs when the port-channel has more than two members.

  Workaround: There is no workaround.

- CSCto70972

  Symptoms: Multicast traffic drops and does not reach the corresponding entries like (*,G/m) or (*,G).

  Conditions: This symptom occurs when multicast traffic drops and does not reach the corresponding entries like (*,G/m) or (*,G).

  Workaround: There is no workaround.

- CSCto80174

  Symptoms: A chunk memory leak may be observed when PTP configuration is applied, changed, or removed with multicast mode.

  Conditions: This symptom is occurs when the PTP clock configuration is on the Cisco 7600 router with spa-2x1GE-SYNC SPA.

  Workaround: There is no workaround.

  Further Problem Description: The chunk memory leak is observed when a few multicast related configurations of PTP are configured on the Cisco 7600 router.

- CSCto90096

  Symptoms: A router crashes while unconfiguring recovered clock configuration.

  Conditions: This symptom occurs when applying “no recovered-clock” to the router.

  Workaround: There is no workaround.

- CSCtq01136

  Symptoms: There is a ping failure over tunnel interface.

  Conditions: This symptom is seen during 6VPE basic configuration.

  Workaround: There is no workaround.

- CSCtq12230

  Symptoms: When overhead accounting command “hw-module slot 1 account np 0 out 4” is configured on the ES+ LC, show policy-map interface counters do not get updated.

  Conditions: This symptom is seen with QoS on any ES+ interface with overhead accounting feature enabled.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.1(2)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(2)S. All the caveats listed in this section are open in Cisco IOS Release 15.1(2)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCti92812

  Symptom: After physical interface flap, GRE tunnel for VRF does not come up correctly.

  Condition: This symptom occurs when GRE tunnel is configured for default (global) routing table.

  Workaround: There is no workaround.

- CSCtk97082

  Symptoms: IPv6 addresses are not cleared from an interface when **vrf forwarding** is applied for an IPv4-only VRF defined with the **vrf definition** command.

  Conditions: The following must be true:

  – The VRF is defined using the **vrf definition** command.
  – **address-family ipv4** is configured.
  – **address-family ipv6** is not configured.
  – An IPv6 address is present on the interface.
  – **vrf forwarding** is then configured on the interface.

  Under these conditions the IPv6 address will not be removed from the interface when **vrf forwarding** is applied.

  Workaround: Clear IPv6 addresses from the interface before applying **vrf forwarding**.

- CSCtk99836

  Symptoms: In scale environment with 4000 udp-jitter probes, responder crashes.

  Conditions: This symptom occurs when source starts running all 4000 probes with group schedule and aggressive frequency. Responder crashes.

  Workaround: There is no workaround.

- CSCtl44112

  Symptoms: MLS adjacencies for few labels are getting corrupted.

  Conditions: This symptom occurs during redundancy switchover.

  Workaround: Associated tunnel shut/no shut.

- CSCtl99266

  Symptoms: CoA service logon is not synced to standby.

  Conditions:

  – Do CoA service logoff of a service that was not installed via CoA service logon (i.e. installed through a rule or as an auto service). This gets synced to standby.
  – Do CoA service logon of the same service. This is not synced.

  Workaround:

  – After the CoA service logon is not synced, reboot the standby.
  – After the standby comes up, a bulk sync from the active is initiated, which will sync the service logon.

- CSCtn15317

  Symptoms: Traffic on MPLS VPN is dropped. When you check LFIB information on P router, you notice that entry has an instruction to TAG all packets that are destined to PE router instead of a POP instruction which is expected on a directly connected P.

  Conditions:

- ISIS protocol is running as IGP on MPLS infrastructure.
- ISIS on PE router is summarizing network that includes BGP VPNv4 update-source.
- P router is running MFI based image.

Workaround:

- Remove **summary-address** command in ISIS on PE.
- Change BGP update source.

- CSCtn19178

  Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, you may experience a situation where the local label for working VRF "A" clears and a new label never is reassigned.

  Conditions: To trigger this issue on the MPLS Edge LSR, remove the configuration of an unused VRF "B", this includes:

  - The vrf interface, for example "no int Gi1/0/1.430".
  - The same vrf process, for example "no router ospf *process id* vrf *vrf name.*

  Run the following command to verify if you are hitting this issue:

  - **sh ip bgp vpnv4 vrf A** *subnet*; this is for the working VRF.
  - **sh mpls forwarding-table labels** *local label*

  Workaround: To reprogram a new local label on the PE router you should clear the mp-bgp session:

  clear ip bgp *mp-bgp neigh* soft in, or **clear ip bgp** *mp-bgp neigh* soft out

- CSCtn26307

  Symptoms: In a scaled setup, a new subinterface will behave as expected during the first 20 minutes, and then will stop working.

  Conditions: This behavior is observed in a scaled setup after deleting and recreating subinterfaces. Though the sequence of commands to reproduce this is not yet clearly identified. It seems to be triggered by deleting interfaces and some timing issues. There should be a entry for the interface/vlan in the hidden vlans section of "show platform vlan". If that entry is missing, then this is probably the defect that is being encountered. There will probably be a entry in the recycled vlans for that interface instead.

  Workaround: Observe the output of "show platform vlan". In the recycled vlans section, those vlans should not stay there more than 20 minutes after a interface is deleted. If it does, then it might be possible to restore service, by following these steps:

  1. deleting the sub-interface that is having problems
  2. creating new temporary subinterfaces until the output of "show platform vlan" no longer has entries stuck in the recycled state.
  3. Add the sub-interface that was broken back into the configuration.
  4. . Observe the output of "show platform vlan" for 20 minutes to ensure that a entry stays in the hidden vlan section.
  5. Delete the temporary sub-interfaces.

  A reboot will also resolve this.

- CSCtn53834

  Symptom: When configuring HvPLS for a new circuit/VFI traffic does not pass. Mac addresses are not assigned to the VFI and traffic is blackholed.

Conditions: This symptom occurs on a Cisco 7600 series router with ES/ES+ module configured for HvPLS that is running Cisco IOS Releases SRD and SRE.

Workaround: Disable Mac Learning on the X-connect VLAN:

no mac address-table learning vlan *vlan-ID*

- CSCtn62287

  Symptoms: Standby router may crash while flapping the interface or while doing soft OIR of the SPA.

  Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flowing across the multilink.

  Workaround: No work around

- CSCtn67637

  Symptoms: Traffic is not forwarded out of DECAP PE for egress replication mode.

  Conditions: The ingtress LC on the DECAP PE must be a CFC LC like 6748/SIP400 and egress replication mode should be used on the DECAP PE in a mVPN setup.

  Workaround: Switch to ingress replication mode on the DECAP PE and the traffic starts flowing.

- CSCtn73941

  Symptoms: After doing an OIR for an ES+ card having EVC configuration with the **module clear-config** command enabled, putting back the old configuration does not work anymore, meaning the traffic will not be forwarded over those service instances. The VLANs used in the previous configuration cannot be effectively used on those ports, not even changing the service instance numbers. It looks like Cisco IOS still believes that port is configured though there is no configuration yet:

```
Router#sh bridge-domain 10
Bridge-domain 10 (3 ports in all)
State: UP                    Mac learning: Enabled
    TenGigabitEthernet4/1 service instance 10

Router#sh run int ten4/1
Building configuration...

Current configuration : 64 bytes
!
interface TenGigabitEthernet4/1
 no ip address
 shutdown
end
```

  Conditions: This symptom only happens with **module clear-config** configured.

  Workaround: There is no workaround.

- CSCtn80120

  Symptoms: VLAN translation in ES+ line cards is not working.

  Conditions: This symptom occurs when configuring VLAN translation in ES+ line card.

  Workaround: There is no workaround.

- CSCtn81231

  Symptoms: Multicast traffic is not forwarded out the RBE interface due to incomplete multicast adjacency.

Conditions: This symptom is seen when ATM DCHP host that is running IGMPv2 is established over RBE interface to router. Multicast group join is successful. However, multicast adjacency is incomplete and hence cannot forward multicast traffic.

Workaround: Shut/no shut the ATM main interface.

- CSCtn89179

  Symptoms: Output drops are observed when traffic is sent beyond 64k rate with single E1 when E1 is configured as unframed. Issue is seen rarely with using time-slots 1-31. After LC OIR, this symptom is not observed. If the channel is removed and attached, this issue reappears.

  Conditions: This symptom occurs on the following hardware and software:

  Hardware: SIP: 7600-SIP-400, SPA: 7/1 8xCHT1/E1 SPA S

  Software: Cisco IOS c7600rsp72043-adventerprisek9-mz.122-33.SRD or later.

  Workaround:

  1. Apply a service policy similar to below:

     policy-map test1
     class class-default
     queue-limit 496 --> (this number is a interface bandwidth (in kbps)*1000 / (8 * 250 * 2) value for the correct behavior.)

  2. Reload line card.

- CSCtn90664

  Symptoms: On a Cisco 7600 router which has globally configured **mls qos protocol arp police** *value* packets, which are received on an ES+ switchport/SVI interface, bypasses the policer and causes high CPU.

  Conditions: This symptom occurs when ES+ switchport/SVI interface with **mls qos protocol arp police <>** is enabled on the router.

  Workaround: Broadcast storm control could be used to rate-limit arp broadcast packets, or the following policy can be configured on the interfaces:

```
Policy-map ingress_policy-map
    Class cos0
      Set cos 0
    Class cos1
     Set cos 1
    Class cos2
       Set cos 2
    Class cos3
         Set cos 3
    Class cos4
      Set cos 4
    Class cos5
     Set cos 5
    Class cos6
       Set cos 6
    Class cos7
         Set cos 7



class-map cos0
   match cos 0
class-map cos1
   match cos 1
class-map cos2
```

```
   match cos 2
class-map cos3
   match cos 3
class-map cos4
   match cos 4
class-map cos5
   match cos 5
class-map cos6
   match cos 6
class-map cos7
   match cos 7
```

and then dscp-transparency is enabled using the CLI:

no mls qos ip rewrite dscp slot *module*

- CSCtn98966

  Symptoms: Topology:

  Topology:

  ----------POA-1(active)

  | |

  DHD |(L3 ICC link and L2 Trunk)

  | |

  ----------POA-2(standby)

  In the above topology, the port-channel link on standby POA may forward packets unexpected to DHD. The problem is observed at both the customer environment and test lab:

  In the customer environment: When DHD sends arp request to ask for MAC of a HSRP virtual IP, it will receive the arp reply from the standby POA, causing MAC flapping on DHD.

  In the lab test environment: Static arp is configured on POAs to bind an IP address with a non-existed MAC address, then ping this IP, so it will do unicast flooding within vlan. When doing the ping, it is observed that POA-2 (standby) also sends out the unicast packet to DHD via its port-channel link.

  Conditions: This problem happens both on Cisco IOS Releases SRE2 and SRE3 with MLACP deployment.

  Workaround: There is no workaround.

- CSCto04744

  Symptoms: A new subinterface will disappear from the list of the “sh platform vlan” hidden VLAN.

  Conditions: This behavior is observed in a scaled setup after a switchover. After deleting and recreating subinterfaces, there should be an entry for the interface/vlan in the hidden vlans section of “show platform vlan”, but that entry is missing. The steps to reproduce are not clearly identified but when the repro succeeds, the steps that lead to the issue are basically:

  1. A switchover.
  2. Removal of 4 subifs.
  3. Recreation of 2 subifs among the 4 removed in 2.
  4. The issue is triggered for one of the 2 recreated subifs.

  Workaround: There is no workaround except to delete the interface and to recreate a new one.

- CSCto15040

  Symptoms: When configuring a service-instance, the service instance may not be programmed properly on the Switch Processor leading to a loss of connectivity

  Conditions: This problem is observed when configuring the service instance under the physical interface of an ES+ card. You also need to run 12.2(33)SRE or above.

  Workaround: Configure the port in a channel-group and move the service instance configuration under the port-channel interface.

Resolved Caveats—Cisco IOS Release 15.1(2)S

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(2)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsh36203

  Symptoms: A Cisco router is crashing at p_dequeue.

  Conditions: This symptom is observed when testing the Echo cancelling feature in the Cisco 1700 platform but is not platform dependent.

  Workaround: There is no workaround.

- CSCsl18054

  Symptoms: A local user created with a one-time keyword is removed after unsuccessful login attempts. A one-time user should be removed automatically after the first successful login, not after failed logins.

  Symptoms: This symptom occurs on a router that is running Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCsm26063

  Symptoms: Router crashes following a **shut/no shut** on the main interface.

  Conditions: Occurs on a router running Cisco IOS Release 12.2SXH2a. IPv6 traffic must be flowing over the WAN interface for multiple IPv6 prefixes. The crash occurs when a **shut/no shut** is done on the main interface on which multiple subinterfaces have been configured and IPv6 routing is enabled.

  Workaround: There is no workaround.

- CSCsq02771

  Symptoms: DHCP relay may hang when request for IP address is received from a DHCP client on an unnumbered in an MPLS and VPN setup.

  Conditions: The symptom is observed on a Cisco 7200 router that is running Cisco IOS Interim Release 12.4(19.16)T1.

  Workaround: There is no workaround.

- CSCsv30540

  Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and a traceback are seen.

  Conditions: These symptoms are observed when the **show running-config/write memory** command is issued.

  Workaround: There is no workaround.

- CSCsv97424

  Symptoms: A router will reload due to memory corruption in the I/O pool. As an indication for this bug, we will see the same caller PC in the output of the show buffer pool Serial0/0/0 command.

  Conditions: This symptom is observed on Cisco routers that are running the adventerprisek9_ivs-mz feature set and when packets are being processed by an ATM interface.

  Frequency: Always.

  Workaround: We can overcome the reload issue by disabling hardware crypto using the following command in global configuration mode: “no crypto engine accelerator”.

  Note: When hardware crypto is turned off, encryption and de-cryption will be done by software and not by hardware. This can slightly hike CPU utilization, and this should not be an issue as long as we are not hit with pretty huge volume of traffic.

- CSCsy33068

  Symptoms: A big SDP HTML template causes an abrupt termination of the SDP process.

  Conditions: The HTTP post to the HTTP server in an IOS router is size-limited. The limit is set to 32KiB by default. In the SDP process, the transition from introduction page to the completion page involves an HTTP post. The post contains information including the SDP bootstrap configuration and the completion template together with the overhead of HTTP post communication. The size limit might be reached with moderate usage of HTML elements. The HTTP post in SDP is base-64 encoded. The total size limit of the SDP bootstrap and the completion template is roughly (32KiB - 2KiB(overhead)) * 3/4(base-64 encoding) = 22.5KB.

  Workaround: Reduce the size of the HTML template, and abridge the configuration. The total size of the two cannot exceed ~22.5KB. Example of abridged configuration:

  ```
  configure terminal => config t
  Interface FastEthernet 1 => int Fa 1
  ```

- CSCsy54233

  Symptoms: exception_reserve_memory is invalid in UNIX image.

  Conditions: UNIX images do not support exception_reserve_memory.

  Workaround: There is no workaround.

- CSCsy61302

  Symptoms: A chunk header corruption and a router crash with BADMAGIC error message is seen for either a free or in-use chunk.

  Conditions: The symptom is observed when the following SNMP commands are configured:

  snmp-server community public ro snmp-server packetsize 17940

  The crash is seen upon doing a **show run** and doing a grep for some keyword (e.g.: **show run | inc mem**). Memory checks need to be enabled. To see this issue reasonably fast, the interval of memory checks needs to be in the order of 3-4 seconds.

  Workaround: Do not configure “snmp-server packetsize more than 2048”.

  Further Problem Description: This crash is seen because of the snmp-server packetsize 17940. There is a local variable in one of SNMP functions with the configured packet size and when we run the CLI **show run**, the exec process stack overflows and corrupts the subsequent malloced block. This causes the memory corruption.

- CSCsy82679

  Symptoms: A Cisco IOS device may leak memory when using commands that generate a configuration.

  Conditions: This symptom occurs with the Embedded Event Manager version 3.1 where a policy description was introduced. If a policy description is applied to an applet, Cisco IOS will leak memory each time that the configuration is generated.

  Workaround: Do not use the policy description for applets.

- CSCsz18634

  Symptoms: An input/output rate is always displayed with “0” in interface status, even though packets are flowing on the ports normally.

```
show int gig 4/1 output
GigabitEthernet4/1 is up, line protocol is up (connected)
......
  Output queue: 0/40 (size/max)
  30 second input rate 0 bits/sec, 0 packets/sec  <<<<<<<<<<<
  30 second output rate 0 bits/sec, 0 packets/sec  <<<<<<<<<<<
     3411001 packets input, 567007874 bytes, 0 no buffer
     Received 818876 broadcasts (725328 multicasts)
```

  Conditions: This issue has been seen on a Cisco 3750 that is running Cisco IOS Release 12.2(46)SE, as well as a Cisco 4500 and Cisco 4900M that are running Cisco IOS Release 12.2(46)SG and Cisco IOS Release 12.2(53)SG1.

  Workaround: This issue is a cosmetic issue and does not affect the functionality of the switch or the traffic flow.

  Use the value of the **show int gigx/y count detail** command to see the raw statistics.

  The rate shown in the **sh int** command uses a complex convergence algorithm. If the rate changes from X to Y, it could take several minutes (15-30) for the rate to converge from X to Y. The rate must be steady and should be sent from a tester to confirm that the convergence is happening correctly.

  Or, execute reload.

  Further Problem Description: On the Cisco 3570 platform, the fix is in Cisco IOS Release 12.2(53)SE. On the Cisco 4500/4900M, the fix for this bug is scheduled to be in Cisco IOS Release 12.2(53)SG2 and Cisco IOS Release 12.2 (50)SG7.

- CSCsz35913

  Symptoms: Interface goes down in spite of carrier-delay configuration.

  Conditions: The symptom is observed on a PA-E3, when the serial interface carrier-delay is configured for one second and any of the alarms (AIS, LOF) are generated for less than or equal to one second.

  Workaround: Increase the carrier-delay.

- CSCsz90894

  Symptoms: L2 broadcast traffic can be leaked through blocked promiscuous port, which will cause SMAC to flap between the ports. As a result the return traffic to SMAC can get black hole until L2 forwarding is correct to show the right port.

  Conditions: This symptom will only happen multiple (at least two) L2 promiscuous ports are connected to other L2 switches, which participate in spanning tree.

  Workaround: Do not connect multiple L2 promiscuous port to other L2 devices in same VLAN.

- CSCta10402

  Symptoms: Continuous packet send by BFD causes a CPU hog.

  Conditions: The symptom is observed when BFD is enabled in the router.

  Workaround: Disable BFD.

- CSCta11223

  Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

  Conditions: This symptom is observed when the device is running Cisco IOS and configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

  Workaround: There is no known workaround.

- CSCta26520

  Symptoms: The following traceback is seen:

  ```
  %IDBINDEX_SYNC-3-IDBINDEX_LINK: Driver for IDB type 0 changed the Identity of
  interface "Tunnel1" without deleting the old Identity first
  ```

  Conditions: This symptom is observed when numerous tunnel interfaces are rapidly added and removed.

  Workaround: There is no workaround

- CSCta43825

  Symptoms: A CMTS walk of the ARP table causes high CPU usage. This symptom is also seen with an SNMP walk of the ARP table.

  Conditions: This symptom is observed in the Cisco IOS 12.2S train.

  Workaround: To prevent high CPU usage due to SNMP walk, implement SNMP view to prevent SNMP walk of the ARP table:

  ```
  snmp-server view cutdown iso included
  snmp-server view cutdown at excluded
  snmp-server view cutdown ip.21 excluded
  snmp-server community public view cutdown ro
  snmp-server community private view cutdown rw
  ```

  Further Problem Description: This symptom is widely observed in Cisco IOS 12.2S train since the arp redesign in 2004. It is not an efficient way to do next search/tree walk. When there are a lot of arp entries, the CPU utilization can reach as high as 99% when polling ipNetToMediaTable or atTable (they share the same logic).

- CSCta53372

  Symptoms: A VPN static route is not seen in the RIB after an interface is shut down and brought back up (shut/no shut).

  Conditions: Configure the crypto client and server routers in such a way that the session is up and RRI installs a static route on the server that is pointing to the client IP address. Now shut down the interface on the server router that is facing the client. The RRI static route disappears from the RIB and never reappears.

  Workaround: Reset the RRI session.

- CSCta78759

  Symptom: Traceback is seen in the new active when switchover is forced from RPR mode.

Conditions: This symptom is seen when the configured redundancy state is SSO and operational state is RPR due to image mismatch in active and standby.

Workaround: There is no workaround.

- CSCta79410

  Symptom: In a closed REP ring topology, where the uplink is VPLS using ES40 card, if one of the REP ports is Open and the other is Alt, then the convergence time is high when the Open port goes down.

  Conditions: The issue is only seen when the Alt port also resides on the same switch where there is a failure, and also if the Uplink happens to be VPLS.

  Workaround: There is no workaround. Reducing the number of VCs to 500 or less reduces the convergence time significantly. Moving the Alt port to some other device also reduces the convergence time significantly.

- CSCtb17152

  Symptoms: A large packet drop may occur when FRF.12 is enabled.

  Conditions: This symptom is observed when FRF.12 is enabled.

  Workaround: There is no workaround.

- CSCtb42862

  Symptoms: A Cisco 3845 router crashes due to illegal memory access.

  Conditions: The symptom is observed in a scale testing environment which has eight key servers and 20 GM routers (simulating 2000 group members) and when there is unicast rekeying. The GM router crashes in steady state (no traffic). This seems to be intermittent.

  Workaround: There is no workaround.

- CSCtb66391

  Symptoms: The following error message is displayed:

  ```
  Unable to operate on vc class. Possibly multiple users configuring IOS
  simultaneously.mapclass name class_vc1 process 374
  ```

  Conditions: This symptom happens when unconfiguring/reconfiguring scaling configuration with VC class.

  Workaround: There is no workaround.

- CSCtb87856

  Symptoms: Router can crash with a "%SYS-3-CPUHOG:" when DMVPN is deployed.

  Conditions: The symptom is observed when the physical interface (tunnel source) of the router is shut, the routing neighborship flaps, and memory consumption is increased to the point that there is no free memory left. This causes the router to crash.

  Workaround: There is no workaround.

- CSCtc27454

  Symptoms: A Cisco router may crash after displaying the following CPUHOG message for the Crypto ACL process:

  ```
  %%SYS-3-CPUHOG: Task is running for (xxxxx)msecs, more than (xxxx)msecs (xx/x),process
  = Crypto ACL.
  ```

  Conditions: This symptom is observed when the DMVPN tunnel is shut down.

  Workaround: There is no workaround.

- CSCtc33679

  Symptoms: Routes are not being controlled properly when PIRO is used.

  Conditions: If more than one exit per BR is configured and PIRO is used to control the routes, the nexthop is not being calculated correctly. As a result, traffic for these traffic classes is not taking the correct route.

  Workaround: There is no workaround.

- CSCtc54248

  Symptoms: CDP neighbors are not seen on subinterfaces.

  Conditions: This symptom is seen when CDP is enabled on subinterface and disabled on main interface.

  Workaround: There is no workaround.

- CSCtc73759

  Summary: The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml

- CSCtd10712

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtd16959

  Symptoms: Traceback is seen on SSO switchover.

  Conditions: This symptom is observed under the following conditions:

  - Configure CBTS master tunnel with 3 member tunnels
  - Delete all 3 member tunnels and then remove master command from master tunnel so it becomes regular TE tunnel
  - Configure auto-tunnel primary and backup setup
  - Make SSO switchover

  Many different tracebacks are seen on newly active RP, which are related to MPLS TE.

  Workaround: Do not delete CBTS Tunnels.

- CSCtd59027

  Symptoms: The device crashes due to a bus error.

Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

Workaround: There is no workaround.

- CSCtd78587

  Symptoms: A Cisco Catalyst 6000 switch running Cisco IOS Release 12.2SX software might crash under rare conditions when err-disable recovery tries to recover a port. The following messages are seen in the logs before the switch resets itself: %CPU_MONITOR-6-NOT_HEARD

  Conditions: This symptom may be observed after the following sequence of events:

  1. An interface on the switch gets err-disabled as expected due to a certain feature; for example, due to BPDU Guard
  2. Shortly after, before BPDU Guard err-disable recovery kicks in, the same port gets err-disabled for a different reason; for example, because a diagnostic error is detected on the already err-disabled port
  3. Err-disable recovery (BPDU Guard) tries to recover the port and this leads to the crash.

  Workaround: Disable err-disable recovery.

- CSCtd86472

  The Cisco IOS? Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  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_sep10.html

- CSCtd91542

  Symptoms: The **show ip multicast rpf tracked** command may cause a crash.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running all Cisco IOS 12.2(33) releases and after executing the **show ip multicast rpf tracked** command.

  Workaround: Avoid using the **show ip multicast rpf tracked** command.

  Further Problem Description: The command **show ip multicast rpf tracked** is not intended for customer use and is being deprecated.

- CSCtd94789

  Symptoms: IPSEC rekey fails after failover with stateful IPSEC HA in use.

  Conditions: The symptom is observed when using PFS and after a failover of the hub devices.

  Workaround: If the security policy allows, removing the PFS eliminates the issue.

- CSCtd95386

  Symptoms: An IPSec tunnel can be torn down if the router receives a replayed QM (Quick Mode) packet.

  Conditions: This is only a problem when a replayed QM packet is received on an IPSec endpoint.

  Workaround: There is no workaround.

- CSCte01606

  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/en/US/products/products_security_vulnerability_policy.html

- CSCte15193

  Symptoms: The **no spanning-tree vlan [vlanno]** command is not removed on standby alone.

  Conditions: The symptom is observed under the following conditions:

  - The **no spanning-tree vlan** *vlanno* command is configured first
  - The **default spanning-tree vlan** *vlan- range* command is entered next
  - The vlanno falls within the designated range, but the last vlan number in the range does not have "no spanning-tree vlan <>" configured for that.

  Workaround: Enter the **default spanning-tree vlan** *vlanno* command to remove it.

- CSCte56437

  Symptoms: NAT programming on a Cisco Catalyst 6500 may become corrupted; the source and/or destination IP addresses of traffic passing through the NAT box are changed to the wrong IP addresses.

  Conditions: This symptom is observed when the NAT configuration is changed during a high-volume traffic session.

  Workaround: There is no workaround.

- CSCte61528

  Symptoms: Router crashes when configuring "tftp hostname" with a longer name.

  Conditions: The symptom is observed with a Cisco 7200 series router loaded with the 151-0.25.T image.

  Workaround: There is no workaround.

- CSCte64621

  Symptoms: VSA stops passing traffic after the first IPSec rekey.

Conditions: The symptom is observed VSA specific.

Workaround: There is no workaround.

- CSCte65688

  Symptoms: Easy VPN server prints “Client_type=UNKNOWN” in “%CRYPTO-6-EZVPN_CONNECTION_UP: (Server)” log, when Software VPN Client establishes an IPSec session.

  Conditions: The symptom is observed when:

  – Easy VPN is configured between a Cisco VPN Client and a Cisco IOS router.

  – “crypto logging ezvpn” is configured.

  Workaround: There is no workaround.

  Further Problem Description: This is simply a cosmetic issue. Currently, this message can identify hardware VPN clients (IOS/PIX/VPN3002) only.

- CSCte68288

  Symptoms: Spurious memory access is seen when a set of configurations is placed under “crypto pki trustpoint *name*”.

  Conditions: The symptom is observed when the router is loaded with the c7200-adventerprisek9-mz.151-0.25.T image.

  Workaround: There is no workaround.

- CSCte77990

  Symptoms: QoS marking does not work.

  Conditions: The symptom is observed with the c7200-advipservicesk9-mz.122-33.SRE image.

  Workaround 1: Use an adventerprisek9 image instead of advipservicesk9 image.

  Workaround 2: Use policer with both confirm and exceed actions set to “mark” and “transmit”.

- CSCte78562

  Symptoms: Trying to run a regexp action on an undefined environment variable generates the following traceback:

  ```
  %SYS-2-FREEBAD: Attempted to free memory at 61, not part of buffer pool
  ```

  Conditions: This symptom is observed if an Embedded Event Manager applet tries to execute a regexp action on an undefined variable.

  Workaround: Trying to perform a regexp search on an undefined variable is not allowed. Make sure all arguments to the regexp action are properly defined.

- CSCte91471

  Symptoms: Clock synchronization with the NTP server could be lost for several hours if router (NTP client) runs NTPv4.

  Conditions: The symptom is observed if the router clock is reset (for example: by using the **clock set** exec command). The router then takes a long time to synchronize again.

  Workaround: There is no workaround. The clock will automatically synchronize after few hours.

- CSCte91782

  Symptoms: Cannot unconfigure “crypto pki server <>” when “crl” is configured.

  Conditions: The symptom is observed on a router loaded with Cisco IOS interim Release 15.1(1.1)T.

  Workaround: There is no workaround.

- CSCtf03436

  Symptoms: A two-level policy attached on a multilink interface is getting detached when the interface undergoes a shut/no shut.

  Conditions: The symptom is observed with a two-level policy configured with shaper/bandwidth percent. It is seen on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCtf23298

  Symptoms: There is high CPU usage when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Conditions: This symptom occurs when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Workaround: Remove single connection option.

- CSCtf36117

  Symptoms: Crash occurs when executing the **show crypto session brief** command with multiple IKEv2 tunnel connections.

  Conditions: The symptom is observed when setting up as many as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established and the command is trying to list down the sessions.

  Workaround: There is no workaround.

- CSCtf41721

  Symptoms: A DMVPNv6 hub might crash upon doing a shut/no-shut on the tunnel interface of the other hub.

  Conditions: The symptom is observed with the following steps:

  1. Configure DMVPNv6 with two hubs and two spokes.
  2. Hub 2 tunnel is shut and unshut.
  3. Hub 1 crashes.

  Workaround: There is no workaround.

- CSCtf48179

  Symptoms: When using an authentication header only (no encryption over the tunnel), a percentage of the outgoing traffic is dropped by the receiver due to incorrect IP header checksums. The percentage dropped depends on the traffic that is flowing over the tunnel.

  Conditions: This problem occurs only when the traffic mix over the tunnel includes both packets with the DF bit set and packets with the DF bit clear. When the DF bit setting differs between two subsequent packets, the second packet is sent with an incorrect IP header checksum.

  Workaround: There is no workaround.

- CSCtf50155

  Symptoms: Disable CDP on the L2 interface, which has a subinterface with VLAN encapsulation configured. CDP neighbors are not shown for the subinterface.

  Conditions: This symptom is observed when running Cisco IOS Release 12.2(33) SXI.

  Workaround: There is no workaround.

- CSCtf52106

  Symptoms: There is a failure of EEM TCL scripts when using the “exit_comb” keyword for the Interface Event Detector.

  Conditions: The symptom is observed when using the “exit_comb” keyword in an EEM TCL script.

  Workaround: There is no workaround.

- CSCtf53537

  Symptoms: Serial interfaces are messed up in second redundancy switchover.

  Conditions: This issue is seen upon second switchover in sb_throttles.

  Workaround: Issue, due to change in if_numbers of serial interfaces.

- CSCtf54561

  Symptoms: A MPLS TE FRR enabled router can encounter a crash if the **show ip cef vrf** *vrf-name* command is issued.

  Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

  Workaround: Command should not be issued when many topology changes occur on interface flaps.

- CSCtf56107

  Symptoms: A router processing a unknown notify message may run into a loop without relinquishing control, kicking off the watch dog timer and resulting in a software-based reload.

  Conditions: The symptom is observed when an unknown notify message is received.

  Workaround: There is no workaround.

- CSCtf57641

  Symptoms: A router crashes after performing a DNS lookup.

  Conditions: The symptom is observed when a command is used which sends out a DNS query such as **ping www.cisco.com** and the DNS server response contains a specially crafted packet.

  Workaround: Configure “no ip domain-lookup”.

- CSCtf65159

  Symptoms: While configuring empty default URL profile, we are seeing inconsistent memory access.

  Conditions: This symptom occurs while configuring empty default URL profile.

  None: There is no workaround.

- CSCtf70959

  Symptoms: EzVPN client is trying to negotiate the connection with a NULL address when the outside interface is a profile-based dialer interface.

  Conditions: This situation is a corner condition. The IP address on the dialer interface will be installed as soon as the dialer negotiation completes and the dialer interface comes up. But in this case, even though the IP address is not installed the dialer interface, the API is returning TRUE and proceeds further with the EzVPN connection.

  Workaround: Use a non profile-based dialer interface.

- CSCtf71010

  Symptoms: Traffic does not flow through the hub.

Conditions: The symptom is observed when a Cisco 3900 series router is configured for VRF-aware tunnel protection for IKEv2 sessions.

Workaround: There is no workaround.

- CSCtf71990

  Symptoms: An alert message is not sent if “source-ip-address” is configured in the call-home configuration. The following message is shown:

  ```
  %CALL_HOME-3-SMTP_SEND_FAILED: Unable to send notification using all SMTP servers (ERR
  7, error in connecting to SMTP server)
  ```

  Conditions: The symptom is observed when “source-ip-address” is configured.

  Workaround: Remove “source-ip-address”.

- CSCtf72328

  Symptoms: BFD IPv4 Static does not fully support AdminDown.

  Conditions: The symptom is observed with the following setup and configuration:

  ```
  Router 1:
  interface e0/0
  ip address 192.168.1.1 255.255.255.0
  bfd interval 51 min_rx 51 multiplier 4
  bfd echo
  no shut
  exit

  interface loopback 0
  ip address 10.10.1.1 255.255.0.0
  exit
  ip route static bfd e0/0 192.168.1.2
  ip route  10.20.0.0 255.255.0.0 e0/0 192.168.1.2

  Router 2:
  interface e0/0
  ip address 192.168.1.2 255.255.255.0
  bfd interval 51 min_rx 51 multiplier 4
  bfd echo
  no shut
  exit

  interface loopback 0
  ip address 10.20.1.1 255.255.0.0
  exit

  ip route static bfd e0/0 192.168.1.1
  ip route  10.10.0.0 255.255.0.0 e0/0 192.168.1.1

  interface e0/0
  no ip route static bfd e0/0 192.168.1.1
  ```

  Though the BFD state is DOWN the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

  Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtf79264

  Symptoms: A Cisco route processor (RP) loses part of its odr-route for the spoke network. With a busy network, and with more than 1000 spokes, the second RP can have the same symptom.

  Conditions: This symptom is observed with a default odr timer.

Workaround: Modifying the odr timer can help, but will not solve the problem.

- CSCtf87039

  Symptoms: Device crashes at crypto_ikmp_process_xauth_reply.

  Conditions: The symptom could occur while processing the xauth response received from the client. The PPC platform crashes (the MIPS64 platform does not crash).

  Workaround: There is no workaround.

- CSCtf95308

  Symptoms: Router crashes on modifying the radius profile and including unexpected values in it, such as empty strings and strings with special characters.

  Conditions: This symptom is seen during an active ISG with sessions coming up and going down.

  Workaround: Avoid changing the radius profile values with active sessions.

- CSCtg08496

  Symptoms: After merge, keyserver deletes all GMs so the rekey fails to be sent (DB is empty) and all the GMs need to re-register.

  Conditions: The symptom is observed when running Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtg13269

  Symptoms: On peers of Route Reflectors (RR), the received prefixes counter shows an incorrect number when session flaps occur during a network churn.

  Conditions: The symptom is observed with BGP RRs.

  Workaround: Use the **clear ip bgp *** command.

- CSCtg18555

  Symptoms: A memory leak is observed with process_online_diag_pak.

  Conditions: This symptom is observed on a card supporting TestNonDisruptiveLoopback and TestFabricChHealth tests.

  Workaround: Disable the HM tests TestNonDisruptiveLoopback and TestFabricChHealth on line cards to stop the leak.

- CSCtg19546

  Symptoms: MPLS forwarding of labeled frames across a tunnel may fail. This symptom arises when an incorrect TAG adjacency is created for the tunnel.

  Conditions: This symptom is observed when adding or removing crypto and a tunnel protection configuration from a tunnel interface also configured with MPLS. When this symptom occurs, an incorrect or missing IPSec post encap feature is observed under the TAG adjacency for the tunnel.

  Workaround: Removing the crypto and/or removing and reconfiguring mpls ip from the tunnel can recover connectivity.

  Alternate Workaround: VTI cannot be combined with MPLS label switching, since IPSec can only encapsulate IP packets, not MPLS packets. This is due to design. In GRE mode, however, this is possible, so use a GRE tunnel with IPSec tunnel protection along with MPLS label switching. Be sure to remove and reapply the “tunnel protection ipsec profile” configuration so that IPSec features will be properly applied to the IP-and MPLS-switching feature paths.

- CSCtg22080

  Symptoms: Memory leak occurs at crypto_ca_cert_hexmode_quit_function.

Conditions: This symptom occurs at crypto_ca_cert_hexmode_quit_function.

Workaround: There is no workaround.

- CSCtg22674

  Symptoms: The router experiences high CPU for several minutes due to “MPLS TE LM” process.

  Conditions: This symptom occurs when a router has many (perhaps as few as 100) MPLS TE tunnels that traverse over a link which experiences repeated flapping in a short duration.

  Workaround: There is no workaround.

  Further Problem Description: Use the command **show process cpu** to determine CPU utilization. If this problem exists, the MPLS TE LM process holds greater than 90% resources for 5 minutes or more.

```
CPU utilization for five seconds: 100%/0%; one minute: 100%; five minutes:
100%
   PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   216   867694836  18357673      47266 99.67% 99.09% 99.11%   0 MPLS TE LM
```

- CSCtg26538

  Symptoms: After applying a CoPP policy, any traffic that would arrive at the CPU with an MPLS label is not classified and is classified in the class-default.

  Conditions: This will be seen for any traffic arriving at the CPU with a MPLS label. The easiest manifestation of this would be to use a loopback in a VRF for management. Any traffic destined to or sourced from that loopback interface will not match the expected CoPP policy classification. For example:

```
interface loopback0
ip vrf forwarding red
ip address 192.168.1.1 255.255.255.255
!
access-list 101 permit ip any host 192.168.1.1
!
class-map  loopback-traffic
 match access-group 101
!
policy-map loopback-copp
 class loopback-traffic
  police 8000
!
control-plane
 service-policy in loopback-copp
```

  Any traffic destined to the loopback0 interface will be classified in *class-default* class.

  Workaround: There is no workaround

- CSCtg28806

  Symptoms: Router crashes at PKI manual enroll.

  Conditions: The symptom is observed on a Cisco 2921 router that is running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- CSCtg41606

  Symptoms: With Reverse Route Injection (RRI) configured with the **reverse-route** command, if the crypto map is applied to a multi-access interface (e.g.: ethernet) then egress traffic may fail when the router cannot populate an ARP entry for the crypto peer address.

Conditions: The symptom could occur when the upstream device does not support proxy arping.

Workaround: Use the **reverse-route remote-peer** *next-hop-ip* command instead of just **reverse-route**.

- CSCtg41733

  Symptoms: Certain crafted packets may cause a memory leak in the device in very rare circumstances.

  Conditions: This symptom is observed on a Cisco IOS router configured for SIP processing.

  Workaround: Disable SIP if it is not needed. To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy infrastructure access control lists (iACLs) to perform policy enforcement of traffic sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For the maximum protection of infrastructure devices, deployed iACLs should be applied in the ingress direction on all interfaces to which an IP address has been configured. An iACL workaround cannot provide complete protection against these vulnerabilities when the attack originates from a trusted source address.

  The iACL policy denies unauthorized SIP packets on TCP port 5060 and 5061 and UDP port 5060 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

  Additional information about iACLs is in Protecting Your Core: Infrastructure Protection Access Control Lists.

```
ip access-list extended Infrastructure-ACL-Policy

     !
      !-- Include explicit permit statements for trusted sources
      !-- that require access on the vulnerable protocols and ports
      !
      permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
      permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
      permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060

      !
      !-- The following vulnerability-specific access control entries
      !-- (ACEs) can aid in identification of attacks
      !

      deny tcp any 192.168.60.0 0.0.0.255 eq 1720
      deny tcp any 192.168.60.0 0.0.0.255 eq 5060
      deny tcp any 192.168.60.0 0.0.0.255 eq 5061
      deny udp any 192.168.60.0 0.0.0.255 eq 5060

      !
      !-- Explicit deny ACE for traffic sent to addresses configured within
      !-- the infrastructure address space
      !

      deny ip any 192.168.60.0 0.0.0.255

     !
      !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
      !-- with existing security policies and configurations
```

```
 !
 !-- Apply iACL to interfaces in the ingress direction
 !

interface GigabitEthernet0/0
 ip access-group Infrastructure-ACL-Policy in
```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages could have the undesired effect of increasing CPU utilization on the device. In Cisco IOS Software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command no ip unreachables. ICMP unreachable rate limiting can be changed from the default using the global configuration command ip icmp rate-limit unreachable interval-in-ms.

More information about how to detect and mitigate this type of issues can be found at the Cisco Applied Mitigation Bulletin: "Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Voice Products" at the following link:

http://www.cisco.com/warp/public/707/cisco-amb-20100922-voice.shtml

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-2010-4683 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/en/US/products/products_security_vulnerability_policy.html

- CSCtg42904

  Symptoms: Router crashes with the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address after applying the flow monitor to
  virtual-template interface
  ```

  Conditions The symptom is observed on a router configured with EasyVPN.

  Workaround: There is no workaround.

- CSCtg44108

  Symptoms: Bus error crashes occur frequently.

  Conditions: This symptom is observed on a Cisco 3945e Integrated Services Router (ISR) that is running Cisco IOS Release 15.1(1)T. IPSec is configured on a GRE multipoint tunnel interface.

  Workaround: There is no workaround.

- CSCtg49109

  Symptom: After a switchover, some of the modules go to MajFail state.

  Conditions: This issue is observed when high traffic is triggered, a lot of packets are dropped by the platform, and numerous IPC messages time out.

  Workaround: There is no workaround.

  Further Problem Description: Due to some unexpected events, one of the IPCs boolean "IPC message blocked" is failing to get set (that is, failing to get unblocked), which is in turn blocking the ICC process from processing further messages. This results in the failure.

- CSCtg49331

  Symptoms: Multicast streams may not be forwarded to some interfaces, even though they are forwarded to other interfaces on the device without issues.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD4 with egress multicast replication mode.

  Workaround: Use ingress replication mode. If egress replication mode is used and the issue is present, service can be restored by using this command:

  clear ip mroute *A.B.C.D*

  Or perform a shut/no shut on the affected interface.

- CSCtg50024

  Symptoms: A router experiences crashes due to TLB (load or instruction fetch) exception.

  Conditions: This problem is observed on a Cisco 7206VXR router with Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtg52885

  Symptoms: The HSRP state on dot1q sub-interfaces remain in INIT state.

  Conditions: This symptom is observed after a physical link flap on a trunk port.

  Workaround: Perform a shut/no shut on the interface.

- CSCtg53953

  Symptoms: A standby router reloads due to a parser sync issue when applying certain neighbor commands (neighbor *ip-address* disable-connected-check, neighbor *ip-address* peer-group pgrp, and others).

  Conditions: This symptom applies only to situations where *ip-address* is the IP address of a peer that has a dynamically created session (a neighborship that is the result of the “bgp listen range ...” feature).

  Workaround: There is no workaround. Such a configuration should not be applied in the first place.

- CSCtg55338

  Symptoms: If a router is reloaded with a GRE tunnel interface configured with tunnel protection and a dialer interface as the tunnel source, the crypto socket is not created and IPSec is not triggered.

  Conditions: This symptom is observed on a Cisco router with a GRE tunnel interface configured with tunnel protection and a dialer interface as the tunnel source.

  Workaround: After the reload, remove and reapply the tunnel protection on each tunnel interface.

- CSCtg55447

  Symptoms: GETVPN keyserver TEK sequence number goes out of sync during network split/KS failure. This causes the GM to reject the older key and reregister.

  Conditions: This symptom is seen during primary keyserver failure or network failure between primary keyserver and secondary keyserver.

  Workaround: There is no workaround.

- CSCtg57831

  Symptoms: In the event of a failover, there is a serial number mismatch on the active and standby.

Conditions: The symptom is observed in an High Availability CA servers environment, using Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCtg58786

  Symptoms: When an external interface on the BR is shut down, the BR could be crashed.

  Conditions: If more than one thousand Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down, this could result in a crash.

  Workaround: There is no workaround.

- CSCtg59328

  Symptoms: When IPCP renegotiates for an existing PPPoE session, the new IPv4 address does not get synced up with the standby.

  Conditions: This symptom is observed when the following tasks are completed:

  – Bring up a PPPoE session and ensure that it is synced to standby.
  – From the PPPoE client run the commands **no ip address** followed by **ip address negotiated** under the Virtual- template interface.
  – As part of the **no ip address** command, the session would first go down on both active and standby. The **ip address negotiated** command would then trigger IPCP re-negotiation and the session would come up on active. On standby, the session remains down and the new IP address is not synced.

  Workaround: There is no workaround.

- CSCtg60302

  Symptoms: CPP ucode crashes after shutting down mpls-te tunnel interfaces.

  ixia ------PE1 ------------PE2 --------------ixia

  This is a 6PE topology with an MPLS TE tunnel between PE1 and PE2 and traffic passing through the TE tunnel. When the TE is shut down, the CPP crashes.

  Conditions: This symptom is observed when the traffic rate is about 500 packets per second.

  Workaround: There is no workaround.

- CSCtg64175

  Symptoms: The ISIS route is missing the P2P link, it is mistakenly marked as “parallel p2p adjacency suppressed”.

  Conditions: The symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

  Workaround: Do a **shut** and **no shut** on the local P2P interface.

- CSCtg73798

  Symptoms: After one or more line card resets or online insertion/removals (OIRs), an MPLS xconnect virtual circuit may come up but reports a TX fault to the LDP peer.

  Conditions: The symptom may occur on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRE or later, Release 12.2(33)XNC or later, or Release 15.0(1)S or later.

  Workaround: Remove and reapply the relevant xconnect configuration.

- CSCtg75452

  Symptoms: RP crashes in dual RP system after doing a **config replace** on POS-configured SDH link.

  Conditions: The symptom is observed if you configure a POS SDH link on a 1XCHSTMOC12/DS0 SPA port and do a **config replace** to a basic router configuration that includes redundancy mode change. This crashes the RP and produces a core file.

  Workaround: There is no workaround.

- CSCtg79262

  Symptoms: A Cisco IOS Embedded Event Manager (EEM) Tool Command Language (Tcl) policy can get stuck in the EEM active scheduler queue. The policy will consume a scheduler thread and cannot be cleared automatically by the maxrun timer or manually using the EEM exec command **event manager scheduler clear all**.

  Conditions: This symptom occurs in very rare circumstances. For example, if the system has enough memory to schedule and start running the EEM policy, but the policy fails due to a lack of memory.

  Workaround: The only way to recover is to reload.

- CSCtg89960

  Symptoms: "no ipv6 spd queue max-threshold *spd value*" causes standby to reload.

  Conditions: This symptom occurs Cisco IOS c7600 router having dual RP and running c7600s72033-adventerprisek9-mz.150-0.12.S image.

  Workaround: There is no work around.

- CSCtg92587

  Symptoms: High CPU in the SNMP Engine process is observed every five minutes.

  Conditions: This symptom occurs when SNMP queries are performed on TE MIB with hundreds of TE tunnels configured.

  Workaround: There is no workaround.

- CSCtg93243

  Symptoms: QoS + tunnel protection does not work if UUT2 is running VSA. Packets get dropped at UUT2 after being decrypted by VSA.

  Conditions: The symptom is observed with crypto, tunnel protection, and VSA only. (If static crypto + VSA, or tunnel protection + SW crypto is used packets get forwarded after decryption as expected.)

  Workaround: There is no workaround.

- CSCtg95940

  Symptoms: The DH operation will fail and no further IKEv2 SAs will come up.

  Conditions: This issue can occur with many IKEv2 requests coming at once and when you are using hardware crypto-engine.

  Workaround: There is no workaround.

  Further Problem Description: You can re-start the router and switch to software-crypto engine if needed.

- CSCtg98116

  Symptoms: An ES-20 crashes on performing a **config copy** from startup-config to running-config.

  Conditions: The symptom is observed with a 4k EVC and QoS policy attached to the EVC when a **config copy** is performed from startup-config to running-config.

Workaround: There is no workaround.

Further Problem Description: ES-20 recovers and works fine after the crash.

- CSCth00317

  Symptoms: When a large number of service groups are configured with multiple service instances on a port-channel, the following anomaly is observed: on addition of a new member-link, not all the policies applied to the port- channel will be configured in the line card.

  Conditions: The symptom is observed upon adding a new member-link (having large policies) to the EVC port-channel.

  Workaround 1: Do a shut/no-shut of the member link.

  Workaround 2: Reset the line card on configuration of the port-channel.

- CSCth02812

  Symptoms: A prolonged unicast flood can be seen on an ingress path after a TCN event. The flood will last until entries in the arp table are refreshed.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SXH3a (issue has been tracked back to Cisco IOS Release 12.2(18)SXF in an L2 asymmetric environment. The flood is only seen if there is no bi-directional flow on the switch. This issue can be seen in all STP modes.

  Workaround: Clearing ip arp will correct this issue. Lowering the arp timeout will also minimize the impact of the flood.

- CSCth03022

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- CSCth05476

  Symptoms: On router bootup, the SIP200 line card is flooded with “%CWSLC-3- DIAGFAIL: Failed to handle diag” messages.

  Conditions: The symptom is observed on a Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCth08962

  Symptoms: A single bit error in the SRAM of the ATM SPA will generate the following error message:

  ```
  EST5EDT,M3.2.0/: spa_atm_v2[241]: SPA ATM4/2 SAR: An error was reported by SAR
  firmware (unsolicited msg): Description: Single-bit SRAM ECC correctable error. [Error
  code 4]
  ```

  It does not cause an operation impact, but the error message will repeat every 6 seconds.

  Single bit correctable errors should be counted but not display an error message since the information is already corrected by parity. Also the rate of these messages may increase during certain conditions, which may choke the queues on the platform.

Conditions: This symptom occurs under normal operating conditions.

Workaround: There is no workaround.

- CSCth09876

  Symptoms: Cisco IOS IP Service Level Agreements (SLAs) cannot be auto- discovered if IP SLAs are removed from the responder first.

  Conditions: This symptom is observed on a Cisco device after IP SLAs have been unconfigured. Subsequent attempts to reconfigure the device as an IP SLAs responder fail.

  Workaround: Reload the router and configure the device as an IP SLAs responder.

- CSCth13415

  Symptoms: One way audio in call transfer due to 491 response during resume re- INV.

  Conditions: The symptom is observed when you have an UPDATE message passing through the CUBE and then a re-INV crossover happens. The re-INV crossover results in a 491 but the 491 is not correctly forwarded by the IPIP GW. This can result in one way audio issues if the crossed over re-INV was changing the media state from hold to resume.

  Workaround: There is no workaround.

- CSCth14305

  Symptoms: Having a bandwidth statement on a multilink bundle interface will cause problems with QoS and BQS if linkmembers flap as the changes in bandwidth will not be handled correctly.

  Conditions: The symptom is observed when you have a bandwidth statement on a multilink bundle.

  Workaround: Avoid bandwidth statements on multilink bundle interfaces.

- CSCth15105

  Symptoms: BFD sessions flap after unplanned SSO (test crash).

  Conditions: The symptom is observed on a UUT up with unicast/multicast along with BGP and BFD configurations. For BFD timers of 1*5, 500*8, after doing a test crash (option C followed by 6), we see BFD sessions flap.

  Workaround: There is no workaround.

- CSCth16011

  Symptoms: After a network event is introduced in the network, such as a 3- percent loss, MOS policy will detect the OOP condition. But PfR will let the prefix stay in the OOP condition for some time and then switch over to an alternative exit.

  Conditions: Introduce loss to network.

  Workaround: There is no workaround.

- CSCth16962

  Symptoms: Primary KS KEK timer gets stuck or reset to zero after a GDOI policy change and rekey. Once the KEK timer gets stuck/reset to zero, there are repeated rekeys, which will impact the whole GET VPN domain. The trigger occurs after a failure event in the primary key server and the secondary key server becomes primary followed by a policy change.

  Conditions: This symptom occurs when KEK timer gets stuck at Zero and there are repeated rekeys to GMs resulting a rekey storm.

  Workaround: There is no workaround.

- CSCth19516

  Symptoms: A router crashes if you have PFR and SAF enabled on the same device.

Conditions: The issue is seen when you have SAF enabled and PFR with multiple links. When the network gets congested or delay is seen and if there is a change over from IN-POLICY state to OOP the router crashes.

Workaround: Disable SAF completely and reload the router.

- CSCth23814

  Symptoms: When using Flexible NetFlow, a traceback or crash can occur.

  Conditions: This symptom is observed when a monitor is configured with a flow record that has the "BGP next hop" field configured.

  Workaround: Ensure that the "BGP next hop" field is not configured for a flow.

- CSCth24984

  Symptoms: High CPU usage is seen when the RP is working as a DMVPN hub.

  Conditions: The symptom is observed when there is 1000 static BGP neighbors (spokes) over MVPN.

  Workaround: There is no workaround.

- CSCth25634

  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.

- CSCth33949

  Symptoms: An LNS standby crashes when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the command **clear ppp all**.

  Conditions: This symptom is observed when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the command **clear ppp all**.

  Workaround: Use the **cle vpdn tunnel l2tp all** command instead.

- CSCth35515

  Symptoms: Line card crash could occur on an SSO when a router runs MPLS.

  Conditions: This symptom may occur when multiple back to back switchovers occur.

  Workaround: There is no workaround.

- CSCth36114

  Symptoms: A crash is seen after executing the **write memory** command via SDM.

Conditions: The symptom is observed on a Cisco 1841 platform that is running Cisco IOS Release 15.1(1)T.

Workaround: Use Cisco IOS 12.4 versions.

- CSCth37092

  Symptoms: A crash is observed in the PKI-HA feature when the standby tries to sync up with the active router.

  Conditions: When the PKI server is created on the active router with a “database archive password” configuration, the PKI server is cloned on the standby. Soon after, the active router crashes.

  Workaround: There is no workaround.

- CSCth37580

  Symptoms: Dampening route is present even after removing “bgp dampening”.

  Conditions: The symptom is observed under the following conditions:

  – DUT connects to RTRA with eBGP + VPNv4. - eBGP + VPNv4 peer session is established and DUT.
  – Also DUT has VRF (same RD) as route advertised by RTRA.

  In this scenario, when DUT learns the route it will do same RD import and the net’s topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

  Workaround: There is no workaround.

- CSCth40213

  Symptom: More than one preshared key for address 0.0.0.0 may not be configurable in different keyrings.

  Conditions: Multiple preshared keys cannot be configured for address 0.0.0.0 in different keyrings.

  Workaround: There is no workaround.

- CSCth41801

  Symptoms: Flows get stuck in LC, even though the RP flow times out and the HPLA flows are removed. If we have reached the LC flow limit when this happens, new flows may not be learnt even though the number of active flows in the system is less than the LC scale value.

  Conditions: This symptom is observed when the hardware timeout value is greater then the software timeout value. In this case, the code ignores the event from RP and does not delete the count from the LC table. In such a scenario, if the LC flow limit has been reached, new flows would not be learnt even though existing flows get timed out.

  Workaround: The only workaround in such a situation is LC OIR, which may not be acceptable. This issue can be avoided if the HW timeout value is less than the SW timeout value.

- CSCth42798

  Symptoms: In a very corner case, when BGP is in read-only mode and attributes are deleted before the networks, memory can be corrupted.

  Conditions: The device should be in read-only mode, and attributes should be deleted before networks.

  Workaround: There is no workaround.

- CSCth55579

  Symptoms: Router reloads at clean_out_RA_certs after enrolment with CA server.

  Conditions: The symptom is observed after enrolment with CA server.

Workaround: There is no workaround.

- CSCth60232

  Symptoms: The port-channel interface may flap when adding or removing a VLAN from the trunk on a port-channel interface when one or more interfaces are in a state other than P or D.

  Conditions: This symptom is observed only when the port-channel interface has interfaces in states other than P or D.

  Workaround: Shut down the non-P members and make the vlan changes.

- CSCth61759

  Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate the video stream.

  Conditions: This symptom is observed in two scenarios:

  Scenario 1: This symptom was observed in the following SIP-SIP Delayed Offer - Delayed Offer (DO-DO) call flow:

  ```
  7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server
  ```

  1. Call is originated by 7985
  2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP “200 OK” response

     m=video 53722 RTP/AVP 96 97 34 31

     b=AS:1920

     a=rtpmap:96 H264/90000

     a=fmtp:96 profile-level-id=42e016;max-mbps=108000;max-fs=3600

     a=rtpmap:97 H263-1998/90000

     a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1

     a=rtpmap:34 H263/90000

     a=fmtp:34 CIF4=1;CIF=1;CIF=1;QCIF=1

     a=rtpmap:31 H261/90000

     a=fmtp:31 CIF=1;QCIF=1

     a=sendrecv
  3. CUBE sets video m-line to 0 in the SDP of the SIP “ACK” response

     m=video 0 RTP/AVP 96

  Scenario 2: End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).

  CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA

  Workaround: There is no workaround.

- CSCth64271

  Symptoms: Routers in redundant configuration end up in Manual Swact = disabled.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCth64316

  Symptoms: Unable to configure “radius-server” using SNMP set.

  Conditions: The symptom is observed when you configure via SNMP MIB.

Workaround: Radius server can be configured through the CLI.

- CSCth66177

  Symptoms: The standby route processor (RP) triggers an active RP crash.

  Conditions: This problem is observed when the standby RP crashes due to a memory parity error.

  Workaround: There is no workaround.

- CSCth66604

  Symptoms: ISSU incompatibility due to different versions of a protocol (NTP v3 and NTP v4).

  Conditions: The symptom is observed with an ISSU upgrade or downgrade.

  Workaround: Unconfigure the CLIs causing MCL errors and repeat the ISSU process again.

- CSCth67788

  Symptoms: sVTI stops forwarding traffic when a local policy is configured on a device.

  Conditions: The symptom has been observed on a router that is running Cisco IOS Release 15.0(1)M1.

  Workaround 1: Do not use a local policy.

  Workaround 2: Configure “no ip route-cache cef” on the tunnel interface.

- CSCth69364

  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://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml.

- CSCth70437

  Symptoms: Crypto sessions drop after the following error message:

```
000059: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=83D91910, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
0x8039460Cz 0x80397B40z
000060: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=83D91CE4, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
0x8039460Cz 0x80397B40z
000061: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=83D920B8, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
0x8039460Cz 0x80397B40z
000062: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=83D82F8C, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
0x8039460Cz 0x80397B40z
```

  Conditions: This symptom is observed on Cisco IOS 8XX series routers and when crypto is applied to dialer interface.

  Workaround: There is no workaround.

- CSCth71349

  Symptoms: Some SSS sessions are staying in “attempting” state for a while when using ISG Static Session Creation.

  Conditions: The symptom is observed when using ISG Static Session Creation.

  Workaround: Stop incoming traffic from subscribers and wait until the sessions recover, then re-apply the traffic.

- CSCth74953

  Symptoms: The SPI value is shown as 0x0, hence the ipsec sa validation is failing.

  Conditions: This symptom is observed when the crypto profiles are being applied. The symptom is not observed with simple crypto maps.

  Workaround: There is no workaround.

- CSCth82164

  Symptoms: A peer's key is cached indefinitely in the key cache.

  The following messages indicate bypassing the revocation check:

  ```
  *Jul 13 18:43:18.095: ISAKMP:(1002): peer's pubkey is cached
  *Jul 13 18:43:18.095: CRYPTO_PKI: Found public key in hash table. Bypassing
  certificate validation
  ```

  Conditions: A method (OCSP, CDP, etc.) to check for certificate revocation is used, then it is changed to "none" ("'revocation check none''), and finally it gets changed to some revocation method again.

  This configuration transition "'revocation check -> no revocation check -> revocation check'' is what causes a problem.

  Workaround: There is no workaround.

  Further Information: The problem is independent of which revocation method is used (OCSP, CDP). The problem will happen when revocation check is disabled with the command "revocation none''. This would cache the peer's key infinitely into the cache. After this, turning on any revocation method will have no effect; validation will always succeed since the keys are cached.

  The problem will only happen if someone turns off revocation and then later realizes that it was a mistake and turns it back on. If remote peer's key is cached within that period then that cache entry will never be deleted. End Result: If the same remote peer tries to establish the tunnel again we would bypass validation and would not check if it is still a valid peer or not.

  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 5.0/4.1:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:U/RC:C

  CVE ID CVE-2011-0935 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/en/US/products/products_security_vulnerability_policy.html

- CSCth84714

  Symptoms: With scaled number of MLP bundles on Sip200 with DLFI enabled, the sip200 crashes.

  Conditions: This symptom occurs with the following conditions:

  1. Reload the SPA having MLP bundles.
  2. Shut/no shut the controller.
  3. Flap the links by any other means.

  Workaround: The issue is not seen without high traffic and without LFI enabled.

- CSCth84995

  Symptoms: Router may reload when performing an ISSU upgrade or downgrade.

  Conditions: This symptom occurs when performing an ISSU upgrade or downgrade.

Workaround: There is no workaround.

- CSCth85618

  Symptoms: Extra syslog gets printed but no other functionality is impacted.

  Conditions: This symptom occurs under normal conditions.

  Workaround: There is no workaround.

- CSCth87195

  Symptoms: Flexwan ATM interface goes down.

  Conditions: This symptom is observed while configuring “mac-address” or “atm bridge-enable”.

  Workaround: Perform a shut/no shut on the interface.

- CSCth87587

  Symptoms: Spurious memory access or a crash is seen upon entering or modifying a prefix-list.

  Conditions: The primary way to see this issue is to have “neighbor *neighbor address* prefix-list out” configured under “address-family nsap” under “router bgp” when configuring/modifying a prefix-list.

  Workaround: There is no workaround.

  Further Problem Description: The issue is only specific to certain scenarios when prefix-lists are used in conjunction with “nsap address-family”.

- CSCth92171

  Symptoms: The serial interface stays down longer if a switchover is done while flapping the multilink interface from the far end.

  Conditions: This symptom is observed when switching over to the standby while flapping the multilink interface from the far end.

  Workaround: Shut the flapping links, then perform the switchover.

- CSCth93218

  Symptoms: The error message “%OER_BR-4-WARNING: No sequence available” displays on PfR BR.

  Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

  Workaround: There is no workaround.

- CSCth94814

  Symptoms: Crash is seen in static route component.

  Conditions: The symptom is observed when changing IVRF on a virtual-template when there are about 100 active sessions.

  Workaround: There is no workaround.

- CSCth94827

  Symptoms: IDBINDEX_SYNC-STDBY tracebacks are seen when unconfiguring ima- group on a SONET-ACR controller.

  Conditions: This symptom is observed on a standby supervisor when unconfiguring and configuring ima-group on a SONET-ACR controller.

  Workaround: There is no workaround.

- CSCth96398

  Symptoms: Local MPLS labels change after an SSO causing a traffic drop a for short period of time.

  Conditions: The symptom is observed when LDP graceful restart is configured and SSO is supported on the platform. Only the prefixes which have a local label but not a remote label before the SSO are affected. After SSO, these prefixes get assigned a new local label. The traffic should recover once the LDP neighbors learned the new labels.

  Workaround: There is no workaround.

- CSCth99021

  Symptoms: Spurious memory access at hqf_send_blt_msg_to_linecards is seen on performing SSO switchover. Some times the router crashes with the same decode.

  Conditions: The symptom occurs on performing an SSO switchover.

  Workaround: There is no workaround.

- CSCth99104

  Symptoms: Certificate that should not be allowed bypasses validations checks.

  Conditions: This happens when the PKI validation test command is used.

  Workaround: Do not use the PKI validation test command.

  Further Information: The PKI validation test command invokes the pubkey insert api which erroneously adds pubkey entries when at times it should not. this results in all subsequent validations bypassed for the same certificate.

  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 1.7/1.4:

  https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:L/AC:L/Au:S/C:P/I:N/A:N/E:F/RL:OF/RC:C/CDP:ND/TD:ND/CR:ND/IR:ND/AR:ND

  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/en/US/products/products_security_vulnerability_policy.html

- CSCth99237

  Symptoms: LNS does not respond to an LCP echo reply when waiting for a response from the AAA server. As a result, the peer may close the session.

  Conditions: The symptom is observed under the following conditions:

  1. If the client starts to send LCP echo requests during the PPP Authentication phase.
  2. If the primary AAA server is unreachable and/or the authentication response is otherwise delayed.

  Workaround: There is no workaround.

- CSCti02076

  Symptoms: On a system running Cisco IOS, after unconfiguring an IPv6 link- local address from an interface, any global ipv6 addresses may disappear.

  Conditions: This issue may occur on systems running Cisco IOS when IPv6 is being configured. This issue occurs if an attempt is made to remove the IPv6 link-local address without use of the **link-local** keyword.

  Workaround: There is no workaround.

- CSCti03199

  Symptoms: During switch-over, standby crashes after every recovery due to config-sync.

  Conditions: The symptom is observed when the standby tries to sync with the active and when “crypto pki trustpoint” is configured with an unavailable port-channel as source-interface.

  Workaround: There is no workaround.

- CSCti04670

  Symptoms: A crash may occur while the system is in flux with iEdge sessions going up and down while at the same time the **show ssm** command is issued on the console.

  Conditions: This symptom is seen when issuing the **show ssm** command.

  Workaround: Issue the **show ssm** command and then show logging to see the results.

- CSCti05663

  Symptoms: A DHCP ACK which is sent out in response to a renew gets dropped at relay.

  Conditions: The symptom is observed in the case of an numbered relay.

  Workaround: There is no workaround.

- CSCti08336

  Symptoms: PfR moves traffic-class back and forth between primary and fallback links the when PfR Link group feature is used.

  Conditions: The symptoms are most likely to occur when there is one exit in the primary link-group and utilization is one of the criteria. The issue can also occur when there are two links in the primary. A traffic-class is moved from the primary link to the fallback link when the primary link is OOP. After the move, the primary link and the fallback link are “IN” policy. At that time, PfR moves the traffic-class back to primary causing the primary link to go “Out” of policy.

  Workaround: There is no workaround.

- CSCti08811

  Symptoms: A router running Cisco IOS may reload unexpectedly when running commands through an Embedded Event Manager (EEM) policy.

  Conditions: This symptom is observed only with EEM policies.

  Workaround: There is no workaround.

- CSCti10518

  Symptoms: Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the RIB.

  Conditions: If redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the NDB in process.

  Workaround: There is no workaround.

- CSCti13286

  Symptoms: Putting this configuration on a router:

```
router rip
  version 2
  no validate-update-source
  network 10.0.0.0
  no auto-summary
  !
  address-family ipv4 vrf test
```

```
 no validate-update-source
 network 172.16.0.0
 no auto-summary
 version 2
exit-address-family
```

and doing a reload causes the “no validate-update-source” statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti15990

  Symptoms: EzVPN will not come up if the dialer interface flaps.

  Conditions: This symptom is observed when the dialer interface is profile- based.

  Workaround: If deploying with PPPoA is not a constraint, then using non-profile based dialer interface as ezvpn outside interface will solve the issue. Other wise there is no workaround.

- CSCti18615

  Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP out-of-sync with the active RP. A and F flags are missing from the multicast forwarding base entries.

  Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, the router is in HA mode SSO, and is reloaded from the RP.

  Workaround: Perform a Shut/no shut of the affected interfaces.

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

  Conditions: The symptom is observed when PfR is configured with the following conditions:

  1. List > application > filter > prefix-list
  2. Learn > traffic-class: keys
  3. Learn > traffic-class: filter > ACL

  Workaround: There is no workaround.

- CSCti22190

  Symptoms: The EIGRP autonomous system command does not NVGEN.

  Conditions:

```
interface Tunnel2
 ip vrf forwarding vpn2
no ip next-hop-self eigrp 10
```

  Now configure the address-family ipv4 command under legacy mode. For example:

```
router eigrp 10
no auto-summary
address-family ipv4 vrf vpn2
 no auto-summary
```

Now show the running configuration; the autonomous system command is not NVGENed.

Workaround: Use the **address-family ipv4 vrf vpn2 autonomous 10** command.

- CSCti22544

  Symptom: IKE fails to come up while using RSA signature. PKI debugs show the following message:

  ```
  PKI-4-CRL_LDAP_QUERY: An attempt to retrieve the CRL from
  ldap://yni-u10.cisco.com/CN=nsca-r1 Cert Manager,O=cisco.com using LDAP has failed
  ```

  Conditions: This symptom is observed when the VRF-aware IPsec feature is used and vrf-label is configured under trustpoint; for example, crypto pki trustpoint yni-u10 enrollment.

  Workaround: There is no workaround.

- CSCti24577

  Symptoms: System crashes on active or hangs on standby.

  Conditions: The symptom is observed when a banner command is in the configuration.

  Workaround: Remove all banner commands.

- CSCti25319

  Symptoms: A directly connected subnet that is covered by a network statement is not redistributed into another routing protocol, even if a redistribute Open Shortest Path First (OSPF) is configured.

  Conditions: This symptom occurs only for those configurations in which a network mask covers multiple supernets. For example, for the following network statement,

  ```
  router ospf 1
  network 192.168.0.0 0.255.255.255 area 0
  the above mentioned symptom occurs if the interfaces are configured with IP
  addresses as follows:
      ip address 192.168.0.1 255.255.255.0
      ip address 192.168.1.1 255.255.255.0
      and so on.
  ```

  Workaround 1: Enable OSPF using interface command “ip ospf *AS* area”

  Workaround 2: Configure multiple network statements with mask/wildcard equal to supernet as shown in the example below:

  ```
  router ospf 1
      network 192.168.0.0 0.0.0.255 area 0
      network 192.168.1.0 0.0.0.255 area 0
      and so on.
  ```

- CSCti25339

  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/en/US/products/products_security_vulnerability_policy.html

- CSCti25780

  Symptoms: One of the case values in the EIGRP registry is corrupted. This is seen right after bootup.

  Conditions: This symptom is observed when some of the files are compiled with optimization.

  Workaround: The corruption is not seen if the files are compiled with optimization disabled.

- CSCti26202

  Symptoms: With a Cisco 3900 series router, Modular Exponent (ModExp) is currently done using software and this leads to bad scalability.

  Conditions: The symptom is observed on a Cisco 3900 series router.

  Workaround: There is no workaround.

- CSCti26852

  Symptoms: Router crashes at ppp_sip_sw_session_cleanup.

  Conditions: The symptom is observed with multilink PPP scaled configurations and with a Cisco 7600 series platform. The crash may be seen following a SPA OIR. The crash decode is:

```
sw_mgr_sm_valid_seg_class (seg_class=0x30343408)
at ../xconnect/seg_sw_mgr_util.c:443
#1  0x120ab814 in sw_mgr_get_segtype (seg_class=0x30343408)
at ../xconnect/seg_sw_mgr_util.c:478
#2  0x1435cd2c in ssf_dp_drop_remove_L2_context (seg1_class=0x30343408)
at ../machine/../sss/ssf_switching_registry.regh:173
#3  0x1435d48c in ssf_dp_remove_dp_only_L2_features (seg_class=0x30343408)
at ../sss/ssf_switching_util.c:113
#4  0x11c850f8 in ppp_sip_sw_session_cleanup (session=0x3a1c54f0)
at ../VIEW_ROOT/cisco.comp/ppp/core/src/ppp_sip_switching.c:537
```

  Workaround: There is no workaround.

- CSCti28710

  Symptoms: Chunk memory leak is observed on oer_mc_nfc_add_template and oer_mc_nfc_get_source

  Conditions: This symptom occurs on oer_mc_nfc_add_template and oer_mc_nfc_get_source.

  Workaround: Change the border IP address.

- CSCti31984

  Symptoms: Router crashes.

  Conditions: This symptom occurs when "Show stats" is used to show auto Ethernet monitor operation.

  Workaround: There is no workaround.

- CSCti32498

  Symptoms: Ingress HQoS policy queues are removed after LC OIR on subinterface.

  Conditions: This symptom occurs when flat SG having shaper is applied in ingress on subif and HQoS queueing policy is applied on subif.

  Workaround: There is no workaround.

- CSCti34396

  Symptoms: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

  Conditions: The symptom is seen when “next-hop-unchanged allpaths” is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is an unreachable.

  Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the nexthop is set to a visible address, you would configure:

```
route-map static-nexthop-rewrite permit 10
match source-protocol static
 set ip next-hop <router ip address>
!
router bgp <asn>
 address-family ipv4 vrf <vrf name>
 redistribute static route-map static-nexthop-rewrite
 exit-address-family
 exit
exit
```

  Workaround 2: Instead of configuring static routes with a next-hop, specify an interface name.

  For example, if you had:

  ip route x.x.x.x 255.255.255.0 y.y.y.y

  And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with:

  ip route x.x.x.x 255.255.255.0 interface serial2/0

  Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration “set ip next-hop self” is added to route-maps.

  When used in conjunction with the newly added configuration:

```
router bgp <asn>
 address-family vpnv4 unicast
  bgp route-map priority
```

  The “set ip next-hop self” will override “next-hop unchanged allpaths” for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti34462

  Symptoms: After FPD upgrade, a **shut** on the active shows **no shut** on the standby.

  Conditions: The symptom is observed after an FPD upgrade.

  Workaround: Perform a **no shut** then shut the interface on the active to sync it properly.

- CSCti34627

  Symptoms: This bug is caused by a problem with the fix for CSCth18982. When a neighbor in multiple topologies is enabled, the open sent for the base topology clears the nonbase topology session for the same neighbor.

  Conditions: A GR-enabled neighbor exists in different topologies, one of them being the base topology.

  Workaround: Disable GR.

- CSCti34795

  Symptoms: In RA mode, SCEP enrolment requests stay in pending status. They will not time out automatically and cannot be cancelled with the **no crypto pki enroll** *tp*.

  Conditions: The symptom is observed when “enrolment mode ra” is configured under the Trust-Point.

  Workaround: Do not use RA mode, although in certain environments it is not scalable.

- CSCti39902

  Symptoms: An RRI route is still seen on the UUT via router1 after the deletion of the IPsec SA.

  Conditions: Configure RRI on the UUT.

  Workaround: There is no workaround.

- CSCti43395

  Symptoms: Tracebacks are seen during DHCP message exchange. Crash may also be seen with the tracebacks.

  Conditions: This symptom is seen when DHCP relay agent is configured with “ip dhcp relay information option vpn” and clients with duplicate MAC address are coming in at the same time.

  Workaround: Unconfigure “ip dhcp relay information option vpn”. Or, disallow clients with duplicate MAC.

- CSCti45732

  Symptoms: Upon a reload, a Cisco 7600 series router configured as VTP server may lose some VLANs from its VLAN database.

  Conditions: The VLANs lost do not have any access ports in the device. All other switches in the network should be in VTP transparent mode. This issue is seen on a Cisco 7600 series router that is running Cisco IOS 12.2 (33)SRE1 and SRE2 Releases.

  Workaround: Configure the Cisco 7600 as VTP transparent instead of VTP server.

- CSCti47550

  Symptoms: With a scaled L3 ACL on EVC on ES+ line cards, some of the ACEs do not work, while others work as normal.

  Conditions: The symptom is observed when the line card or router is reloaded with the ACL configuration present.

  Workaround: Remove and add ACL on the EVC.

- CSCti48014

  Symptoms: A device reloads after executing the “show monitor event *comp*... all detail” command (where *comp* is an option listed under “show monitor event ?”).

  Conditions: This symptom is observed if the configurations are done in the order below:

  ```
  monitor event-trace <comp> stacktrace <depth>
  monitor event-trace <comp> size <size value>
  ```

  and any related event gets recorded in between the above two configurations.

  Workaround: To avoid the crash, change the order of the above configurations; that is, configure the **size** command first and then configure the **stacktrace** command.

- CSCti48504

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- CSCti49472

  Symptoms: System “accounting off” record is seen with suppress-CLI enabled.

  Conditions: With AAA CLI for suppressing system accounting records on switchover enabled, “Accounting OFF” is sent from a Cisco 7600 router.

  Workaround: There is no workaround.

- CSCti49508

  Symptoms: The command **show platform isg session all** displays stale entries on a Cisco 7600 series router for ISG sessions that are not on the router.

  Conditions: This symptom is observed under the following conditions:

  1. A number of port channel subinterfaces are configured with ISG
  2. ISG sessions are active on the subinterfaces
  3. The main port channel is removed without removing the sessions or ISG configuration from the individual port channel subinterfaces, using the **no interface port-channel** <> command

  Workaround: There is no workaround.

  To avoid this symptom:

  1. Delete the session/ISG configuration from the individual port channel subinterface
  2. Then delete the port channel.

- CSCti50419

  Symptoms: For PPPoMPLS/HDLCoMPLS pseudowires, after you perform the switchover, traffic loss is seen and CE interfaces stay down.

  Conditions: The symptom is observed on performing an SSO switchover with PPPoMPLS and HDLCoMPLS pseudowires. The control word gets programmed incorrectly on the line card leading to traffic loss.

  Workarounds:

  1. Unprovision and provision the pseudowire.
  2. Perform a SPA OIR.

- CSCti50607

  Symptoms: A Cisco 7200 SRE1 router drops GRE packet size 36-45.

  Conditions: The symptom is observed on a Cisco 7200 series router with SRE1 code.

  Workaround: There is no workaround.

- CSCti51145

  Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

  Conditions: In order to see this problem, ALL of the following conditions must be met:

  - The non-reloading device must have a “neighbor x.x.x.x transport connection- mode passive” configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword “established” or “eq bgp”.
  - It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload.
  - When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages.
  - Both peers must be multisession capable.
  - “transport multi-session” must not be configured on either device, or enabled by default on either device.
  - “graceful restart” must not be configured.

  Workarounds:

  1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
  2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor.
  3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.
  4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**.
  5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

  Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where “neighbor x.x.x.x transport single-session” is configured and NSF is not configured.

  The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

  Note that the fix does not solve the problem when interacting with Cisco IOS Release 12.2(33)SB based releases if the Cisco IOS Release 12.2(33)SB router is the one not reloading.

- CSCti53664

  Symptom: CoPP hardware counters not incrementing when **sh policy-map control-plane** command is run for traffic coming on ES20+ cards.

  Conditions: This symptom is observed when CoPP is configured and traffic is coming in on ES20+, which is destined to switch the ip address.

Workaround: Move the l3 interface from the switch for the traffic coming in on ES20+ line cards.

- CSCti54173

  Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCti56980

  Symptoms: Applying a service-policy under an interface or subinterface on an ES+ card in a Cisco 7600 series router may fail with the following error:

  random-detect aggregate is not supported in output direction for this interface Configuration failed!

  Conditions: The symptom only occurs when a SIP400 is being replaced by an ES+ card on which the QoS configuration will be applied.

  Workaround: Reload the router with the ES+ card installed.

- CSCti58027

  Symptoms: MPLS TE FRR fails on P2MP tunnels.

  Conditions: This symptom occurs on Cisco IOS c7600 series routers that are running Cisco IOS Release 15.0(1)S and when the following conditions are met:

  – Link protection configured for primary tunnel.
  – Incoming, primary output, and secondary output interfaces are all on the same line card.

  Workaround: Move the input interface to another slot.

- CSCti58272

  Symptoms: A PKI server with the **grant auto trustpoint** command will crash on client re-enrolment if PKI-AAA is enabled on the trustpoint associated with the **grant auto** command.

  Conditions: If trustpoint “pki-trustpoint” contains an authorization list PKI- AAA option, and pki-trustpoint is used as the “grant auto trustpoint” option on the PKI server:

```
!
crypto pki server ca-server
  ...
  grant auto trustpoint pki-trustpoint
  ...
crypto pki trustpoint pki-trustpoint
  authorization list aaa
!
```

  The device crashes whenever a re-enrolment attempt is made to the PKI server.

  Workaround: Remove authorization list from the trustpoint (and skip the PKI- AAA process).

- CSCti59562

  Symptoms: DHCP accounting stop does not clear IP initiated sessions and radius-proxy sessions.

  Conditions: This symptom occurs when VRF mapping is being used.

  Workaround: There is no workaround.

- CSCti59656

  Symptoms: When a TP tunnel is configured on a distributed system, the adjacencies are not in sync between the active and standby.

Conditions: Configure TP tunnel in a distributed system.

Workaround: There is no workaround.

- CSCti61949

  Symptoms: Unexpected reload with a “SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header” and “chunk name is BGP (3) update” messages.

  Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

  Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti62125

  Symptoms: When a 67XX card is inserted in slot 2 of a 7606-S chassis, then other cards (such as ES+, ES, and SIP) in the other slot face fabric CRC errors. The ES+ in the other slot gets hung and leads to a crash.

  Conditions: The symptom is observed when a 67XX card is inserted in slot 2 of a 7606-S chassis.

  Workaround: There is no workaround.

- CSCti62267

  Symptoms: An IPv6 CEF output is not seen in SP.

  Conditions: This symptom is observed when IPv6 is configured on UUT. This symptom is not observed with Ping.

  Workaround: There is no workaround.

- CSCti62913

  Symptoms: IP SLA repeatedly sends traps.

  Conditions: This symptom is observed in Cisco IOS Release 15.1T when IP SLA probes start failing and the router is configured to send traps, as in the following sample configuration:

```
ip sla 1
 icmp-echo 10.22.22.22 source-ip 10.11.11.11
 threshold 2000
 timeout 2000
 frequency 3
ip sla schedule 1 life forever start-time now
ip sla reaction-configuration 1 react timeout threshold-type consecutive 3 action-type
trapOnly
```

  Workaround: There is no workaround.

  Further Problem Description: When reaction condition is reached, a flag should be set and only one probe should be sent. No additional traps should be sent until the flag is set.

- CSCti65716

  Symptoms: The access interface connecting to the client is on global routing domain. If a service logon profile on a VRF is downloaded to the client, the client could potentially stay on a VRF even when a service logoff is performed later. The client traffic has to return to global domain when a service logoff is performed.

  Conditions: This symptom is see when access interface is on global routing domain. Service logon is on a VRF.

  Workaround: There is no workaround.

- CSCti66076

  Symptoms: A standby HSRP router could be unknown after reloading the ES20 module that configured HSRP.

  Condition: This symptom is observed under the following conditions:

  - HSRP version 1 is the protocol that must be used.
  - Use HSRP with sub-interfaces on ES20 module
  - Reload the ES20 module

  Workaround: Change to HSRPv2, which is not exposed to the issue.

  Alternate Workarounds:

  1. Reconfigure HSRP on all subinterfaces
  2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti66155

  Symptoms: A Cisco IPSec router may unexpectedly reload due to bus error or software-forced crash because of memory corruption or STACKLOW error.

  Conditions: This is seen when the WAN link goes down and causes recursion between multiple tunnels using tunnel protection. (That is, there are tunnel 0 and tunnel 1. After the WAN link goes down, the routing table shows a link to the tunnel 0 destination through tunnel 1 and the tunnel 1 destination is through tunnel 0.)

  Workaround 1: Change the tunnel source to be the physical WAN interface so that when the WAN link does go down, the tunnels are brought down immediately.

  Workaround 2: Change the routing protocol so that the router in question does not have recursive routing when the link goes down.

  Workaround 3: If possible, create a floating null route for the tunnel destinations that is less preferred than the route normal route to the tunnel destination, but more preferred than the route that gets installed after the WAN link goes down.

- CSCti67102

  Symptoms: Tunnel disables due to recursive routing loop in RIB.

  Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

  Workaround: There is no workaround.

- CSCti67429

  Symptoms: A REP segment configured on 7600-ES+20G3CXL interfaces on a Cisco 7600 series router that is running Cisco IOS Release 15.0(1)S is not recovering as expected upon link failure recovery of the edge port configured on the 7600. A traffic storm triggered by ISIS protocol configured between 7600 and the MWR 2941s in the REP ring is occurring when the failed REP edge port becomes operational again.

  Conditions: The symptom is observed with a REP ring including two Cisco 7600 series routers equipped 7600-ES+20G3CXL and running Cisco IOS Release 15.0(1) S configured with ISIS and MPLS LDP. The problem is also present in Cisco IOS Release 12.2(33)SRE1.

  Workaround: Configure static routes between the 7600 routers and the MWR 2941s instead of ISIS.

- CSCti67447

  Symptoms: During an SSO, an 8 to 12 second packet drop may occur on EoMPLS VCs.

  Conditions: The symptom is observed under the following conditions:

  1. EoMPLS port-based or VLAN-based configuration; VC between PE1 and PE2.
  2. Enable MPLS LDP GR.

  Workaround: There is no workaround.

- CSCti67832

  Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.

  Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug **debug crypto gdoi gm all-features**.

  Workaround: There is no workaround.

- CSCti68721

  Symptoms: The output of show performance monitor history interval <all | given #> will appear to have an extra column part way through the output.

  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

  Workaround: If the symptom occurs, repeat the command.

- CSCti69008

  Symptoms: When dampening is configured for many VRFs, doing full vpnv4 radix tree walk and the proposed fix improves convergence by doing subtree walk based on VRF/RD.

  Conditions: Dampening configuration changes for VRFs.

  Workaround: There is no workaround.

- CSCti69990

  Symptoms: A router crashes after deconfiguring IPv6 and then reconfiguring.

  Conditions: The symptom is observed only under specific conditions. Router has IPv6 configured on a number of interfaces and also has GLBP configured. IPv6 configuration is removed from all interfaces and then re-applied.

  Workaround: There is no workaround.

- CSCti72498

  Symptom: A crash occurs on a device acting as DHCP Server.

  Conditions: This symptom is observed when a requested IP address option is present in DHCP requests.

  Workaround: Disable the DHCP ping check with the help of CLI “ip dhcp ping packets 0.”

- CSCti74736

  Symptoms: A traffic drop might appear on a GREoMPLS tunnel after an SSO switchover in an egress direction. If an ingress interface is located on a SIP400 series line card, the following error message will be continuously printed:

  ```
  %INTR_MGR-3-BURST: HY_FD_PP_EC_EC_ERR_INT[0x1] bad payload CRC exceeds threshold
  ```

Conditions: The presence of “mls mpls tunnel-recir” is required for the GREoMPLS feature to work. After the second SSO switchover since bootup, the command will be inactive and the feature broken. The issue is applicable to Cisco IOS Release 12.2(33)SRE2, but not to Release 12.2(33)SRE1.

Workaround: Reload the router.

- CSCti74962

  Symptoms: “%PM-SP-4-PORT_BOUNCED: bounced by Consistency Check IDBS UP” message seen on A3-1 new active router after line card OIR followed by an SSO switchover.

  Conditions: This symptom will occur only with a line card OIR followed by an SSO switchover.

  Workaround: There is no workaround.

- CSCti76466

  Symptoms: A static PW over P2MP functionality outage occurs.

  Conditions: This symptom is observed with static PW over P2MP Tunnel configurations.

  Workaround: There is no workaround.

- CSCti77521

  Symptoms: Policy-map is not attached to a DLFIoATM interface after a SPA OIR.

  Conditions: The symptom is observed upon performing a SPA OIR. The issue is seen with ATM SPA on a SIP400.

  Workaround: Perform a shut/no shut of the ATM interface.

- CSCti80876

  Symptoms: Malloc subroutine fails on a setup with 600 s,gs with a CFC card.

  Conditions: This symptom occurs when churning the l2 Switched Virtual Interface (SVI) OIFs on SP.

  Workaround: There is no workaround.

- CSCti80904

  Symptoms: A router reloads at sec_send_command while booting up.

  Conditions: The symptom is observed on a Cisco 887 and a Cisco 888 router.

  Workaround: There is no workaround.

- CSCti81177

  Symptoms: Features like Videomon do not work on routed port.

  Conditions: This symptom occurs when an interface is configured as a switchport and reconfigured to routed Port.

  Workaround: Reload the line card.

- CSCti81444

  Symptoms: Traffic does not flow in egress direction over VPLS PW on router reload.

  Conditions: The symptom is observed after a router reload. POE bits for the imposition interface are not getting programmed on the egress line card.

  Workaround: There is no workaround.

- CSCti82141

  Symptoms: The following symptoms are observed:

  1. The “none” option will be missing in the **show run** output after “ntp pps-discipline none inverted stratum *#value*” is configured.
  2. “Invalid input detected” error message will be thrown during the bootup and the configured “ntp pps-discipline none inverted stratum *#value*” will vanish after a reload.

  Conditions: The symptom is observed when the “inverted” option is included in the “ntp pps-discipline” CLI.

  Workaround: Configure the CLI without the “inverted” option.

- CSCti82670

  Symptoms: An RSP will crash when the CFM automated test script (consisting of 53 tests) is run twice in succession.

  With SUP720, the crash is seen with a single run.

  Conditions: The automated test script must be run on 3 connected routers.

  Workaround: Adding a **no shut** on UUT interface with UP- MEPS before doing the LeakConfig seems to prevent the crash and provide a clean run.

  Further Problem Description: Other problems observed are:

  - The CFM MIB will return infinite results for getmany.
  - A **show** command will crash the router.

- CSCti83705

  Symptoms: IPv4 unicast traffic not forwarded out of a Cisco 7600 series router’s GREoMPLS in VRF tunnel.

  Conditions: The symptom is observed with an IPv6 Address Family (AF) configured under VRF. If the IPv6 AF is in the startup configuration then the feature is broken straight after boot up. If the IPv6 AF is configured after boot up, then feature gets broken after this configuration.

  Workaround: Remove IPv6 AF from the tunnel’s VRF.

- CSCti83737

  Symptom: A module will crash with a software-forced crash. The following will be seen in the crash logs.

  ```
  Aug 29 06:11:05 UTC: DFC7: sip10g_tefrr_program_vc_list() TMEM_ASSERT failed on line
  5692 %Software-forced reload
  06:11:05 UTC Sun Aug 29 2010: Breakpoint exception, CPU signal 23, PC = 0xXXXXXXXX
  ```

  Conditions: This symptom is observed on a SIP-600 and 7600-ES20-10G3C.

  Workaround: There is no workaround.

- CSCti84762

  Symptoms: Update generation is stuck with some peers held in refresh started state (SE).

  Conditions: This is seen with peer flaps or route churn and with an interface flap.

  Workaround: Do a hard reset of the stuck peers.

- CSCti85402

  Symptoms: Cisco 10000 VRF transfer will fail for IP DHCP sessions.

  Conditions: This symptom occurs after RP switchover.

Workaround: There is no workaround.

- CSCti85446

  Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

  Conditions: The symptom is observed with the following conditions:

  1. Configure a nexthop static route with permanent keyword.
  2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface).
  3. Change the configuration in such a way that nexthop is reachable.
  4. Configure a new static route through the same nexthop IP address used in step 1.

  Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti86169

  Symptoms: A device that is acting as a DHCP relay or server crashes.

  Conditions: This symptom is observed when the **no service dhcp** command is configured.

  Workaround: There is no workaround.

- CSCti87912

  Symptoms: While bringing up PPP sessions, server fails to add a route to the client after the IPCP negotiation happens.

  Conditions: This symptom occurs with the following two conditions:

  1. “ip unnumbered...” per user configuration that is received from radius is applied on the virtual-access interface.
  2. Virtual-template that used for Virtual-access creation is configured with “ip unnumbered <>”.

  Workaround: There is no workaround.

- CSCti88062

  Symptoms: Traffic stops flowing through ports configured with REP over EVC BD when an ES20 line card is replaced by an ES+ in the same slot.

  Conditions: The symptom is observed on a router running MST, having an ES20 card configured with EVC BD which is replaced by an ES+ in the same slot with an EVC BD configuration. MST puts the BD VLAN in a disabled state and the traffic on that VLAN stops flowing.

  Workaround: Reload the router.

- CSCti92798

  Symptoms: A Cisco router crashes while configuring http commands with atm.

  Conditions: This symptom is observed on a Cisco7200 router running Cisco IOS Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCti94938

  Symptoms: With more than 1 L2TP sessions on virtual template interface, when applying non-existent route-map and modifying non-existent route map, router crashes.

  Conditions: This symptom occurs with PPPoE sessions with modifying policy configuration with non-existent route-map.

  Workaround: Configure route-map first before applying policy.

- CSCti95511

  Symptoms: The command **no buffer header permanent** does not restore the default number of header buffers.

  Conditions:

  1. Issue is seen only when configuring header/fast switching buffers.
  2. Buffers need to be created for this pool.

  Workaround: Configure the buffer CLIs carefully. This issue could be avoided by:

  1. Not configuring “buffer header permanent” with a high value when available memory is low.
  2. Not configuring “no buffer header permanent” when the number of buffers in the free list is less than the minimum value.

- CSCti97759

  Symptoms: IPSG configuration with DHCP snooping entry configuration causes the RP to crash.

  Conditions: This is seen when DHCP static entry is configured.

  Workaround: There is no workaround.

- CSCti97810

  Symptoms: A “%SYS-2-FREEBAD” memory traceback is seen on an HA router.

  Conditions: The symptom is observed on an HA router approximately 3-4 minutes after loading the image on an HA router.

  Workaround: There is no workaround.

- CSCti98931

  Symptoms: Some sessions may be lost after Layer 2 Tunneling Protocol (L2TP) switchover.

  Conditions: This symptom occurs after L2TP switchover.

  Workaround: There is no workaround.

- CSCtj00039

  Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

  Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

  Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj00728

  Symptoms: A router crashes when enabling a DECnet neighbor.

  Conditions: The symptom is observed with a DECnet neighbor limit on a single node of 32. If one exceeds 32, the crash is seen.

  Workaround: Limit neighbor count to 32.

- CSCtj01623

  Symptoms: REP topology stays incomplete after manual pre-emption. When the issue occurs, REP pre-emption will not take effect.

  Conditions: The symptom can be observed for EVC or switchport.

  Workaround: There is no workaround.

- CSCtj04278

  Symptoms: In a DMVPN setup that is running the code of Cisco IOS Release 15.1TPI15, it is possible that NHRP Registrations are not sent by the box. This is seen if crypto is not configured using tunnel protection.

  Conditions: This symptom occurs when tunnel protection is not configured.

  Workaround: perform a shut/no shut of the tunnel interface.

- CSCtj05198

  Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

  Conditions: This symptom is observed when there are two EIGRP router processes.

  Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj05591

  Symptoms: Memory corruption and SP crash seen.

  Conditions: The symptom is observed when creating 600 subinterfaces as OIF for Mroute entries.

  Workaround: There is no workaround.

- CSCtj05903

  Symptoms: Some virtual access interfaces are not created for VT, on reload.

  Conditions: This symptom occurs on scaled sessions.

  Workaround: There is no workaround.

- CSCtj06390

  Symptom: Ping fails after configuring crypto.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.18)T.

  Workaround: There is no workaround.

- CSCtj07904

  Symptoms: EIGRP neighbor relationship goes down with “no passive interface” configured.

  Conditions: The symptom is observed when “no passive interface” is configured.

  Workaround: Do not configure “passive-interface default” and allow the interface to be non-passive by default. Configure “passive-interface *interface*” for the interface to be passive.

- CSCtj08368

  Symptoms: Router software crash at process_run_degraded_or_crash.

  Conditions: The symptom is observed when the allocated memory block is freed.

  Workaround: There is no workaround.

- CSCtj08448

  Symptoms: No Shared Port Adaptors (SPA) come up after switch over.

  Conditions: This symptom occurs with RPR mode, if a switchover with traffic is performed.

  Workaround: There is no workaround.

- CSCtj08533

  Symptoms: QoS classification fails on egress PE if the route is learnt via BGP.

Conditions: The symptom is observed when there are redundant paths to the CPE.

Workaround: Use only one path between PE and CPE.

- CSCtf71673

  Symptoms: A Cisco 10000 series router shows a PRE crash due to memory- corruption with block overrun.

  Conditions: This symptom is seen when the system is configured for PTA and L2TP access. The system is using a special based on Cisco IOS Release 12.2(34) SB4 during a pilot phase. Other systems in same environment that are using a widely deployed special based on Cisco IOS Release 12.2(31)SB13 have not shown this so far.

  Workaround: There is no workaround.

- CSCtg85402

  Symptoms: Multicast packet software switching MFIB platform flags “NP RETRY RECOVERY HW_ERR HAL” after SSO/ISSU.

  Conditions: Issue seen only with CFC cards and not with DFC. Specific to mVPN configuration with egress CFC cards. Issue seen under rare condition with SSO/ISSU.

  Workaround: Remove and add Default MDT configuration.

- CSCti25339

  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/en/US/products/products_security_vulnerability_policy.html

- CSCtj10592

  Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.

  Conditions: The symptom is observed with a simple SVTI to DVTI connection.

  Workaround: There is no workaround.

- CSCtj11497

  Symptoms: Shared Port Adaptor (SPA) crashes after receiving “%INTR_MGR-3- INTR: PL3 RX Sequence error”.

  Conditions: This symptom occurs under normal working conditions.

  Workaround: The SPA reloads automatically and clears the problem.

- CSCtj13146

  Symptoms: Stand by redundancy mode mismatch occurs.

  Conditions: This symptom occurs when a switch from RPR mode to SSO mode happens.

Workaround: There is no workaround.

- CSCtj13191

  Symptoms: V4 multicast groups do not flow across the first hop router. Debugging shows that mfib is dropping the source traffic due to acceptance check failure.

  Conditions: V4 multicast routing is enabled and pim sparse mode traffic is flowing across the first hop router with a traffic source directly connected to it.

  Mfib debugs show this message “(TS) Acceptance check failed - dropping” on the first hop router:

  sh ip mfib “multicast group” shows no C flag for the *,g entry

  Workaround: Disable/enable multicast routing on the router to get the traffic flow to resume.

- CSCtj15805

  Symptoms: Keepalive functionality not working. An ICMP echo reply coming back from a client is ignored by ISG.

  Conditions: The symptom is observed when a VRF mapping service is used.

  Workaround: There is no workaround.

- CSCtj17316

  Symptoms: EIGRP flaps up and down in a large scale network, when there is a lot of data to be sent.

  Conditions: In an EIGRP network that has a large number of peers on a single interface, EIGRP might stop sending data to peers. This causes a flap due to packets not being acknowledged.

  Workaround 1: Find the instability in the network and fix the interface.

  Workaround 2: Summarize more routes.

  Workaround 3: Change more routers to stub.

  Workaround 4: Upgrade to rel7 of EIGRP.

- CSCtj17545

  Symptoms: Immediately after a switchover, the restarting speaker sends TCP- FIN to the receiving speaker, when receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

  Conditions: The symptom can occur when a lot of BGP peers are established on different interfaces.

  Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

  template peer-session ce-v4 transport connection-mode passive

- CSCtj17561

  Symptoms: Description for T1 broken in Prowler/Chopper SDH > C-11 mode. This might lead to sync issues while switching over.

  Conditions: The symptom is observed in SDH > C-11 mode.

  Workaround: There is no workaround.

- CSCtj17667

  Symptoms: The **debug radius** debug command may cause memory corruption and crash in rp2 and 1ru images.

  Conditions: This symptom is seen with the **debug radius** command in rp2 and 1ru images.</B>

  Workaround: Do not use the **debug radius** command.

- CSCtj18753

  Symptoms: Memory leak is seen with MLDP scale test.

  Conditions: The issue is seen only when there is a switchover from default- data-default MDT trees.

  Workaround: Avoid default-data-default MDT tree switchovers.

- CSCtj20163

  Symptoms: On a PE1-P-PE3 setup, a crash is seen on P (core) router with scaled MLDP configurations.

  Conditions: The symptom is observed with the following conditions:

  1. Execute **show mpls mldp database**.
  2. Reload Encap PE.
  3. Crash is seen on P router when MLDP neighbors go down.

  Workaround: There is no workaround.

- CSCtj20362

  Symptoms: Router does not allow configuring more than one secondary IP address in the same subnet, on an interface in the same VRF.

  Conditions: This symptom occurs when configuring a secondary address on an interface, which has already one secondary IP address in the same subnet. This applies to VNET capable interfaces.

  Workaround: There is no workaround.

- CSCtj20776

  Symptom: Accounting-stop record is sent for radius proxy session when re- authentication happens for that session.

  Accounting-stop record is sent for radius proxy session when re- authentication happens for that session.

  Conditions: This issue is seen in the following scenarios:

  1. Authentication request comes from AP.
  2. Accounting request comes from AZR and session on ISG is associated to AZR.
  3. ISG receives a re-authentication request from AP.

  The Accounting-stop record is sent for Radius-Proxy session and the services under the session, but the radius-proxy session is still active and no stop record is sent for the session on clearing the session. Also acct- terminate- cause in the stop record is set to none.

  Workaround: There is no workaround.

- CSCtj21696

  Symptoms: The virtual access interface remains down/down after an upgrade and reload.

  Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

```
Router1#sho inv
NAME: "chassis", DESCR: "2801 chassis"
PID: CISCO2801 , VID: V04 , SN: FTX1149Y0KF
NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet"
PID:CISCO2801 , VID: V04 , SN: FOC11456KMY
NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface daughtercard"
PID:VIC2-2E/M= , VID: V , SN: FOC081724XB
NAME: "WIC/VIC/HWIC 1", DESCR: "4 Port FE Switch"
```

```
PID: HWIC-4ESW , VID: V01 , SN: FOC11223LMB
NAME: "WIC/VIC/HWIC 3", DESCR: "WAN Interface Card - DSU 56K 4 wire"
PID:WIC-1DSU-56K4= , VID: 1.0, SN: 33187011
NAME: "PVDM 1", DESCR: "PVDMII DSP SIMM with one DSP with half channel capcity"
PID:PVDM2-8 , VID: NA , SN: FOC09123CTB
```

Workaround: Do a shut/no shut the serial interface.

- CSCtj24453

  Symptoms: The following traceback is observed when **clear ip bgp *** is done:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 5905A0A8
  chunkmagic 120000 chunk_freemagic 4B310CC0 -Process= "BGP Scanner", ipl= 0, pid= 549
  with call stack
  0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
  0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
  0x403A4E84:bgp_scanner(0x403a4c50)+0x234
  ```

  Conditions: It is rarely observed, when **clear ip bgp *** is done with lot of routes and route-map-cache entries.

  ```
  Router# show ip bgp sum
  BGP router identifier 10.0.0.1, local AS number 65000
  BGP table version is 1228001, main routing table version 1228001 604000
  network entries using 106304000 bytes of memory
  604000 path entries using 31408000 bytes of memory
  762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
  381 BGP AS-PATH entries using 9144 bytes of memory
  382 BGP community entries using 9168 bytes of memory
  142685 BGP route-map cache entries using 4565920 bytes of memory
  ```

  The **clear ip bgp *** command is not a very common operation in production network.

  Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj25243

  Symptoms: If non-LLQ or parent (logical) is rate-limited and oversubscribed, this can cause some policer drops in the LLQ queue, if LLQ exceeds the bandwidth allocated to it.

  Conditions: The symptom is observed if non-LLQ or parent (logical) is rate- limited and oversubscribed and if LLQ exceeds the bandwidth allocated to it.

  Workaround: There is no workaround.

  Further Problem Description: This issue is caused by CSCth85449. That caveat was intended to detect congestion on the physical interface and police LLQ traffic if it exceeds the configured bandwidth and the physical link is congested.

- CSCtj28696

  Symptoms: Session QoS will not get applied after an OIR of the line card.

  Conditions: The symptom is observed with sessions (with QoS) on a port- channel subinterface.

  Workaround: Clear session and bring up again.

- CSCtj28747

  Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an “Exit Mismatch” message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

Workaround: There is no workaround.

- CSCtj29382

  Symptoms: When cellular interface passes packets and users configure “tx-ring-limit” on cellular interface, system will crash.

  Conditions: This symptom occurs under the following conditions:

  1. Traffic runs through cellular interface.
  2. Change “tx-ring-limit” on cellular interface with traffic running in the background.

  Workaround: Stop the traffic and change “tx-ring-limit”.

- CSCtj30155

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCtj31743

  Symptoms: Memory leaks are observed at at slaAddSeqNum.

  Conditions: This symptom occurs when “pfs border” is configured.

  Workaround: There is no workaround.

- CSCtj32769

  Symptoms: Data path fails with Layer-2 Virtual Private Network (L2VPN)on ACR interface when asynchronous mode is enabled.

  Conditions: This issue occurs when a VPN is configured on ACR interface in asynchronous mode with cellpacking configurations. This issue does not occur in normal synchronous mode or Layer-2 Virtual Circuits (L2VCs).

  Workaround: Configure the same Maximum Number of Cells Packed (MNCP) value for local and remote provide edge (PE) devices.

- CSCtj35573

  Symptoms: When an interface is configured as an access interface, back-to-back ping will fail.

  Conditions: The ping failure is seen only for access interfaces intermittently. This issue is observed with the SRE2 image with SUP720 and ES+ card, in a situation when the ping packet coming from source has the BPDU bit set.

  Workaround: There is no workaround.

- CSCtj36294

  Symptoms: Traffic fails when PW switchover occurs.

Conditions: This symptom occurs when a primary PW and backup PW are configured. Shut primary PW and allow the traffic to go through backup PW. The traffic is dropped by the router.

Workaround: There is no workaround.

- CSCtj36521

  Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

  Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

  Workaround: Make sure IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj38234

  Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.

  An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.

  Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).

  Workaround: There is no workaround.

- CSCtj38346

  Symptoms: Router crash is seen when configuring the **default transmit- interface** command.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.1(2.19)T.

  Workaround: There is no workaround.

- CSCtj38519

  Symptoms: EIGRP pacing timer is large when there is a large number of peers on NBMA interfaces.

  Conditions: The symptom is observed when EIGRP is configured with a large number of peers on a single NBMA interface.

  Workaround: Ensure spokes are setup as stub and properly summarized.

- CSCtj38606

  Symptoms: The following error message is seen:

  ```
  %SYSTEM_CONTROLLER-3-MISTRAL_RESET: System Controller is reset:Normal Operation
  continues
  ```

  The **show ibc** exec command reports increments of the following counter:

  ```
  Hazard Illegal packet length = 7580
  ```

  Conditions: The symptom is observed on a Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCtj39558

  Symptoms: Sub-interface queue depth cannot be configured.

  Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

  Workaround: There is no workaround.

- CSCtj41215

  Symptoms: On an ES+, a service instance configuration is rejected with following error:

  Service instance configuration Failed. Service-Policy has already been configured on this interface

  Conditions: The symptom is observed when an ES+ is inserted in the same slot where an ES20 was previously present.

  Workaround: Unconfigure service-policy from the interface and then create a service instance.

- CSCtj41867

  Symptoms: A Cisco 2900 Integrated Service router that is running Cisco IOS Release 15.1(2)T exhibits increased memory utilization over time.

  Conditions: The symptom is observed when a Cisco 2900 Integrated Services router that is running Cisco IOS Release 15.1(2)T is configured as a branch router that has an VPN WAN connection, Quality Of Service (QoS) classification configured ("qos pre-classify"), and WAAS Express enabled on a several interfaces with MLPPP enabled.

  Workaround 1: Disable QoS classification on VPN tunnel interface.

  Workaround 2: Disable WAAS Express on VPN tunnel interface.

  Workaround 3: Reduce the number of serial interfaces down to one

  Further Problem Description: The symptom is not observed when QoS classification is not configured or when MLPPP is not configured or when WAAS Express is not enabled.

- CSCtj42230

  Symptoms: IOSD crashes on unconfiguring the service policy.

  Conditions: The crash is seen when trying to unconfigure service policy without detaching it from the ATM PVP subinterface.

  Workaround: There is no workaround.

- CSCtj43778

  Symptoms: Multiple met cc processes running on DFC.

  Conditions: This symptom occurs when toggling the met cc processes using mentioned commands.

  Workaround: Perform the toggling with sufficient time (1 minute) between the no form of the command and the command itself.

- CSCtj44237

  Symptom: High CPU observed in RP.

  Conditions: The symptom is observed with MVPN configurations.

  Workaround: There is no workaround.

- CSCtj45571

  Symptoms: If OAM VC state reaches to "AIS/RDI" after PVC is flapping, then OAM Loopback status gets stuck in "OAM failed" state. Loopback cell is not generated until shut/no shut is performed on the subinterface.

  Conditions: The symptom is observed when the OAM VC state reaches "AIS/RDI".

  Workaround: Perform a shut/no shut on the subinterface.

- CSCtj46297

  Symptoms: Ping fails when performing a shut/no shut on the outgoing interface in an FRR setup.

Conditions: The symptom is observed in an FRR setup when performing a shut/no shut on the outgoing interface.

Workaround: Perform a shut/no shut on the tunnel interface.

- CSCtj47736

  Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

  Conditions: The symptom is observed when the neighbor is learned, then you add a max-service limit on an address family. Then do a shut/no shut on the interface.

  Workaround: There is no workaround.

- CSCtj48220

  Symptoms: A Cisco router may unexpectedly reload due to bus error.

  Conditions: This symptom occurs with AAA.

  Workaround: There is no workaround.

- CSCtj48629

  Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtj48913

  Symptoms: Track does not recognize when an HTTP IP SLA probe’s status changes to OK.

  Conditions: The symptom is observed with an HTTP IP SLA probe and with a tracker.

  Workaround: There is no workaround.

- CSCtj49133

  Symptoms: After attaching a policy-map to a sub-interface, the policy-map is then renamed and then the sub-interface is deleted. The policy-map definition can not be deleted and still shows up in the running configuration.

  Conditions: The symptoms are observed with the following steps:

  1. Attach a policy to a sub-interface.
  2. Rename the policy-map.
  3. Remove the sub-interface.
  4. Removing the definition of policy-map will not succeed.

  Workaround: Remove the service policy from sub-interface before removing the sub-interface.

- CSCtj50072

  Symptoms: High CPU interrupt level caused by IPv4 unicast or multicast traffic received via GREoIP or GREoMPLS tunnel if rate is high. If ingress interface is tunnel and egress is tunnel (MDT included) as well, then outer IP ToS of egress packet will be reset to 0x0.

  Conditions: The symptom is observed after a reload (under 10% probability), GRE tunnel must be in VRF:

```
#show running-config interface tunnel 513
interface Tunnel513
 vrf forwarding REN
 ip address 10.0.2.1 255.255.255.0
 ip pim sparse-mode
```

```
 tunnel source Loopback513
 tunnel destination 10.0.113.2 (via IP or MPLS interface)
 tunnel vrf REN
end
```

To confirm hit:

```
#show vlan internal usage | include Tunnel513
4074 Tunnel513

#remote command switch show mls vlan-ram 4074 4074
(If there is 256, the defect is present)
```

Workaround: Reload the router.

- CSCtj52077

  Symptoms: Policy at subinterface is not accepted with CBWFQ.

  Conditions: This symptom is observed when policy is used in Ethernet subinterface.

  Workaround: There is no workaround.

- CSCtj52865

  Symptoms: Unable to utilize 16 queues per lowq port.

  Conditions: If you remove any QoS policy on subtargets of lowq port, because of stale lowq count on the **show platform lowq** command, we will not be able to use maximum number of queues per lowq port.

  Workaround: Only reloading the router resolves the issue.

- CSCtj55920

  Symptoms: Flapping BGP session observed. Debug IP TCP transactions found to be advertising incorrect MSS.

  Conditions: This symptom occurs when MP-BGP is running between non-directly connected peers.

  This is a day 1 bug in IOS code since BGP PMTUD feature. The issue happens in a scenario where BGP PMTUD is disabled globally on a fresh config and then peers are configured or upon reload because of the order of parsing (by default PMTUD is enabled and not nvgenn'ed). The impact is a possible session flap if an intermediate link MTU is much smaller than the negotiated PMTU. There is a way to get out of this after the issue happens and if aware an easy enough way to not get into this.

  Workaround 1: Unconfigure the global PMTUD configuration and reconfigure

  Workaround 2: Unconfigure PMTUD on per neighbor using "neighbor x.x.x.x transport path-mtu-discovery disable".

- CSCtj56142

  Symptoms: ISG uses dummy user-name within EAP re-authentication related access-requests as the session identifier.

  Conditions: The symptom is observed during EAP re-authentications and likely after CoA-based service activation on an EAP-authenticated session. This happens only when the EAP access-requests carry a dummy user-name and access- accept does not have the correct username.

  Workaround: There is no workaround.

- CSCtj58405

  Symptoms: Full multicast traffic is not sent from the source PE.

Conditions: The issue is observed only with ECMP links and with a higher scale (above 75 MVRF and 100 mroutes per VRF) for default MDTS. It is seen when one of the ECMP links which was down earlier, comes up. If all the ECMP links are already up, then the issue is not seen.

Workaround: Clear the IP mroute using **clear ip mroute** command.

- CSCtj59254

  Symptoms: Data to default MDT switchover fails in highly scaled scenarios.

  Conditions: The symptom is observed during a default to data MDT switchover.

  Workaround: There is no workaround.

- CSCtj61252

  Symptoms: Router crash when bringing up PPP sessions.

  Conditions: The symptom is observed when adding QoS classes using parametrized QoS attributes where a class name to be added happens to be sub- string of an already existing class.

  Workaround: Do no add or configure class names which are sub-strings of other classes on the router.

- CSCtj61748

  Symptom: Service activation fails occasionally.

  Conditions: This symptom occurs with multiple services in the session authentication or authorization response that are configured in the same service-group.

  Workaround: Remove fields that are related to “service-group” or “service- type” in service definitions.

- CSCtj62999

  Symptoms: PPP sessions do not come up.

  Conditions: This symptom occurs when PBR is configured under Virtual-template interface.

  Workaround: There is no workaround.

- CSCtj64899

  Symptoms: In the Cisco IOS 7600 series router, ISG CoPP does not get installed in SIP-400 LC, when burst is specified.

  Conditions: This symptom occurs for ISG CoPP with burst is configured.

  Workaround: There is no workaround.

- CSCtj65553

  Symptoms: Static route that is installed in default table is missing.

  Conditions: Static route is missing after Route Processor (RC) to Line Card (LP) to Route Processor transition on Cisco Catalyst 3000 series switching module.

  Workaround: Configure the missing static route.

- CSCtj66392

  Symptoms: Tunnel interface does not go up on standby router and IKE and IPSec SAs are not synchronized to the standby router. Even if tunnel protection is configured, crypto socket is not opened.

  Conditions: This symptom is observed when IPSec stateful failover for tunnel protection is configured.

  Workaround: Use Cisco IOS Release 12.4(11)T4.

- CSCtj69886

  Symptoms: NTP multicast over multiple hops.

  Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

  Workaround: There is no workaround.

- CSCtj70271

  Symptoms: Non-local replications are programmed as local replications in the MET3 (i.e.: if the replications are on slot 3 DFC module, then the supervisor is programmed with the sublsps of slot 3 as local replications). This causes a waste of TCAM resources and can cause traffic outage.

  Conditions: The symptom is observed with LSM/MLDP configurations.

  Workaround: Use this command: **clear ip mroute** *source group*.

- CSCtj72148

  Symptoms: A Cisco 7600 router might face an SP crash upon first reload after upgrade from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2. After successive reloads, the system functionality is restored.

  Conditions: This symptom is observed when upgrading from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2.

  Workaround: There is no workaround.

- CSCtj72730

  Symptoms: If an Enhanced Interior Gateway Routing Protocol (EIGRP) **address-family** configuration command is removed, any redistribution commands that refer to that address-family should also be removed. This defect documents a case where the redistribution command is not removed.

  Conditions: This issue occurs when the redistribution command is not removed after removing the corresponding EIGRP address-family configuration command.

  Workaround: Manually remove the redistribution commands that remain after the **address-family** command is removed.

- CSCtj74611

  Symptoms: Active supervisor in the Cisco 7600 series router reloads.

  Conditions: The symptom is observed after a line card is powered off due to keepalive failures. Possible sequence of syslog messages:

```
%OIR-SP-3-PWRCYCLE: Card in module 7, is being power-cycled off (Module not
responding to Keep Alive polling)
<...>
%C7600_PWR-SP-4-DISABLED: power to module in slot 7 set off (Failed to
configure the line card)
<...>
%EM-SP-4-AGED: The specified EM client (EM_TYPE_FABMAN_NORMAL type=29,
id=8887)
 did not close the EM event within the permitted amount of time (900000 msec).
SP: em_fabman_act_event_end_cb: (timer) SWM event 8887  (slot 7 -> HELIOS /
CARD_RUNNING) was not closed properly
```

  Workaround: There is no workaround.

- CSCtj76297

  Symptoms: Router hangs with interoperability of VM and crypto configurations.

Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

Workaround: Disable AIM and use onboard CE.

- CSCtj76788

  Symptoms: Standby RP does not come up because of <set ip nexthop recursive vrf <> X.X.X.X> sync failure.

  Conditions: This symptom occurs when the route map has a set clause referring to a VRF and the VRF is deleted without first deleting the route map set clause.

  Workaround: Configure the <set ip nexthop recursive X.X.X.X> and then do <no set ip nexthop recursive X.X.X.X> to effectively removes the set clause.

- CSCtj77004

  Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

  Conditions: The symptom is observed when “archive log config” is configured.

  Workaround: There is no workaround.

- CSCtj77188

  Symptoms: When performing an ISSU downgrade from RLS8 to RLS7 and then aborting it, the backup pseudowires are no longer setup.

  Conditions: This symptom occurs when the ISSU procedure is either cancelled or is left incomplete.

  Workaround: To clear this errored state use the **clear xconnect all** command.

- CSCtj79368

  Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.

  Conditions: The symptom is observed when removing RSA keys.

  Workaround: Stay on the same RSA keys.

- CSCtj79750

  Symptoms: Multicast responses are not obtained.

  Conditions: After a Multicast Listener Discovery (MLD) join, multicast responses are not obtained.

  Workaround: There is no workaround.

- CSCtj79769

  Symptoms: LC crashes.

  Conditions: Issue is seen in unconfiguration part.

  Workaround: There is no workaround.

- CSCtj79992

  Symptoms: Receiver end flooded in an MVPN scenario.

  Conditions: The symptom is observed even after stopping traffic.

  Workaround: There is no workaround.

- CSCtj81938

  Symptoms: The L3VPN profile configuration “transport ipv4 source *interface*” is not synced to standby, if the source interface is same as the auto-source that is picked by BGP.

  Conditions: This symptom occurs when the source interface is same as the auto- source that is picked by BGP.

  Workaround: There is no workaround.

- CSCtj82292

  Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

  Conditions: This issue occurs when summary address is advertised as follows:

  ip summary-address eigrp AS# x.x.x.x y.y.y.y 255

  Workaround: There is no workaround.

- CSCtj85333

  Symptoms: System may crash when config-template contains the config command **ip ips signature-category** and when the template is downloaded to the router using the CNS config feature commands **cns config retrieve** exec command, **cns config initial** config command. This symptom may also occur when the config template is downloaded to the router using the device Config-Update operation of Config Engine.

  Conditions: This is normal mode operation, but this symptom will occur when such CNS feature is used.

  Workaround: There is no workaround.

- CSCtj85858

  Symptoms: Coexistance of flat class-default shape policy-map (port level shape) and QOS on sub-targets (sub-interface, service instance, sessions and so on) is not supported on LowQ ES+.

  Conditions: This symptom occurs only on LowQ ES+.

  Workaround: There is no workaround.

- CSCtj86464

  Symptoms: Bundling does not occur with Distributed Link Fragmentation and Interleaving (dLFI) over ATM.

  Conditions: Bundle keeps flapping with dLFI over ATM.

  Workaround: There is no workaround.

- CSCtj86514

  Symptoms: An SNMP walk on Cisco AAL5 MIB may not return information for all PVCs configured on the device.

  Conditions: An SNMP walk query on the Cisco AAL5 MIB may fail to return information of bundled PVCs that are in down state. Information about PVCs in UP state is returned correctly.

  Workaround: To get information of bundled PVCs in down state, you need to poll with more specific OIDs. Instead of doing an snmpwalk on “1.3.6.1.4.1.9.9.66.1.1.1.1.3”, do an snmpget on “1.3.6.1.4.1.9.9.66.1.1.1.1.3.<IfIndex>.<VPI>.<VCI>”.

- CSCtj87180

  Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of “SSS Manager Disconnected Session”.

Conditions: The symptom is observed when the LAC router receives an incorrect “Error code(9): Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID” from the multihop peer.

Workaround: There is no workaround.

- CSCtj87846

  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

  Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

  Workaround: Do Shut/no shut on PfR master or PfR border.

- CSCtj88428

  Symptoms: CPP lock down occurs and fman_fp crashes.

  Conditions: This symptom occurs while performing IOSd SSO switchover with local switching configuration.

  Workaround: Reload the router.

- CSCtj88825

  Symptoms: Fabric utilization goes high and drops are seen.

  Conditions: The symptom is observed when egress replication is configured with multicast. Global ICROIF index (0x02006) is programmed which causes high fabric utilization.

  Workaround: There is no workaround.

- CSCtj91149

  Symptoms: A delay of approximately 30 seconds is observed in dynamic xconnect- based ISG session that comes up on standby, after it is up on active.

  Conditions: This symptom occurs on switchover.

  Workaround: There is no workaround.

- CSCtj91764

  Symptoms: A UC560/UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to CPU.

  Conditions: The crash happens during a complete SNMP MIB walk.

  Workaround: The CISCO-CALL-APPLICATION-MIB can be excluded via configuration.

- CSCtj92092

  Symptoms: VPN-ID is sent as the username AAA authorization fails.

  Conditions: This symptom occurs when a DHCP server is configured to use RADIUS server for providing IP to the client.

  Workaround: There is no workaround.

- CSCtj92341

  Symptoms: PIM packets are bridged causing them to not hit the decap adjacency. Hence, PIM neighborship for a few VRFs is not up.

  Conditions: This symptom is seen when all the VRFs in a scaled setup are removed, and added through a script.

  Workaround: Reload the box or reset the line card.

- CSCtj92837

  Symptoms: Router throws the error messages NoSubTkn> while accessing the filenames with special characters like (' ").

  Conditions: This symptom is observed while accessing the filenames with special characters like (' ").

  Workaround:

  1. Disable IOS.sh feature using "no shell processing".
  2. Escape shell specific characters, so that these characters are not interpreted. For example, flash:START17Mar'10.

- CSCtj94188

  Symptoms: After an LC OIR, the Red AIE peer and AIE peer ID become the same. This causes the PWs to go down.

  Conditions: LC OIR causes the Red AIE peer ID and AIE peer id to become the same.

  Workaround: Use the **clear xconnect all** to reprovision the PWs.

- CSCtj94297

  Symptoms: "F" flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

  Conditions: The symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRF.

  Workaround: Use the **clear ip mroute** in the affected mroute.

- CSCtj94358

  Symptoms: SIP400 will pass the traffic through a previously configured VLAN on reconfiguring the **bridge-domain** command.

  Conditions: This symptom is seen with the egress interface that is a SIP400 with MPB configured.

  Workaround: Remove the "bridge-domain" configuration and then add the new "bridge-domain".

- CSCtj94490

  Symptoms: Route Processor (RP) reloads after 30 RP switchovers.

  Conditions: This symptom occurs after 30 RP switchovers during 28000 PPPoEoA sessions while traffic is flowing.

  Workaround: There is no workaround.

- CSCtj94835

  Symptoms: Spurious memory access and tracebacks are seen on router reload.

  Conditions: The symptom is observed when the router is reloaded.

  Workaround: There is no workaround.

- CSCtj95032

  Symptoms: PIM packets are dropped at SIP400. As a result PIM neighborship is not formed between the CEs.

  Conditions: This symptom is seen when the egress interface is on SIP400 with bridging configured on it.

  Workaround: There is no workaround.

- CSCtj95782

  Symptoms: MDT tunnel is assigned to the default VRF instead of the configured VRF.

  Conditions: This symptom is observed when there are multiple VTY sessions into a router and **mdt default** *MDT Group Addr* command is executed in the VRF configuration submode of one VTY session just after the VRF is deleted from another VTY session.

  Workaround: Avoid configuring and unconfiguring a particular VRF from different VTY sessions.

- CSCtj96489

  Symptoms: In a CISCO 7600 router, a freshly provisioned interface, or an interface which has been administratively no shut, belonging to non-default VRF, may fail to forward traffic.

  Conditions: This is a race condition and hence timing sensitive.

  Workaround: Another interface **shut/no shut** may help restore service.

- CSCtj96915

  Symptoms: LNS router hangs up at interrupt level and goes into an infinite loop.

  Conditions: Unknown. See Further Problem Description below.

  Workaround: There is no workaround. Only power cycle can remove the symptom.

  Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtj97360

  Symptoms: Punted datapaths are multicast flows GREoIP->DefaultMDT and GREoMPLS->Default MDT.

  Conditions: This symptom occurs with device bootup with IPv4-only VRF. After bootup IPv6 is enabled for VRF, which triggers the problem.

  Workaround: Do not have IPv6 AF and the mcast configurations in the same VRF.

- CSCtj97823

  Symptoms: The 32-byte topology names are not handled correctly on bootup.

  Conditions: This symptom occurs when 32-byte topology names are not handled correctly on bootup.

  Workaround: Use topology names shorter than 32 characters.

- CSCtj99415

  Symptoms: Traffic is not dropped when the packet size is more than the egress interface MTU.

  Conditions: This symptom occurs when the egress interface is on SIP400. When the outgoing interface is on ES20 the packets are dropped at RP with an error message.

  Workaround: There is no workaround.

- CSCtk00398

  Symptoms: When receiving DHCPv6 SOLICIT from two clients with same DUID, DHCPV6 binds the Delegated-Prefix to incorrect client.

  Conditions: This symptom occurs when two clients are sending SOLICIT with same DUID.

  Workaround: There is no workaround.

- CSCtk00976

  Symptoms: File descriptor reaches the maximum threshold limit. You will be unable to save the configuration or do any file system related operation as file descriptors are exhausted. You will get "File table overflow" error.

  Conditions: The symptom is observed when running the **dir/recursive <>** command periodically using the ANA tool.

  Workaround: Do not run **dir/recursive <>** command if leaks are detected. Also, if it is running through ANA server polling, disable it.

- CSCtk02155

  Symptom: Attachment to the CHOC3 SPA console fails after seeing VC configuration command failures.

  Conditions: This symptom is seen with CHOC3 SPA on SIP200 or SIP400.

  Workaround: Reset the line card.

  Further Problem Description: The periodic process resyncs the IPC between the host and CHOC3 SPA. As this is not happening, we are not able to attach to the SPA console.

- CSCtk02647

  Symptoms: On an LNS configured for L2TP aggregation, it might be that per- user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

  Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL downloaded for PPP users via radius.

  Workaround: There is no workaround.

- CSCtk02661

  Symptoms: Bundles stop forwarding any traffic.

  Conditions: The symptom is observed when you move the SPA to a different bay on a SIP-400 and apply configurations on the new bay.

  Workaround: Reload spa on both ends.

  Alternate workaround: Unconfigure multilink before moving the SPA out.

- CSCtk02666

  Symptoms: During a graceful restart event, the peer undergoes reconfiguration. This may result in stale labels on the RRP.

  Conditions: The symptom is observed with GR + SSO + peer reprovisioning.

  Workaround: Perform a **clear xconnect** or flap the local VC.

- CSCtk05652

  Symptoms: UDLD, that uses end-to-end across an AToM link, causes the CE link on one side to be put in err-disabled state.

  See the following topology:

  SW1 (CE) <-- PE-1 <-> MPLS cloud <-> PE-2 (7600 running 12.2(33)SRE2 --> SW2 (CE)

  UDLD err-disabling the port on SW2 is seen though the link is not unidirectional.

  Conditions: This issue is observed on Cisco IOS Release 12.2(33)SRE2.

  Workaround: Run Cisco IOS Release 12.2(33)SRD5.

- CSCtk06750

  Symptoms: IP-directed broadcast packets do not get forwarded by downstream router.

  Broadcast-source----R1---serial----R2-------rcr

  Conditions: When the serial link encapsulation is set to High-Level Data Link Control (HDLC), which is the default encapsulation, the layer2 HDLC frames are sent out with an incorrect address type in HDLC header. The downstream router does not recognize the payload as a broadcast packet and it does not forward it further as a directed broadcast packet.

  Workaround: Change the encapsulation to Point-to-Point Protocol (PPP) on the affected serial interfaces.

- CSCtk07240

  Symptoms: When a member-link is removed from an L2 port-channel (A port- channel with switchport configured under it), the traffic stops flowing.

  Conditions: A member link of L2 port-channel passing traffic is removed from the port-channel.

  Workaround: Remove and add the port-channel configurations again.

- CSCtk07369

  Symptoms: The buginf statement “draco2_fastsend: PAK_BUF_ON_OBL processing vlan” appears on the console.

  Conditions: This is displayed in certain cases, such as multicast replication.

  Workaround: There is no workaround.

- CSCtk07632

  Symptoms: Even with the filter option, traffic on a different VLAN on trunk port is getting spanned.

  Conditions: The symptom is observed when the filter vlan specified is not configured on the box.

  Workaround: Configure the vlan on the box, then configure it as SPAN filter vlan.

- CSCtk10279

  Symptoms: A router configured for LISP may crash if it receives a LISP Map- Reply message with an IPv6 RLOC, when IPv6 routing is not enabled.

  Conditions: This symptom occurs when LISP is configured using the **ip lisp {itr | etr | proxy-itr | proxy-etr}** command, the router does not have IPv6 routing configured using the **ipv6 unicast-routing** command.

  Workaround: Enable the IPv6 routing by entering **ipv6 unicast- routing** command.

- CSCtk12243

  Symptoms: Traffic drop may be seen when you enable or disable IGMP snooping through CLI.

  Conditions: This symptom occurs when you enable or disable IGMP Snooping through CLI on a router operating in ingress replication mode only.

  Workaround: Perform a shut/no shut on interfaces after the CLI change.

- CSCtk12252

  Symptoms: Priority 1, valid SONET controller network clock source does not get picked as an active clock source. Instead, the clock remains as FREERUN.

  Conditions: This issue occurs after reloading the router, when there is a valid but not present, priority 2 network clock source.

  Workaround: Perform a shut/no shut on the near-end Prio1 clock source SONET controller.

- CSCtk12608

  Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, 15.1 (2)T and 15.1(01)S and with the following configurations:

  Router 1:

```
interface Ethernet0/0
 ip address 10.0.12.1 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.1 255.255.255.0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.0.1 remote-as 200
 neighbor 172.16.0.1 ebgp-multihop 255
 no auto-summary
!

ip route 0.0.0.0 0.0.0.0 10.10.200.1
ip route 172.16.0.1 255.255.255.255 10.0.12.2
ip route 172.16.0.1 255.255.255.255 10.0.120.2
```

  Router 2:

```
interface Loopback200
 ip address 10.10.200.1 255.255.255.0
!
interface Loopback201
 ip address 172.16.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.12.2 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.2 255.255.255.0
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 10.10.200.0
 neighbor 10.0.12.1 remote-as 100
 neighbor 10.0.12.1 update-source Loopback201
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.12.1
!
```

  Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes”.

- CSCtk12681

  Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

  Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

  Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk12708

  Symptoms: Router crashes when holdover clock source is deleted.

  Conditions: This symptom occurs when the holdover clock source is deleted.

  Workaround: There is no workaround.

- CSCtk13364

  Symptoms: Traffic is blackholed over EVC bridge domain interfaces on the port.

  Conditions: The symptom is observed when a subinterface is deleted and an EVC with the same encapsulation dot1q is created and configured with a bridge domain. The traffic over all the other EVCs on the interface is blackholed.

  Workaround: After the configuration, perform a shut/no shut on the interface.

- CSCtk14941

  Symptoms: Memory leak seen at fh_applet_config_entry_proc.

  Conditions: This symptom occurs when the description keyword is used in an EEM applet.

  Workaround: There is no workaround.

- CSCtk15360

  Symptoms: xauth userid mode http-intercept does not prompt for a password and the Ezvpn session does not come up.

  Conditions: This symptom occurs when the EzVPN client, x-auth is configured as http-intercept.

  Workaround: There is no workaround.

- CSCtk15997

  Symptoms: With interworking VLAN configured for a VFI, the VC is up, but packets do not flow.

  Conditions: This symptom occurs when internetworking VLAN is configured for a VFI.

  Work Around: If possible, do not configure interworking VLAN.

- CSCtk16310

  Symptoms: Timeout failure occurs due to”No socket” error.

  Conditions: This symptom occurs with Udp-jitter packet with VRF.

  Workaround: There is no workaround.

- CSCtk18607

  Symptoms: Router crashes at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Conditions: This symptom occurs at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Workaround: There is no workaround.

- CSCtk18774

  Symptoms: Met cc process does not run.

  Conditions: This symptom occurs with SSO.

  Workaround: Reload the router.

- CSCtk19108

  Symptoms: MVPN traffic failing.

  Conditions: The symptom is observed after an SSO switchover.

Workaround: There is no workaround.

- CSCtk30807

  Symptoms: A box that acts as a DHCP relay/server crashes when the DHCP service is toggled (no service dhcp/service dhcp).

  Conditions: This issue occurs when the box is also configured as ISG.

  Workaround: There is no workaround.

- CSCtk31340

  Symptoms: Cisco route processor (RP) crashes when a port-channel is removed and the member link is defaulted.

  Conditions: When a port-channel is removed (no int port-channel 200) and the member link is defaulted, the port-channel does not automatically remove the configurations on the member link. This crashes the route processor.

  Workaround: There is no workaround.

- CSCtk31401

  Symptoms: A Cisco router crashes when the SSH session from it is exited.

  Conditions: This symptom is observed when “aaa authentication banner” is configured on the router.

  Workaround: There is no workaround.

- CSCtk31515

  Symptoms: Router or line cards crash upon removing VLAN interfaces that are in the OIF list.

  Conditions: The symptom is observed with a series of VLAN interfaces in the access and with the hosts joining groups. Configured is “ssm-mapping”. Access facing line cards can be DFC or CFC.

  Workaround: There is no workaround.

- CSCtk32104

  Symptoms: PPPoE data traffic gets process switched.

  Conditions: This symptom occurs on PPPoE data traffic.

  Workaround: There is no workaround.

- CSCtk32975

  Symptoms: The system crashes.

  Conditions: This symptom occurs when traffic is flowing through the device and fair-queue is configured on ATM PVC.

  Workaround: There is no workaround.

- CSCtk33682

  Symptoms: Storm control stops working.

  Conditions: The symptom is observed after a shut/no shut of the interface on an ES-20.

  Workaround: Remove/add the storm control command on the interface.

- CSCtk33784

  Symptoms: After ISSU from SRE1 to SRE3 seeing CONST_MFIB_LC-SP-6-MET_MCAST_ALLOC_FAILURE for particular group is continuously observed.

  Conditions: This symptom occurs when 10 groups and 32 OIFs are configured.

  Workaround: There is no workaround.

- CSCtk33821

  Symptoms: When polling VidMon metrics through SNMP during MSE intervals, no metric values are returned.

  Conditions: This symptom is observed when the MSE interval is being polled.

  Workaround: There is no workaround.

  Further Problem Description: When we get a MSE interval, the Cisco 7600 does not export the interval data to SNMP. During the MSE interval MRV will be - 100, CMM uses this value to determine the Media stop event. So it is critical to export the MSE interval to SNMP.

- CSCtk34026

  Symptoms: Adding, deleting and re-adding an access subinterface may sometimes cause loss of data path.

  Conditions: The symptom is observed when the configuration sequence involves an add-delete-add sequence.

  Workaround: Create access subinterfaces from scratch.

- CSCtk35650

  Symptoms: Router hangs while generating IP SLA auto schedule with maximum length.

  Conditions: This symptom occurs while generating IP SLA auto schedule.

  Workaround: There is no workaround.

- CSCtk35953

  Symptoms: The dampening information will not be removed even if dampening is unconfigured in VPNv4 AF.

  Conditions: The symptom is observed only if DUT has eBGP-VPNv4 session with a peer and a same-RD import happens on the DUT for the route learned from VPNv4 peer.

  Workaround: A hard reset of the session will remove the dampening information.

- CSCtk36029

  Symptoms: The **match protocol** *icmp* command is not available under class map configuration.

  Conditions: This symptom is seen on the Cisco 7600 with ISG CoPP.

  Workaround: There is no workaround.

- CSCtk36059

  Symptoms: Active SRE does a silent reload while undergoing an ISSU from Cisco IOS Release 12.2(33)SRD to 12.2(33)SRE.

  Conditions: The symptom is observed with scaled configurations.

  Workaround: There is no workaround.

- CSCtk36064

  Symptoms: QoS policy-map with set CoS is applied on switchport interface of ES+ LC in ingress. CoS value is not copied to EXP while adding label in L3VPN/VPLS scenarios.

  Conditions: This symptom is seen on a Cisco 7600 router. ES+ LC, QoS policy- map with set CoS is applied on switchport interface in ingress. CoS value is not copied to EXP while adding label in L3VPN/VPLS scenarios.

  Workaround: There is no workaround.

- CSCtk36090

  Symptoms: Router crashes at draco2_inband_dma_pak after a router reload with the following Cisco IOS Release 12.(33)SRE image:

  s72033-adventerprisek9_dbg-mz.nightly_sre_2010-11-20

  Conditions: The symptom is observed following a router reload.

  Workaround: There is no workaround.

- CSCtk36377

  Symptoms: VRF ping fails for some of the VRFs after deleting and adding MVRFs.

  Conditions: This symptom is seen when adding and deleting MVRFs using a script.

  Workaround: Delete VRF and add it back.

- CSCtk36582

  Symptoms: Accounting on/off messages from AZR clears session from all the sessions in the client pool.

  Conditions: This symptom occurs in the following scenarios:

  1. When there are two AZRs 192.168.100.1 and 192.168.100.2, configure the client in the ISG under radius proxy as “client 192.168.0.0 255.255.0.0”
  2. Account on or off from any of the clients is clearing sessions from both the clients.

  Workaround: Configure clients individually instead of pool configuration.

- CSCtk37068

  Symptoms: Policing is not happening.

  Conditions: This symptom occurs when CoPP is enabled.

  Workaround: There is no workaround.

- CSCtk39301

  Symptoms: Tracebacks such as the following can appear on the RP:

  ```
  %C6K_MPLS_RP-STDBY-3-INFINITE_OCE: In label: 17 Invalid OCE previous oce type: 29 prev
  ptr: 0x5648A2B0, next oce type: 29 next oce ptr: 0x0
  -Traceback= 42319368z 42322E68z 42BA0EF0z 438DCE10z 438D17F0z 405A209Cz 405AC198z
  405A7900z 405EA768z 405EA9E0z 438D06B4z 438D0EE4z 438DAF98z 438FFE40z 422200D0z
  4222123Cz
  ```

  Conditions: The symptom is observed if there are more than eight or 10 ECMP paths for any prefix (i.e.: when there is a loadbalance object in the forwarding OCE chain).

  Workaround: Reduce the number of paths and do a **clear ip route** to re-initiate hardware programming.

- CSCtk47891

  Symptoms: Traffic might be blackholed when LC is reset, if Fast Reroute (FRR) is in use.

  Conditions: This symptom occurs when FRR is configured and it is in active state when the LC is reset.

  Workaround: There is no workaround.

- CSCtk47960

  Symptoms: Large CLNP packets may be dropped when forwarded over SIP- 200/Flexwan2 module. Header Syntax errors may be recorded on receiving host.

Remote side will generate the following:

%CLNS-3-BADPACKET: ISIS: L1 LSP, packet (902) or wire (896) length invalid

Conditions: This symptom is seen on Cisco 7600 switch with SIP-200 line card that is running Cisco IOS 12.2(33)SRD3 and later releases.

Issue is seen when packets larger than 911 bytes are sent (Payload and Header).

Workaround: If CLNS is only used for ISIS neighborships “no isis hello padding” can be configured to establish ISIS neighborship. For the LSP packets, configure lns-mtu 903 under router isis on the Cisco 7600 to make this work.

- CSCtk53130

  Symptoms: You may be unable to configure pseudowire on a virtual PPP interface. The command is rejected with the following error:

  ```
  Incompatible with ipv6 command on Vp1 - command rejected.
  ```

  Conditions: The symptom occurs when an IPv6 address has already been configured on the virtual PPP interface.

  Workaround: There is no workaround.

- CSCtk53463

  Symptoms: For configuring the **shape average** *cir value bc value* command currently across all platforms, *bc value* is limited by 4ms * *cir value*. The 4ms here represents minimum interval time for bursts. ES+ LC however can support interval value that is faster (smaller) than 4ms. This has been expected behavior with exception of ES+ LC.

  Conditions: Currently all platforms restrict interval time for shape from going below 4ms.

  Workaround: There is no workaround.

- CSCtk53657

  Symptoms: WCCP black-holes traffic, if WCCP is disabled on the cache engine.

  Conditions: This symptom occurs when you configure WCCP to use L2 / Mask on the cache engine, leave the router interface up with the cable connected and disable WCCP on the cache engine. When the “SERVICELOST” message appears on the Cisco 7600 and the hardware is still programmed, WCCP blackholes the traffic.

  Workaround: There is no workaround.

- CSCtk53763

  Symptoms: Traffic for some of the SubLSPs is not flowing with P2MP TE or MLDP.

  Conditions: The symptom is observed with LSM and MLDP configurations with multiple SubLSPs.

  Workaround: Use the following command: **clear ip mroute ***.

- CSCtk54318

  Symptoms: VC creation fails on disabling and re-enabling the card for SIP-400 with 4XT3E3 SPA with below messages on console:

  ```
  SLOT 2: %NP_CLIENT-3-INITFAIL: NP Client Initialization Failed - fr_npc_vc_add: vc
  creation failure, np: 0, hwidb: 0x4ACA3500, dlci: 0
  SLOT 2: %NP_CLIENT-3-INITFAIL: NP Client Initialization Failed - fr_npc_vc_add: vc
  creation failure, np: 0, hwidb: 0x4ACA3500, dlci: 1023
  ```

  Condition: This issue is seen when the below commands are executed on a T3 serial interface of the SPA 4XT3E3 configured as DTE with frame relay encapsulation:

  no card type t3 *slot bay*

card type t3 *slot bay*

Then unconfigure and reconfigure frame relay enacapsulation.

Workaround: Reload the SPA.

- CSCtk55382

  Symptoms: A SPA-OC192POS-VSR or SPA-OC192POS-XFP may fail boot diagnostic test.

  Conditions: The symptom is observed when Control Plane Policing (CoPP) is configured on the system. The diagnostic test that fails is the “TestACLPermit” test displayed in “show diagnostic result”. The output of “show module” will indicate a “Minor error” on the subslot.

  Workaround: Before a system reload or module reset, disable the CoPP feature. After the module is booted, CoPP can be enabled again.

- CSCtk57002

  Symptoms: For some PIM-SM groups, met3 entry becomes zero after SSO, when OIF is a port-channel.

  Conditions: This symptom occurs when the OIF is a port-channel

  Workaround: Perform a shut and no shut on the port-channel.

- CSCtk58732

  Symptoms: The router may crash if the following configuration is applied:

```
ip sla 1
icmp-jitter 192.0.2.1 source-ip 192.0.2.2 num-packets 1 interval 10
threshold 1000
timeout 1000
frequency 10

ip sla schedule 1 start-time now life forever

track 1 ip sla 1 reachability
```

  The following error message is displayed:

```
%ALIGN-1-FATAL: Illegal access to a low address 10:49:31 UTC Mon Feb 21 2011 addr=0x1,
pc=0x62D97F30z , ra=0x62D98848z , sp=0x67CE34D0
10:49:31 UTC Mon Feb 21 2011: Address Error (store) exception, CPU signal 10, PC =
0x62DA2E10
```

  Conditions: This symptom occurs in Cisco IOS Release 15.1(3)T release. The router may continually reload following the crash.

  Workaround: Use the ICMP Echo operation instead, as shown below:

```
ip sla 1
icmp-echo 192.0.2.1 source-ip 192.0.2.2
threshold 1000
timeout 1000
frequency 10
```

- CSCtk59347

  Symptoms: CPU is busy and console is locked up for minutes after entering the **clear counter** command.

  Conditions: This symptom occurs with a large scale configuration with hundreds of interfaces and service groups configured on the system.

  Workaround: Instead of clearing all counters of all interfaces, clear the counters of specific interfaces as needed.

- CSCtk59686

  Symptoms: Complete traffic drop occurs.

  Conditions: This symptom occurs when Stateful Switch Over (SSO) occurs and is followed by line card (LC) rest at head-end.

  Workaround: Delete and recreate the tunnel.

- CSCtk61069

  Symptoms: The Cisco IOS router crashes.

  Conditions: This symptom occurs while performing “write memory” or “show running configuration” on the router after configuring “privilege exec level 15 show adjacency”.

  Workaround: Do not set the privilege exec level for any form of the **show adjacency** command.

- CSCtk62247

  Symptoms: IKEv2 session fails to come up with RSA sign authentication.

  Conditions: The symptom is observed with a hierarchical CA server structure.

  Workaround: Use non-hierarchical CA servers.

- CSCtk62950

  Symptom: SSH over IPv6 may crash the router.

  Conditions: This symptom occurs with SSH over IPv6.

  Workaround: There is no workaround.

- CSCtk64538

  Symptoms: The **ip igmp join-group** and **ipv6 mld join- group** commands will not work as expected on Cisco 7600 platform.

  Conditions: This symptom occurs with basic configurations of join group on Cisco 7600 series routers.

  Workaround: Use the **ip igmp static-group** or **ipv6 mld static-group** commands instead.

  Further Problem Description: The **ip igmp join-group** and **ipv6 mld join-group** commands are not normal configurations on the Cisco 7600 router. They cause traffic to be punted to RP CPU and cause problems.

- CSCtk65429

  Symptoms: In an encrypted CE-PE session, traffic sourced by the VRF (for example, ping) works, but traffic coming from MPLS does not reach the crypto map.

  Conditions: This issue is observed in CEF code images, like Cisco IOS Releases 12.4(22)T2, 12.4(24)T4 and 15.1(3)T. This issue is not observed in 12.4 mainline releases, such as Cisco IOS Release 12.4(25d).

  Workaround: There is no workaround.

- CSCtk66080

  Symptoms: LACP/PAGP BPDUs are not tunneled by EVC Xconnect on ES+ and ES20.

  Conditions: This symptom occurs with EVC Xconnect with encapsulation untagged/deault and LACP/PAGP BPDUs ingressing on it.

  Workaround: There is no workaround.

- CSCtk66678

  Symptoms: T1s are down after ISSU CC/SPA upgrade from Cisco IOS XE31 or Cisco IOS XE32 to Cisco IOS XE33.

  Conditions: This symptom is observed only with images created between 10/10/2010 to 12/16/2010.

  Workaround: There is no workaround.

- CSCtk67073

  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipsla.shtml.

- CSCtk67658

  Symptoms: Traceback and infrequent crash of the new active are seen when SSO is performed on a router.

  Conditions: This symptom occurs when SSO is performed on a router.

  Workaround: There is no workaround.

- CSCtk69810

  Symptoms: After performing In Service Software Upgrade (ISSU) from SRE1 CCO image to latest SRE3 on R4, the rwindex is set to invalid in the “catch all” entry. Because of this, the PIM neighbor on MDT is not up and the traffic does flow.

  Conditions: This symptom occurs after performing ISSU from SRE1 CCO image to latest SRE3 on R4.

  Workaround: Delete MDT and add it under VRF.

- CSCtk74970

  Symptoms: TE autoroute announced tunnel is not installed in the routing table.

  Conditions: The symptom is observed if you configure TE with one hop-LDP and then unconfigure. Then configure TE with one hop with non-LDP. The TE autoroute announced tunnel is not installed in the routing table.

  Workaround: Configure “no ip routing protocol purge interface”.

- CSCtk76190

  Symptoms: The RSP/SUP fails to switchover automatically when the “TestSPRPInbandPing” fails for more than 10 instances.

  Conditions: The symptom is observed when the “TestSPRPInbandPing” fails for more than 10 instances.

  Workaround: There is no workaround.

- CSCtk83760

  Symptoms: Met updates from SUP are reaching Cisco 67xx DFC cards.

  Conditions: This symptom is observed during OIF churn. This is not reproduced locally, and the fix is put in as a sort of preventive mechanism.

  Workaround: There is no workaround.

- CSCtk84116

  Symptoms: A GETVPN ks crash may occur when split-and-merge is happening between the key servers.

  Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

  Workaround: There is no workaround.

- CSCtk95742

  Symptoms: Traffic does not flow from EVC-BD.

  Conditions: This symptom occurs with port-channel EVC-BD configuratIon with ES20 memberlinks. This symptom occurs if ES20 LC is replaced with the ES+ LC and added the same port as ES20 to the port-channel.

  Workaround: Remove and add the EVC.

- CSCtk95992

  Symptoms: DLSw circuits to not come up when using peer-on-demand peers.

  Conditions: This symptom occurs when DLSw uses UDP for circuit setup.

  Workaround: Configure the command **dlsw udp-disable**.

  Further Problem Description: This symptom occurs in the following (and later) Cisco IOS Releases:12.4(15)T14, 12.4(24)T4, 15.0(1)M3, 15.1(1)S, 15.1(2)T, 12.2(33)SXI4, and 12.2(33)SXI4a.

- CSCtk98030

  Symptoms: After replacing an ES20 line card with an ES+ line card or vice versa in the same slot, some service groups reject new members to join if the old line card had ethernet service instances in these groups. Similarly, a named EVC rejects new ethernet service instances if it had association with the old line card. The named EVC cannot be deleted, complaining that it still has service instances.

  Conditions: The symptom is observed if an ES20 line card has been replaced with an ES+ line card or vice versa in the same slot. The old line card had ethernet service instance members in some service groups and/or named EVCs. The old associations between ethernet service instances and service groups or named EVCs are not cleaned up properly, blocking new association to these groups and EVCs.

  Workaround: Configure new service groups and named EVCs with same configuration as the problematic ones. Abandon the use of the old groups and EVCs. Assign ethernet service instances from the new line card to the new groups and EVCs.

- CSCtk98726

  Symptoms: ANCP shaper fails to be applied on ATM VC.

  Conditions: This symptom occurs after clearing and re-establishing the PPPoE session.

  Workaround: There is no workaround.

- CSCtl04285

  Symptoms: After provisioning a new BGP session, a BGP route reflector may not advertise IPv4 MDT routes to PEs.

  Conditions: The symptom is observed on a router running BGP, configured with new style IPv4 MDT and peering with an old style IPv4 MDT peer. Affected releases are 12.2(33)SRE, 15.0M, 12.2(33)XNE and later releases.

  Workaround: No workaround.

- CSCtl05684

  Symptoms: Xauth user information remains in “show crypto session summary” output.

  Conditions: This symptom is observed when running EzVPN and if Xauth is performed by different username during P1 rekey.

  Workaround: Use save-password feature (without interactive Xauth mode) to avoid sending the different username and password during P1 rekey.

- CSCtl05785

  Symptoms: Connectivity is broken on Cisco 7600 L3 subinterfaces upon reconfiguration of the assigned VRF. Directly connected devices are no longer reachable. Input path is broken (packets are seen in netdr but do not reach the RP).

  Conditions: This symptom is observed on Cisco 7600 routers that are running Cisco IOS Release 12.2(33)SRE2. This issue is seen on Sip-400 subinterfaces.

  Workaround: Reload the router.

- CSCtl05926

  Symptoms: Packets exceeding the MTU size are dropped with the following error messages:

  *Dec 17 08:24:39.795: %CONTROLLER-3-TOOBIG: An attempt made to send giant packet on GigabitEthernet7/3/1 (1491 bytes from 10010046, max allowed 1476

  Conditions: This symptom occurs if the outgoing interface is on SIP400.

  Workaround: There is no Workaround.

- CSCtl05979

  Symptoms: In SSO mode, PPPoE sessions with PAC2 ISG service are replicated to Standby RP, with policy-maps missing on Standby RP. PAC2 service should poison the PPPoE session.

  Conditions: This symptom is observed in SSO mode, when PPPoE sessions with PAC2 ISG service are established.

  Workaround: Use dummy ISG service applied from RaBaPol to force poisoning.

- CSCtl07955

  Symptoms: BFD neighbor goes down and does not come up again when an unrelated LC is powered down by using **no power enable module X** command.

  Conditions: This symptom occurs when an unrelated LC is powered down.

  Workaround: There is no workaround.

- CSCtl08014

  Symptoms: Router crashes with memory corruption symptoms.

  Conditions: This symptom occurs when performing switchover or Online Insertion and Removal (OIR), while MLP sessions are initiating.

  Workaround: There is no workaround.

- CSCtl08594

  Symptoms: After upgrading to Cisco IOS Release 15.1(3)T, routers are not able to connect to the EZVPN server anymore. ISAKMP fails to find the key.

  Conditions: This symptom occurs with the following conditions: - DHCP is configured on outside interface - Outside interface is FastEthernet. This symptom does not occur if the outside interface is VLAN. This symptom is not seen in Cisco IOS Release 15.1(2)T1

Workaround: Downgrade to 15.1(2)T1, use VLAN interface or remove “ip route 0.0.0.0 0.0.0.0 fastethernet4 dhcp” statement from the config and reload the router.

- CSCtl10395

  Symptoms: Control Plane Policing (CoPP) stops dropping packets in hardware on a Cisco 7600 series router after double switchover.

  Conditions: This symptom occurs on the Cisco 7600 platform when CoPP is configured on the router and SSO (HA Switchover) is done twice.

  Workaround: Remove and reconfigure the CoPP.

- CSCtl18652

  Symptoms: After replacing an ES20 with an ES+ line card on the same slot, or vice versa, adding ethernet service instance members from the new line card to an existing service group that was associated with the old line card may cause a reload of the standby RP in SSO mode. This is due to stale configuration on the standby RP.

  Conditions: An ES20 line card has been replaced by a different type of line card or vice versa, on the same slot. New members are assigned to a service group that had members from the old line card. There is a standby RP in SSO mode.

  Workaround: Create a new service group with the same configuration as the existing group and assign new members to the new group. Abandon the use of the old group.

- CSCtl19347

  Symptoms: On configuring additional bundles, LC crashes. This occurs with SIP- 400 when copying the dLFI configurations from a disk to the running configuration to bundle up.

  Conditions: This symptom occurs when copying the dLFI configurations from a disk to the running configuration to bundle up.

  Workaround: There is no workaround.

- CSCtl20993

  Symptoms: Router crashes during IPsec rekey.

  Conditions: The conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtl21884

  Symptoms: When enabling auto-summary under the BGP process, a BGP withdraw update is not sent even though the static route goes down.

  Conditions: The symptom is observed under the following conditions:

  - Enable auto-summary under the BGP process. - Static route is brought into the BGP table via the **network** command.

  Workaround: Use **clear ip bgp *** or disable **auto-summary** under the BGP process.

- CSCtl22871

  Symptoms: CoS value (applied from setcos policy) does not get copied to EXP while adding a label to the VPLS case, VPLS cfgd on EVC BD Vlan.

  Conditions: This symptom occurs on ES+ and QoS policy-map when set CoS is applied on EVC BD with VPLS configured on BD Vlan.

  Workaround: There is no workaround.

- CSCtl23348

  Symptoms: IOS crashes on OSPFv3 code.

  Conditions: This symptom occurs when the redistribution statement and the redistributed protocol are deleted simultaneously.

  Following is an example of a CLI that causes the IOS to crash, if it is copied and pasted:

```
ipv6 router ospf 1
no redistribute bgp 1
!
no router bgp 1
```

  Workaround: Do not delete the routing process at the same time as redistribution.

- CSCtl41921

  Symptoms: There is a traffic duplication.

  Conditions: This symptom occurs with bootup with scale having 2000 sLSPs.

  Workaround: Do a shut/no shut on the tunnel.

- CSCtl43925

  Symptoms: Including a P2P GRE tunnel in VRF on the access side, causes the multicast traffic for the VRF to be dropped.

  Conditions: After removing a GRE header and encapsulation change from Tunnel VLAN to QoS vlan, the next entry to be hit has incoming vlan as VPN QoS vlan. This symptom occurs only when CR=1. However, when the tunnels are brought up in vrf, CR=0 gets programmed, causing packets to get bridged and dropped.

  Workaround: Reload the LC or router in SM mode. Wait for a little while and start traffic again to trigger a re-install.

- CSCtl46703

  Symptoms: T1/E1 tributary on Prowler SPA stays down occasionally after LC/SPA is reloaded.

  Conditions: This symptom occurs after LC/SPA is reloaded.

  Workaround: Reconfigure clock configuration (e.g. vtg 1 t1 1 clock source line/internal) on the affected T1/E1.

- CSCtl46903

  Symptoms: VLAN mapping or translation feature does not work on ES+, when the port is configured as L2 switchport.

  Conditions: This symptom occurs when the port is configured on L2 switchport.

  Workaround: Configure the feature under EVC framework or L2 switchport on LAN cards.

- CSCtl50815

  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

```
%OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
Non-OER, OOP Reason <reason>
```

  Conditions: The symptom is observed under the following conditions:

  - Use ECMP.
  - Use **mode monitor passive**.

Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl50930

  Symptoms: For some SIP messages like OPTION, SBC asserts failure when called through VRF.

  Conditions: This symptom occurs on 1001, 1002, or 1004 non-redundant modes.

  Workaround: Configure the redundant mode SSO.

- CSCtl54033

  Symptoms: Resignaling sub-LSPs for P2MP TE tunnels may take up to 10 seconds, after the sub-LSP has been pruned or torn down.

  Conditions: This symptom occurs when a P2MP TE tunnel is configured to request FRR protection, but for the physical link down the path on the tunnel headend, there is no backup tunnel configured at the failure point (TE tunnel headend) to protect the sub-LSP. The TE tunnel headend will take 10 seconds for sub-LSP resignaling.

  Workaround: Configure FRR backup tunnels at TE tunnel headend to provide link protection for P2MP TE tunnels for the physical link that is connected to the TE tunnel headend in the TE tunnel path.

- CSCtl54415

  Symptoms: A Cisco router or switch may reload.

  Conditions: This symptom is experienced on multiple platforms when single- connection timeout is configured under an aaa group server, and there is no TACACS key configured:

```
aaa group server tacacs+ <NAME>
 server-private x.x.x.x single-connection timeout 2
 server-private x.x.x.x single-connection timeout 2
 ip tacacs source-interface Loopback0
(no tacacs-server key configured)
```

  Workaround: Either configure the correct matching key or do not configure single-connection timeout.

- CSCtl55828

  Symptoms: LDP/OSPF PDUs get dropped when line rate traffic is running on the Interface in case the link is over subscribed.

  Conditions: This symptom occurs with the following Hardware and software:

  Hardware - ES+ LC

  Software - Cisco IOS Releases 15.0(1)S, 15.0(1.1)S, 15.1(1)S Link over subscription, output drops at the MPLS interface.

  Workaround: There is no workaround.

- CSCtl57055

  Symptoms: A router may unexpectedly reload when the rttMonStatsTotalsEntry MIB is polled by SNMP.

  Conditions: The symptom is observed on a router that is running a Cisco IOS 15.1T release, is configured for SNMP polling, and when the rttMonStatsTotalsEntry is polled with an IP SLA probe configured.

  Workaround 1: Configure NMS to stop polling the rttMonStatsTotalsEntry or create a view and block the MIB on the router.

  Workaround 2: The issue only affects Cisco IOS 15.1T releases, so use a Cisco IOS 15.0(1)M rebuild or earlier.

- CSCtl58005

  Symptoms: Accounting delay start is sent before any NCP has been negotiated, with “aaa accounting delay-start” configured. According to PRD, accounting start should not be sent until first NCP has been negotiated.

  Conditions: This symptom occurs when “aaa accounting delay-start” is configured.

  Workaround: There is no workaround.

- CSCtl67195

  Symptoms: The following three BGP debug commands are not allowed to enable:

  debug ip bgp vpnv4 unicast debug ip bgp vpnv6 unicast debug ip bgp ipv6 unicast

  Conditions: The symptom is observed with the above BGP debug commands.

  Workaround: There is no workaround.

- CSCtl69609

  Symptoms: When bringing down the shortest route, traffic blackholing occurs in MLDP on one of the OIFs.

  Conditions: This condition occurs in MLDP and branch point combination.

  Workaround: There is no workaround.

- CSCtl82922

  Symptoms: Fast memory leak occurs on standby Switch Processor (SP)/SP or DFC in the “mfib-const-lc” process. Once this process depletes memory, the starving system generates “MALLOC” errors for any other processes that request memory at that time. Eventually, standby SP crashes and the system operation recovers.

  “Holding” number in standby SP can grow with the speed of 60kB/s:

  #remote command standby-sp show proc mem | i mfib-const-lc|Holding

  PID TTY Allocated Freed Holding Getbufs Retbufs Process

  281 0 106300144 4061004 103339316 0 0 mfib-const-lc

  Pr

  Conditions: This symptom is seen with the multicast stream timeout & restart in an MVPN environment. Stream S,G entry might not be installed in HW, and following MFIB Platform flags error might be seen for this stream along with the memory leak:

  #show ip mfib vrf <vrf_name> verbose | i HW_ERR

  (176.2.76.2,229.2.76.2) Flags: ET K DDE

Platform Flags: NP RETRY RECOVERY HW_ERR HAL:5

Workaround: There is no workaround.

- CSCtl83736

  Symptoms: Each V4 session set-up leaks approximately 100 bytes. Each V6 session set-up leaks approximately 112 bytes.

  The following command can be used to verify the above symptom:

  show platform software memory messaging ios rp active | inc st_sb_cfg

  Note that the "diff:" number increases continuously.

  Conditions: This symptom occurs in IP sessions.

  Workaround: There is no workaround.

- CSCtl85926

  Symptom: Output drops are observed when traffic is sent beyond 64k rate with single E1 when E1 is configured as unframed. Issue is seen rarely with using time-slots 1-31. After LC OIR, this symptom is not observed. If the channel is removed and attached, this issue reappears.

  Conditions: This symptom occurs on the following hardware and software:

  Hardware: SIP: 7600-SIP-400, SPA: 7/1 8xCHT1/E1 SPA

  Software: Cisco IOS c7600rsp72043-adventerprisek9-mz.122-33.SRD or later.

  Workaround:

  1. Configure a service policy like the following:

     policy-map test1

     class class-default

     queue-limit 386 ((this number is a interface bandwidth(in kbps)*1000 / (8 * 250 * 2) value for the

     correct behavior.). for T1 (1544, it will be 1544 * 1000 / (8*250*2) = 386). for Full E1, it will be 496.
  2. Reload line card.

- CSCtl88066

  Symptoms: A router reloads (seen with a Cisco ASR 1000 Series Aggregation Services router) or produces a spurious memory access (seen with most other platforms).

  Conditions: The symptom is observed when BGP is configured and you issue one of the following commands:

  show ip bgp all attr nexthop

  show ip bgp all attr nexthop rib-filter

  Workaround: Do not issue either of these commands with the **all** keyword. Instead, issue the address-family specific version of the command for the address family you are interested in.

  For example, the following are safe:

  show ip bgp ipv4 unicast attr nexthop

  show ip bgp attr nexthop

  show ip bgp vpnv4 vrf *vrfname* **attr nexthop**

Further Problem Description: While the **show ip bgp all attr nexthop** has never done anything that **show ip bgp attr nexthop** did not do, the reload bug was introduced during the development of multi-topology routing. All versions of Cisco IOS which include multi-topology routing or which are derived from versions which included multi-topology routing, and where this fix is not integrated are impacted.

The fix prevents the issuing of commands beginning with **show ip bgp all attr**.

- CSCtl90890

  Symptoms: With pim-bidir in MVPN core, MVPN traffic might not flow if a PE is also a rendezvous point (RP) for the pim-bidir in core.

  Conditions: This symptom occurs with pim-bidir in MVPN core.

  Workaround: Use non pim-bidir modes.

- CSCtl93514

  Symptoms: QoS configurations do not get applied on the interfaces when the router is upgraded from ES20 to ES+.

  Conditions: This issue happens when the ES20 is replaced with ES+. Remove the ES20 LC and insert the ES+ LC on the same slot.

  Workaround: Remove all QoS policies applied on the ES20 interfaces. Insert ES+ and reapply all QoS policies once the ES+ interfaces are up.

- CSCtl97648

  Symptoms: Tab completion does not work.

  Conditions: This symptom occurs when IOS.sh is not enabled.

  Workaround: Enable Cisco IOS Shell (IOS.sh) using “term shell”.

- CSCtl98132

  Symptoms: XDR CPU hog may cause system crash.

  Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.

  Workaround: There is no workaround.

  Further Problem Description: The crash can be avoided if the system has no double failure.

- CSCtl98270

  Symptoms: Changing the VC hold-queue under the PVC on a WIC-1ADSL card is not reflected correctly in the **show hqf interface** output.

  Conditions: The symptom is observed in Cisco IOS 15.1(2)T2 Release and later releases.

  Workaround: Execute a shut/no shut to fix the issue.

- CSCtn01832

  Symptoms: The following command sequence crashes the router at check syntax mode:

  config check syntax route-map hello match local-preference no match local-preference

  Conditions: The symptom is observed with the commands above.

  Workaround: There is no workaround.

- CSCtn10922

  Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic and in some cases may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.

  Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.

  Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.

- CSCtn16899

  Symptoms: PIM neighborship is lost between source node and receiver nodes.

  Conditions: This issue is seen when TE FRR is configured for the link between source node and root node and after FRR cutover is done.

  Workaround: Shut and no shut the egress interface of the backup tunnel on the root node.

- CSCtn17267

  Symptoms: Broadband call admission control (CAC) is not working.

  Conditions: This symptom occurs under the following conditions:

  1. DHCP initiated sessions.
  2. PPPoE sessions on an interface where IP session configurations are present.

  Workaround: There is no workaround.

- CSCtn25100

  Symptoms: PPP sessions take longer to come up.

  Conditions: This symptom occurs in all conditions.

  Workaround: There is no workaround.

- CSCtn38711

  Symptoms: A router crashes.

  Conditions: This symptom occurs during SSO on a heavily loaded Cisco 7600 router.

  Workaround: There is no workaround.

- CSCtn41245

  Symptoms: Subinterface ingress stats do not work for access subinterfaces.

  Conditions: This symptom is observed only for the access subinterface. Interface stats and regular subinterface stats work as expected.

  Workaround: There is no workaround.

- CSCtn41662

  Symptoms: Standby RP crashes sometimes when policymap configuration is done. This crash happens randomly with the following crash decode:

```
0xA65C01C:qm_make_final_vmr(0xa65bf14)+0x108
0xA64799C:qm_send_merge_replace_request(0xa647834)+0x168
0xA6471B0:qm_tm_merge_replace(0xa646ee4)+0x2cc
0xA63B3FC:qm_tcam_modify_service_policy(0xa63adbc)+0x640
0xA63A8AC:qm_process_mqc_event_hdlr(0xa63a51c)+0x390
0xA63BE7C:qm_process_events_q_hdlr(0xa63bad0)+0x3ac
0xA63CAA0:qm_process(0xa63c9cc)+0xd4
```

Conditions: This symptom occurs randomly when policymap, class-map is modified, which is applied on different interfaces. This does not happen consistently.

Workaround: There is no workaround.

- CSCtn60353

  Symptoms: In sub-package ISSU, some OM objects on standby RP may be missing.

  Conditions: This symptom occurs with ISSU between two releases and new release that adds new TDL message type.

  Workaround: Force a reload of the standby RP before a final RP switchover.

- CSCtn83293

  Symptoms: Out-to-in packets may drop because the ARP reply is missing from NAT router.

  Conditions: This symptom may happen under the following conditions:

  1. Inside global address is a subnet of the NAT outside interface.
  2. When the translation is created off of VRF NAT mappings.

  Workaround: Avoid using inside global address in VRF NAT static mapping or in the address pool of a dynamic mapping that belongs to an interface subnet.

Caveats for Cisco IOS Release 15.1S

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section consists of the following subsections:

- Resolved Caveats—Cisco IOS Release 15.1(1)S2, page 297
- Resolved Caveats—Cisco IOS Release 15.1(1)S1, page 307
- Open Caveats—Cisco IOS Release 15.1(1)S, page 335

Resolved Caveats—Cisco IOS Release 15.1(1)S2

Cisco IOS Release 15.1(1)S2 is a rebuild release for Cisco IOS Release 15.1(1)S. The caveats in this section are resolved in Cisco IOS Release 15.1(1)S2 but may be open in previous Cisco IOS releases.

- CSCsl18054

  Symptoms: A local user created with a one-time keyword is removed after unsuccessful login attempts. A one-time user should be removed automatically after the first successful login, not after failed logins.

  Symptoms: Occurs on a router running Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCtg85402

  Symptoms: Multicast packet software switching MFIB platform flags “NP RETRY RECOVERY HW_ERR HAL” after SSO/ISSU.

  Conditions: Issue seen only with CFC cards and not with DFC. Specific to mVPN configuration with egress CFC cards. Issue seen under rare condition with SSO/ISSU.

  Workaround: Remove and add Default MDT configuration.

- CSCth84714

  Symptoms: With scaled number of MLP bundles on Sip200 with DLFI enabled, the sip200 crashes.

  Conditions: This symptom occurs with the following conditions: 1. Reload the SPA having MLP bundles. 2. Shut / No shut the controller. 3. Flap the links by any other means.

Workaround: The issue is not seen without high traffic and without LFI enabled.

- CSCti66454

  Symptoms: Router crashes when using the **show crypto session detail** command after using the **clear crypto session** command.

  Conditions: This symptom is observed when the router is running any form of tunnel protection, and SAs have been cleared. Then the user executes a **show** command.

  Workaround: Wait a few moments (30 seconds) between the **show** command and the **clear** command.

- CSCti81177

  Symptoms: Features like Videomon do not work on routed port.

  Conditions: This symptom occurs when an interface is configured as a switchport and reconfigured to routed Port.

  Workaround: Reload the line card.

- CSCti92812

  Symptoms: After physical interface flap, GRE tunnel for VRF does not come up correctly.

  Conditions: This symptom occurs when GRE tunnel is configured for default (global) routing table.

  Workaround: There is no workaround.

- CSCtj30238

  Symptoms: WRED counters are wrongly updated. The default counter should be 0, but the counter is wrongly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there are no traffic matches in the class.

  Conditions: This issue is seen on the Cisco 7600 router with ES+ line card only. The Es+ line card does not support per WRED class based counters. There was a recent breakage due to the Transmit packets/bytes column that started showing up for the Es+ line card. This is wrong. As ES+ writes same value to WRED transmit count (not the per subclass base count, but total count), this value does not make sense.

  Workaround: Do not use WRED subclass Transmit packets/bytes counters for ES+ line card on the Cisco 7600 router.

- CSCtj56142

  Symptoms: ISG uses dummy user-name within EAP re-authentication related access-requests as the session identifier.

  Conditions: The symptom is observed during EAP re-authentications and likely after CoA-based service activation on an EAP-authenticated session. This happens only when the EAP access-requests carry a dummy user-name and access- accept does not have the correct username.

  Workaround: There is no workaround.

- CSCtj58405

  Symptoms: Full multicast traffic is not sent from the source PE.

  Conditions: The issue is observed only with ECMP links and with a higher scale (above 75 MVRF and 100 mroutes per VRF) for default MDTS. It is seen when one of the ECMP links which was down earlier, comes up. If all the ECMP links are already up, then the issue is not seen.

  Workaround: Clear the IP mroute using **clear ip mroute** command.

- CSCtj61748

  Symptom: Service activation fails occasionally.

  Conditions: This symptom occurs with multiple services in the session authentication or authorization response that are configured in the same service-group.

  Workaround: Remove fields that are related to “service-group” or “service- type” in service definitions.

- CSCtj79769

  Symptoms: LC crashes.

  Conditions: When disabling MLD snooping on an interface or disabling IPV6 multicast in general.

  Workaround: There is no workaround.

- CSCtj85333

  Symptoms: System may crash when config-template contains the config commands “ip ips signature-category” and when the template is downloaded to the router using the CNS config feature commands “cns config retrieve” exec command, “cns config initial” config command. This symptom may also occur when the config template is downloaded to the router using the device Config-Update operation of Config Engine.

  Conditions: This is normal mode operation, but this symptom will occur when such CNS feature is used.

  Workaround: There is no workaround.

- CSCtj87846

  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

  Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

  Workaround: Do Shut/no shut on PfR master or PfR border.

- CSCtj91764

  Symptoms: A UC560/UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to CPU.

  Conditions: The crash happens during a complete SNMP MIB walk.

  Workaround: The CISCO-CALL-APPLICATION-MIB can be excluded via configuration.

- CSCtj94510

  Symptoms: When sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and 4 SA dual per session, a crash happens on Crypto_SS_process.

  Conditions: This symptom occurs when sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and four SA dual per session.

  Workaround: There is no workaround.

- CSCtj99431

  Symptoms: Session have shared key mismatch between ISG and Radius client. Non- subnet client (Best Match) does get preference over subnet client.

  Conditions: This symptom is observed on a Cisco ASR1000 series router when it functions as an ISG Radius-Proxy router.

  Workaround: Remove “ignore server key” from “aaa server radius dynamic-author”.

- CSCtk18607

  Symptoms: Router crashes at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Conditions: This symptom occurs at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Workaround: There is no workaround.

- CSCtk31401

  Symptoms: A Cisco router crashes when the SSH session from it is exited.

  Conditions: This symptom is observed when “aaa authentication banner” is configured on the router.

  Workaround: There is no workaround.

- CSCtk32104

  Symptoms: PPPoE data traffic gets process switched.

  Conditions: This symptom occurs on PPPoE data traffic.

  Workaround: There is no workaround.

- CSCtk35953

  Symptoms: The dampening information will not be removed even if dampening is unconfigured in VPNv4 AF.

  Conditions: This symptom is observed only if DUT has an eBGP-VPNv4 session with a peer and a same-RD import happens on the DUT for the route learned from the VPNv4 peer.

  Workaround: A hard reset of the session will remove the dampening information.

- CSCtk36582

  Symptoms: Accounting on/off messages from AZR clears session from all the sessions in the client pool.

  Conditions: This symptom occurs in the following scenarios: 1) When there are two AZRs, 192.168.100.1 and 192.168.100.2, and you configure the client in the ISG under radius proxy as “client 192.168.0.0 255.255.0.0”. 2) Accounting on or off from any of the clients is clearing sessions from both the clients.

  Workaround: Configure clients individually instead of pool configuration.

- CSCtk53657

  Symptoms: WCCP black-holes traffic, if WCCP is disabled on the cache engine.

  Conditions: This symptom occurs when you configure WCCP to use L2 / Mask on the cache engine, leave the router interface up with the cable connected and disable WCCP on the cache engine. When the “SERVICELOST” message appears on the Cisco 7600 and the hardware is still programmed, WCCP blackholes the traffic.

  Workaround: There is no workaround.

- CSCtk61069

  Symptoms: The Cisco IOS router crashes.

  Conditions: This symptom occurs while performing “write memory” or “show running configuration” on the router after configuring “privilege exec level 15 show adjacency”.

  Workaround: Do not set the privilege exec level for any form of the **show adjacency** command.

- CSCtk62950

  Symptom: SSH over IPv6 may crash the router.

Conditions: This symptom occurs with SSH over IPv6.

Workaround: There is no workaround.

- CSCtk66080

  Symptoms: LACP/PAGP BPDUs are not tunneled by EVC Xconnect on ES+ and ES20.

  Conditions: This symptom occurs with EVC Xconnect with encapsulation untagged/deault and LACP/PAGP BPDUs ingressing on it.

  Workaround: There is no workaround.

- CSCtk67455

  Symptoms: The fragmented traffic is dropped when the LOG option is set for IPv6 ACLs on 3CXL PFC-based supervisors.

  Conditions: This symptom is observed when the LOG keyword is specified for IPv6 ACLs on 3CXL PFC mode.

  Workaround: There is no workaround.

- CSCtk67768

  Symptoms: RP crash is observed in DHCPD receive process.

  Conditions: This symptom occurs on Cisco IOS DHCP server that is used on Cisco IOS ASR routers and acting as ISG.

  Workaround: There is no workaround.

- CSCtk68109

  Symptoms: A Cisco ASR 1000 router reloads when running CVP survivability TCL.

  Conditions: This symptom is observed when “pass-thru content sdp” is used in the Cisco ASR 1000 router configuration.

  Workaround: Use “codec transparent” instead of “pass-thru content sdp”.

- CSCtk69114

  Symptoms: RP resets while doing ESP reload with crypto configuration.

  Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.

  Workaround: There is no workaround.

- CSCtk95106

  Symptoms: CPU 1 of SPA 8XT1E1 goes into a forced reload followed by a software forced reload of line card SIP-200 when a multilink PPP with interleave enabled having fragment size 42 is disabled and enabled. One member of the link is removed.

  Conditions: This issue is noticed when traffic is pumped onto the DUT from remote end. Size could be as low as 800 bytes. Interleave is disabled and enabled on the mulilink interface, and one of the members of the MP is detached from the bundle using the **no ppp multlink group** <> command.

  Workaround: There is no workaround.

- CSCtk95742

  Symptoms: Traffic does not flow from EVC-BD.

  Conditions: This symptom occurs with port-channel EVC-BD configuration with ES20 memberlinks. This symptom occurs if ES20 LC is replaced with the ES+ LC and added the same port as ES20 to the port-channel.

Workaround: Remove and add the EVC.

- CSCtl00127

  Symptoms: The output of **show ip int** command does not indicate whether the "ip security ignore-cipso" option is configured and/or operational.

  Conditions: Configure "ip security ignore-cipso" on an interface. This was not indicated on the **show ip interface** *interface name* command output of that interface.

  This symptom is observed on the following devices:

  - Cisco IOS Catalyst 6500 router that is running Cisco IOS Releases 12.2(33)SXH and 12.2(33)SXI.
  - Cisco IOS Catalyst 7600 router that is running Cisco IOS Releases 12.2(33)SRA7, 12.2(33)SRB, 12.2(33)SRC, 12.2(33)SRD, and 12.2(33)SRE.
  - Cisco IOS Catalyst 4500 router that is running Cisco IOS Release 12.2(40)SG.

  The output is indicated correctly when it is enabled on Cisco IOS Release 12.2(18)SXF17a.

  Workaround: There is no workaround.

- CSCtl05785

  Symptoms: Connectivity is broken on Cisco 7600 L3 subinterfaces upon reconfiguration of the assigned VRF. Directly connected devices are no longer reachable. Input path is broken (packets are seen in netdr but do not reach the RP).

  Conditions: This symptom is observed on Cisco 7600 routers that are running Cisco IOS Release 12.2(33)SRE2. This issue is seen on Sip-400 subinterfaces.

  Workaround: Reload the router.

- CSCtn07415

  Symptoms: Crash is observed at crypto_map_get_map_method_bitmask while reconfiguring IPSec with 1300 GRE tunnel interfaces, with old configurations still present.

  Conditions: This symptom occurs with IPSec with GRE tunnel interfaces.

  Workaround: There is no workaround.

- CSCtl07955

  Symptoms: BFD neighbor goes down and does not come up again when an unrelated LC is powered down by using the **no power enable module X** command.

  Conditions: This symptom occurs when an unrelated LC is powered down.

  Workaround: There is no workaround.

- CSCtl22871

  Symptoms: CoS value (applied from setcos policy) does not get copied to EXP while adding a label to the VPLS case, VPLS cfgd on EVC BD Vlan.

  Conditions: This symptom occurs on ES+ and QoS policy-map when set CoS is applied on EVC BD with VPLS configured on BD Vlan.

  Workaround: There is no workaround.

- CSCtl71478

  Symptoms: In an HA system, the following error message is displayed on the standby RP and LC: "OCE-DFC4-3-GENERAL: MPLS lookup unexpected".

Conditions: This symptom is observed on standby/LC modules when you bring up both the RP and standby/LC routers with or without any configuration.

Workaround: There is no workaround.

- CSCtl79512

  Symptoms: The default BRR of the L2 node is configured as 255.

  Conditions: This symptom is observed when applying port-shaper on port channel main interface. Configure EVCs on port channel with two EVCs having HQoS policy-map and with two other EVCs having service-group with HQoS policy- map.

  Workaround: There is no workaround.

- CSCtl90890

  Symptoms: With pim-bidir in MVPN core, MVPN traffic might not flow if a PE is also a rendezvous point (RP) for the pim-bidir in core.

  Conditions: This symptom occurs with pim-bidir in MVPN core.

  Workaround: Use non pim-bidir modes.

- CSCtl98132

  Symptoms: XDR CPU hog may cause system crash.

  Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.

  Workaround: There is no workaround.

  Further Problem Description: The crash can be avoided if the system has no double failure.

- CSCtn10922

  Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic and in some cases may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.

  Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.

  Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.

- CSCtn15877

  Symptoms: For access subinterface, ingress stats on the **show interface** *interface type number* **stats** command will not work.

  Conditions: The issue is seen only on access subinterface.

  Workaround: There is no workaround.

- CSCtn16840

  Symptoms: VPLS imposition traffic does not go through for some of the VCs when the core is a port channel on ES20.

  Conditions: This symptom is observed when core facing is a port channel on ES20.

  Workaround: Do a shut/no shut on the port channel.

- CSCtn16899

  Symptoms: PIM neighborship is lost between source node and receiver nodes.

Conditions: This issue is seen when TE FRR is configured for the link between source node and root node and after FRR cutover is done.

Workaround: Shut and no shut the egress interface of the backup tunnel on the root node.

- CSCtn17267

  Symptoms: Broadband call admission control (CAC) is not working.

  Conditions: This symptom occurs under the following conditions:

  1. DHCP initiated sessions.
  2. PPPoE sessions on an interface where IP session configurations are present.

  Workaround: There is no workaround.

- CSCtn17680

  Symptoms: When performing an OIR on a Cisco WS-X6708 module, the router may crash. When inserting the card, the following message is displayed:

  ```
  %EARL_L2_ASIC-SP-4-DBUS_HDR_ERR: EARL L2 ASIC #0: Dbus Hdr. Error occurred. Ctrl1
  0xB88D0E3D
  ```

  Then, the following message is displayed:

  ```
  %CPU_MONITOR-SP-2-NOT_RUNNING: CPU_MONITOR messages have not been sent for 60 seconds
  [*Sched* 41%/0% (00:01:00.244 99%/99%)]
  ```

  Finally, a timeout occurs, followed by the crash:

  ```
  %CPU_MONITOR-SP-3-TIMED_OUT: CPU_MONITOR messages have failed, resetting system
  (self) [5/0]
  ```

  Conditions: This symptom is observed on Cisco IOS 7600 series routers with either a single or dual RSP720 supervisor. In the case of dual supervisors, both supervisors crash. The cause of the crash is unknown. However, after the router reloads, the affected module has been installed again without further issue in a couple of instances.

  Workaround: There is no workaround.

- CSCtn19444

  Symptoms: mLACP memberlinks may be bundled on an isolated PoA with a core failure, resulting in both PoAs becoming active.

  Conditions: This symptom occurs when running mLACP. The ICRM connection between the PoAs is lost. The PoAs are in a split brain situation and both PoAs attempt to become active. If the interface configured as “backbone interface” goes down on one of the PoAs, that PoA may keep the port-channel memberlinks bundled. The end result is that both PoAs are in mLACP active state, and both have their port-channel memberlinks bundled. After the fix the PoA with the backbone interface failure will unbundle its port-channel memberlinks, leaving only one PoA as active.

  Workaround: Configure shared control by configuring “lacp max-bundle” on the Dual Homed Device (DHD) if the device supports it. This would prevent the DHD from bundling the memberlinks to both PoAs at the same time.

- CSCtn22728

  Symptoms: See the following:

  Router(config)#monitor session 1 type erspan-source

  Router(config-mon-erspan-src)#destination ?

  <cr>

  Router(config-mon-erspan-src)#destination int g11/48

Router(config-if)#

Config Sync: Line-by-Line sync verifying failure on command:

destination int g11/48

due to parser return error

Conditions: This symptom is seen when using unsupported interface CLI option with destination keyword in ERSPAN source session configuration, which may result in Config-Sync failure between Active and Standby-RP, therefore reloading Standby-RP.

Workaround: Do not issue not applicable commands.

- CSCtn24024

  Symptoms: A Cisco ASR 1000 router with dynamic crypto maps may intermittently experience a condition where an IPSec SA will decrypt traffic but not encrypt traffic.

  This is generally seen when the remote peer IP address has changed.

  It is observed that there is a duplicate flow created in the hardware and therefore the traffic to be encrypted matches a stale flow so that packets are not encrypted to the right peer.

  Conditions: This symptom is observed when dynamic crypto maps are used.

  Workaround: Try to clear the crypto session from the spoke. In some cases when the new IPSec SA is built, it will correct the problem.

- CSCtn38711

  Symptoms: A router crashes.

  Conditions: This symptom occurs during SSO on a heavily loaded Cisco 7600 router.

  Workaround: There is no workaround.

- CSCtn41245

  Symptoms: Subinterface ingress stats do not work for access subinterfaces.

  Conditions: This symptom is observed only for the access subinterface. Interface stats and regular subinterface stats work as expected.

  Workaround: There is no workaround.

- CSCtn41662

  Symptoms: Standby RP crashes sometimes when policymap configuration is done. This crash happens randomly with the following crash decode:

  ```
  0xA65C01C:qm_make_final_vmr(0xa65bf14)+0x108
  0xA64799C:qm_send_merge_replace_request(0xa647834)+0x168
  0xA6471B0:qm_tm_merge_replace(0xa646ee4)+0x2cc
  0xA63B3FC:qm_tcam_modify_service_policy(0xa63adbc)+0x640
  0xA63A8AC:qm_process_mqc_event_hdlr(0xa63a51c)+0x390
  0xA63BE7C:qm_process_events_q_hdlr(0xa63bad0)+0x3ac
  0xA63CAA0:qm_process(0xa63c9cc)+0xd4
  ```

  Conditions: This symptom occurs randomly when policymap, class-map is modified, which is applied on different interfaces. This does not happen consistently.

  Workaround: There is no workaround.

- CSCtn45777

  Symptoms: Align messages are seen when enabling the **debug cwan atom** debug command.

  Conditions: This symptom is observed when the **cwan atom** debug command is enabled. Spurious memory access messages are seen on the router console.

Workaround: There is no workaround.

- CSCtn64500

  Symptoms: Multicast traffic does not pass through an ATM point to a multipoint subinterface.

  Conditions: This issue is caused by an incomplete inject p2mp multicast adjacency on ATM P2MP interface. The output of the **show adjacency ATM interface detail** command shows that the Inject P2MP multicast adjacency is in incomplete state.

  Workaround: Run the **clear adjacency** command to force repopulating the incomplete adjacency. Note that you should be aware of the impact of this system-wide command. As an alternative, use unicast commutation if it is possible to do so.

- CSCtn68329

  Symptoms: When source and receivers are in the same VLAN, receivers are unable to receive multicast traffic unless IGMP snooping is disabled for the VLAN.

  Conditions: This issue is not seen when VLAN is in global routing table (no MVPN).

  Workaround: Disable IGMP snooping for the VLAN.

- CSCtn89179

  Symptoms: Output drops are observed when traffic is sent beyond 64k rate with single E1 when E1 is configured as unframed. Issue is seen rarely with using time-slots 1-31. After LC OIR, this symptom is not observed. If the channel is removed and attached, this issue reappears.

  Conditions: This symptom occurs on the following hardware and software:

  Hardware: SIP: 7600-SIP-400, SPA: 7/1 8xCHT1/E1 SPA

  Software: Cisco IOS c7600rsp72043-adventerprisek9-mz.122-33.SRD or later releases

  Workaround:

  1. Apply a service policy similar to below:

     ```
     policy-map test1
     class class-default
     queue-limit 496 --> (this number is a interface bandwidth(in kbps)*1000 / (8
     * 250 * 2) value for the correct behavior.)
     ```

  2. Or reload of the LC.

- CSCtn95395

  Symptoms: VTEMPLATE Background Mgr crashes on DVTI server after using the **clear crypto session** command on DVTI client.

  Conditions: This symptom is seen on DVTI server when sessions are setting up with the IPSec DVTI configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. We might run into VTEMPLATE Background Mgr process crashing after executing the **clear crypto session** command a couple of times on DVTI client.

  Workaround: There is no workaround.

- CSCtn98521

  Symptoms: After the CLI is enabled on ES+ for the control packets hitting on ES+ to not go into special queue, CLI does not reflect in the running configuration on RP sometimes.

  Conditions: This symptom occurs after enabling the **platform control- packet use-priority-q disable** command on ES+ for the control packets hitting on ES+ to not go into special queue. CLI does not reflect in the running configuration on RP.

  Workaround: There is no workaround.

- CSCtn98562

  Symptoms: CLI is enabled on ES+ for the control packets hitting on ES+ to not go into special queue. When doing ES40 LC OIR, control packets that are seen hitting on ES+ port are bypassing the QoS that is configured on the port, and all packets are going in hi-p interface queue.

  Conditions: This symptom is observed after enabling the **platform control-packet use-priority-q disable** command on ES40 LC OIR. The control packets that are hitting on ES+ port are bypassing the QoS that is configured on the port, and all packets are going in hi-p interface queue.

  Workaround: There is no workaround.

- CSCtn99440

  Symptoms: LC CPU high is due to the mfib-const-lc process.

  Conditions: This symptom is observed for scaled mvpn gre configs when more gre mdt tunnels come up.

  Workaround: There is no workaround.

- CSCto08790

  Symptoms: When BRAS is applying an ANCP shaper with specific policy-map name, ActualDownstreamRate and dslType value, a policy-map is created with a policy-map name resulting in hash value 0.

  Policy-map names with Hash value 0 are not handled properly by QoS client and cause the router to crash.

  Conditions: This symptom is seen with certain policy-map or class-map names that can result in internal hash algorithm generating hash value 0, and therefore invalid policy-map or class-map id causes IOSD to crash.

  Workaround: There is no workaround.

- CSCto44585

  Symptoms: Packets with DF-bit set across the l2tpv3 tunnel are punted/dropped on the CPU.

  Conditions: This symptom occurs when PMTU in pseudowire-class configuration is enabled.

  Workaround: Reduce MTU on client side.

- CSCto61263

  Symptoms: With port-channel service-instance (EVC), the traffic stops flowing on new member-links added across different NP on ES+.

  Conditions: This symptom is seen with Cisco 7600, ES+ line card, port-channel service-instances (EVC) with member-links on different NP on a line card.

  Workaround: Use the **shutdown** command followed by the **no shutdown** command on the port channel main interface to resolve the issue.

Resolved Caveats—Cisco IOS Release 15.1(1)S1

Cisco IOS Release 15.1(1)S1 is a rebuild release for Cisco IOS Release 15.1(1)S. The caveats in this section are resolved in Cisco IOS Release 15.1(1)S1 but may be open in previous Cisco IOS releases.

- CSCta43825

  Symptoms: A CMTS walk of the ARP table causes high CPU usage. This symptom is also seen with an SNMP walk of the ARP table.

Conditions: This symptom is observed in the Cisco IOS 12.2S train.

Workaround: To prevent high CPU usage due to SNMP walk, implement SNMP view to prevent SNMP walk of the ARP table:

```
snmp-server view cutdown iso included
snmp-server view cutdown at excluded
snmp-server view cutdown ip.21 excluded
snmp-server community public view cutdown ro
snmp-server community private view cutdown rw
```

Further Problem Description: This symptom is widely observed in Cisco IOS 12.2S train since the ARP redesign in 2004. It is not an efficient way to do next search/tree walk. When there are a lot of ARP entries, the CPU utilization can reach as high as 99% when polling ipNetToMediaTable or atTable (they share the same logic).

- CSCtc73759

  Summary: The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml

- CSCtd10712

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtd16959

  Symptoms: Traceback is seen on SSO switchover.

  Conditions: This symptom is observed under the following conditions:

  - Configure CBTS master tunnel with 3 member tunnels
  - Delete all 3 member tunnels and then remove master command from master tunnel so it becomes regular TE tunnel
  - Configure auto-tunnel primary and backup setup
  - Make SSO switchover

  Many different tracebacks are seen on newly active RP, which are related to MPLS TE.

  Workaround: Do not delete CBTS Tunnels.

- CSCtd72318

  Symptoms: Cisco ASR 1004 router crashes at in __be_dhcpc_for_us.

Conditions: This symptom occurs when running Cisco IOS Release 12.2(33)XNC2. This is possibly associated with DHCP configuration.

Workaround: There is no workaround.

- CSCtd78587

  Symptoms: A Cisco Catalyst 6000 switch running Cisco IOS Release 12.2SX software might crash under rare conditions when err-disable recovery tries to recover a port. The following messages are seen in the logs before the switch resets itself:

  ```
  %CPU_MONITOR-6-NOT_HEARD
  ```

  Conditions: This symptom may be observed after the following sequence of events:

  3. An interface on the switch gets err-disabled as expected due to a certain feature; for example, due to BPDU Guard
  4. Shortly after, before BPDU Guard err-disable recovery kicks in, the same port gets err-disabled for a different reason; for example, because a diagnostic error is detected on the already err-disabled port
  5. Err-disable recovery (BPDU Guard) tries to recover the port and this leads to the crash.

  Workaround: Disable err-disable recovery.

- CSCtd94789

  Symptoms: IPSEC rekey fails after failover with stateful IPSEC HA in use.

  Conditions: The symptom is observed when using PFS and after a failover of the hub devices.

  Workaround: If the security policy allows, removing the PFS eliminates the issue.

- CSCte15193

  Symptoms: The **no spanning-tree vlan [vlanno]** command is not removed on standby alone.

  Conditions: The symptom is observed under the following conditions:

  – the **no spanning-tree vlan** *vlanno* command is configured first
  – the **default spanning-tree vlan** *vlan- range* command is entered next
  – the vlanno falls within the designated range, but the last vlan number in the range does not have “no spanning-tree vlan <>”configured for that.

  Workaround: Enter the **default spanning-tree vlan** *vlanno* command to remove it.

- CSCte56437

  Symptoms: NAT programming on a Cisco Catalyst 6500 may become corrupted; the source and/or destination IP addresses of traffic passing through the NAT box are changed to the wrong IP addresses.

  Conditions: This symptom is observed when the NAT configuration is changed during a high-volume traffic session.

  Workaround: There is no workaround.

- CSCte65688

  Symptoms: Easy VPN server prints “Client_type=UNKNOWN” in “%CRYPTO-6-EZVPN_CONNECTION_UP: (Server)” log, when Software VPN Client establishes an IPSec session.

  Conditions: The symptom is observed when:

  – Easy VPN is configured between a Cisco VPN Client and an IOS router.

– "crypto logging ezvpn" is configured.

Workaround: There is no workaround.

Further Problem Description: This is simply a cosmetic issue. Currently, this message can identify hardware VPN clients (IOS/PIX/VPN3002) only.

- CSCtf23298

  Symptoms: There is high CPU usage when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Conditions: This symptom occurs when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Workaround: Remove single connection option.

- CSCtf41721

  Symptoms: A DMVPNv6 hub might crash upon doing a shut/no-shut on the tunnel interface of the other hub.

  Conditions: The symptom is observed with the following steps:

  1. Configure DMVPNv6 with two hubs and two spokes.
  2. Hub 2 tunnel is shut and unshut.
  3. Hub 1 crashes.

  Workaround: There is no workaround.

- CSCtf72328

  Symptoms: BFD IPv4 Static does not fully support AdminDown.

  Conditions: The symptom is observed with the following setup and configuration:

```
Router 1:
interface e0/0
ip address 192.168.1.1 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.10.1.1 255.255.0.0
exit
ip route static bfd e0/0 192.168.1.2
ip route  10.20.0.0 255.255.0.0 e0/0 192.168.1.2

Router 2:
interface e0/0
ip address 192.168.1.2 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.20.1.1 255.255.0.0
exit

ip route static bfd e0/0 192.168.1.1
ip route  10.10.0.0 255.255.0.0 e0/0 192.168.1.1

interface e0/0
```

```
no ip route static bfd e0/0 192.168.1.1
```

Though the BFD state is DOWN the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtg18555

  Symptoms: A memory leak is observed with process_online_diag_pak.

  Conditions: This symptom is observed on a card supporting TestNonDisruptiveLoopback and TestFabricChHealth tests.

  Workaround: Disable the HM tests TestNonDisruptiveLoopback and TestFabricChHealth on LCs to stop the leak.

- CSCtg28806

  Symptoms: Router crashes at PKI manual enroll.

  Conditions: The symptom is observed on a Cisco 2921 router that is running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- CSCtg64175

  Symptoms: The ISIS route is missing the P2P link, it is mistakenly marked as “parallel p2p adjacency suppressed”.

  Conditions: The symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

  Workaround: Do a **shut** and **no shut** on the local P2P interface.

- CSCth02812

  Symptoms: A prolonged unicast flood can be seen on an ingress path after a TCN event. The flood will last until entries in the arp table are refreshed.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SXH3a (issue has been tracked back to Cisco IOS Release 12.2(18)SXF in an L2 asymmetric environment. The flood is only seen if there is no bi-directional flow on the switch. This issue can be seen in all STP modes.

  Workaround: Clearing ip arp will correct this issue. Lowering the arp timeout will also minimize the impact of the flood.

- CSCth03022

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- CSCth13415

  Symptoms: One way audio in call transfer due to 491 response during resume re- INV.

Conditions: The symptom is observed when you have an UPDATE message passing through the CUBE and then a re-INV crossover happens. The re-INV crossover results in a 491 but the 491 is not correctly forwarded by the IPIP GW. This can result in one way audio issues if the crossed over re-INV was changing the media state from hold to resume.

Workaround: There is no workaround.

- CSCth37580

  Symptoms: Dampening route is present even after removing “bgp dampening”.

  Conditions: The symptom is observed under the following conditions:

  - DUT connects to RTRA with eBGP + VPNv4.
  - eBGP + VPNv4 peer session is established and DUT.
  - Also DUT has VRF (same RD) as route advertised by RTRA.

  In this scenario, when DUT learns the route it will do same RD import and the net’s topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

  Workaround: There is no workaround.

- CSCth60232

  Symptoms: The port-channel interface may flap when adding or removing a VLAN from the trunk on a port-channel interface when one or more interfaces are in a state other than P or D.

  Conditions: This symptom is observed only when the port-channel interface has interfaces in states other than P or D.

  Workaround: Shut down the non-P members and make the vlan changes.

- CSCth61759

  Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate video stream.

  Conditions: There are a couple of scenarios where this problem was observed.

  Scenario 1: This problem was observed in the following SIP-SIP Delayed Offer - Delayed Offer (DO-DO) call flow:

  7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server

  1. Call is originated by 7985
  2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP “200 OK” response

     m=video 53722 RTP/AVP 96 97 34 31
     b=AS:1920
     a=rtpmap:96 H264/90000
     a=fmtp:96 profile-level-id=42e016;max-mbps=108000;max-fs=3600
     a=rtpmap:97 H263-1998/90000
     a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1
     a=rtpmap:34 H263/90000
     a=fmtp:34 CIF4=1;CIF=1;CIF=1;QCIF=1
     a=rtpmap:31 H261/90000
     a=fmtp:31 CIF=1;QCIF=1
     a=sendrecv
  3. CUBE sets video m-line to 0 in the SDP of the SIP “ACK” response

     m=video 0 RTP/AVP 96

  Scenario 2: End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).

CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA

Workaround: There is no workaround.

- CSCth69364

  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://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml.

- CSCth82164

  Symptoms: When OCSP is being used as the revocation check method for IKE, only the 1st connection attempt (after reboot or cache clearing of public RSA keys) undergoes an OCSP check. Subsequent revocation checks are bypassed because the peer's public key appears to be cached indefinitely.

  No CRL or other lifetime parameters are involved, OCSP should be consulted for each IKE tunnel setup.

  The following messages indicate bypassing the revocation check:

  ```
  ISAKMP:(1002): peer&apos;s pubkey is cached
  CRYPTO_PKI: Found public key in hash table. Bypassing certificate validation
  ```

  Conditions: This symptom is occurs when OCSP is configured as revocation check method for IKE.

  Workaround: There is no workaround.

- CSCth93218

  Symptoms: The error message “%OER_BR-4-WARNING: No sequence available” displays on PfR BR.

  Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

  Workaround: There is no workaround.

- CSCti08811

  Symptoms: A router running Cisco IOS may reload unexpectedly when running commands through an Embedded Event Manager (EEM) policy.

  Conditions: This symptom is observed only with EEM policies.

  Workaround: There is no workaround.

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

  Conditions: The symptom is observed when PfR is configured with the following conditions:

  1. list > application > filter > prefix-list
  2. Learn > traffic-class: keys
  3. Learn > traffic-class: filter > ACL

  Workaround: There is no workaround.

- CSCti25319

  Symptoms: A directly connected subnet that is covered by a network statement is not redistributed into another routing protocol, even if a redistribute Open Shortest Path First (OSPF) is configured.

  Conditions: This symptom occurs only for those configurations in which a network mask covers multiple supernets. For example, for the following network statement, router ospf 1 network 192.168.0.0 0.255.255.255 area 0 the above mentioned symptom occurs if the interfaces are configured with IP addresses as follows:

```
ip address 192.168.0.1 255.255.255.0
    ip address 192.168.1.1 255.255.255.0
    and so on.
```

  Workaround 1: Enable OSPF using interface command “ip ospf <AS> area”.

  Workaround 2: Configure multiple network statements with mask/wildcard equal to supernet as shown in the example below:

```
router ospf 1
    network 192.168.0.0 0.0.0.255 area 0
    network 192.168.1.0 0.0.0.255 area 0
    and so on.
```

- CSCti25339

  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/en/US/products/products_security_vulnerability_policy.html

- CSCti34396

  Symptoms: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

  Conditions: The symptom is seen when “next-hop-unchanged allpaths” is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is an unreachable.

  Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the nexthop is set to a visible address, you would configure:

```
route-map static-nexthop-rewrite permit 10
match source-protocol static
 set ip next-hop <router ip address>
!
router bgp <asn>
 address-family ipv4 vrf <vrf name>
 redistribute static route-map static-nexthop-rewrite
 exit-address-family
 exit
exit
```

Workaround 2: Instead of configuring static routes with a next-hop, specify an interface name.

For example, if you had:

ip route x.x.x.x 255.255.255.0 y.y.y.y

And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with:

ip route x.x.x.x 255.255.255.0 interface serial2/0

Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration "set ip next-hop self" is added to route-maps.

When used in conjunction with the newly added configuration:

```
router bgp <asn>
 address-family vpnv4 unicast
  bgp route-map priority
```

The "set ip next-hop self" will override "next-hop unchanged allpaths" for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti34462

  Symptoms: After FPD upgrade, a **shut** on the active shows **no shut** on the standby.

  Conditions: The symptom is observed after an FPD upgrade.

  Workaround: Perform a **no shut** then shut the interface on the active to sync it properly.

- CSCti36310

  Symptom: A Cisco ASR 1000 Series Aggregation Services router is leaking memory when IKE attributes are pulled by SNMP.

  Conditions: This symptom is observed on a Cisco ASR 1000 Series Aggregation Services router with SNMP enabled. The leak has been observed with the asr1000rp1-adventerprisek9.03.01.00.S.150-1.S and asr1000rp1-adventerprisek9.02.06.01.122-33.XNF1 images.

  Workaround: There is no workaround.

- CSCti48504

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- CSCti51145

  Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

  Conditions: In order to see this problem, ALL of the following conditions must be met:

- The non-reloading device must have a “neighbor x.x.x.x transport connection- mode passive” configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword “established” or “eq bgp”.
- It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload.
- When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages.
- Both peers must be multisession capable.
- “transport multi-session” must not be configured on either device, or enabled by default on either device.
- “graceful restart” must not be configured.

Workarounds:

1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor.
3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.
4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**.
5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where “neighbor x.x.x.x transport single-session” is configured and NSF is not configured.

The effect of this fix is as follows: when the neighbor is in single-session mode, and the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS Release 12.2(33)SB based releases if the Cisco IOS Release 12.2(33)SB router is the one not reloading.

- CSCti54173

  Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCti61949

  Symptoms: Unexpected reload with a “SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header” and “chunk name is BGP (3) update” messages.

  Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti67102

  Symptoms: Tunnel disables due to recursive routing loop in RIB.

  Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

  Workaround: There is no workaround.

- CSCti67429

  Symptoms: A REP segment configured on 7600-ES+20G3CXL interfaces on a Cisco 7600 series router that is running Cisco IOS Release 15.0(1)S is not recovering as expected upon link failure recovery of the edge port configured on the 7600. A traffic storm triggered by ISIS protocol configured between 7600 and the MWR 2941s in the REP ring is occurring when the failed REP edge port becomes operational again.

  Conditions: The symptom is observed with a REP ring including two Cisco 7600 series routers equipped 7600-ES+20G3CXL and running Cisco IOS Release 15.0(1) S configured with ISIS and MPLS LDP. The problem is also present in Cisco IOS Release 12.2(33)SRE1.

  Workaround: Configure static routes between the 7600 routers and the MWR 2941s instead of ISIS.

- CSCti68721

  Symptoms: The output of show performance monitor history interval <all | given #> will appear to have an extra column part way through the output.

  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

  Workaround: If the symptom occurs, repeat the command.

- CSCti74962

  Symptoms: "%PM-SP-4-PORT_BOUNCED: bounced by Consistency Check IDBS UP" message is seen on A3-1 new active router after line card OIR followed by an SSO switchover.

  Conditions: This symptom will occur only with a line card OIR followed by an SSO switchover.

  Workaround: There is no workaround.

- CSCti84762

  None

  update generation is stuck with some peers held in refresh started state(SE).The workaround is only hard reset of the stuck peers

- CSCti85446

  Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

  Conditions: The symptom is observed with the following conditions:

  1. Configure a nexthop static route with permanent keyword.
  2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface).
  3. Change the configuration in such a way that nexthop is reachable.
  4. Configure a new static route through the same nexthop IP address used in step 1.

Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti94938

  Symptoms: With more than 1 L2TP sessions on virtual template interface, when applying non-existent route-map and modifying non-existent route map, router crashes.

  Conditions: This symptom occurs with PPPoE sessions with modifying policy configuration with non-existent route-map.

  Workaround: Configure route-map first before applying policy.

- CSCti97759

  Symptoms: IPSG configuration with DHCP snooping entry configuration causes the RP to crash.

  Conditions: This is seen when DHCP static entry is configured.

  Workaround: There is no workaround.

- CSCti98931

  Symptoms: Some sessions may be lost after Layer 2 Tunneling Protocol (L2TP) switchover.

  Conditions: This symptom occurs after L2TP switchover.

  Workaround: There is no workaround.

- CSCtj05591

  Symptoms: Memory corruption and SP crash seen.

  Conditions: The symptom is observed when creating 600 subinterfaces as OIF for Mroute entries.

  Workaround: There is no workaround.

- CSCtj08533

  Symptoms: QoS classification fails on egress PE if the route is learnt via BGP.

  Conditions: The symptom is observed when there are redundant paths to the CPE.

  Workaround: Use only one path between PE and CPE.

- CSCtj17316

  Symptoms: EIGRP flaps up and down in a large scale network, when there is a lot of data to be sent.

  Conditions: In an EIGRP network that has a large number of peers on a single interface, EIGRP might stop sending data to peers. This causes a flap due to packets not being acknowledged.

  Workaround 1: Find the instability in the network and fix the interface.

  Workaround 2: Summarize more routes.

  Workaround 3: Change more routers to stub.

  Workaround 4: Upgrade to rel7 of EIGRP.

- CSCtj17545

  Symptoms: Immediately after a switchover, the restarting speaker sends TCP- FIN to the receiving speaker, when receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

  Conditions: The symptom can occur when a lot of BGP peers are established on different interfaces.

  Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

```
template peer-session ce-v4
  transport connection-mode passive
```

- CSCtj17667

  Symptoms: The **debug radius** debug command may cause memory corruption and crash in rp2 and 1ru images.

  Conditions: This symptom is seen with the **debug radius** command in rp2 and 1ru images.

  Workaround: Do not use the **debug radius** command.

- CSCtj20362

  Symptoms: Router does not allow configuring more than one secondary IP address in the same subnet, on an interface in the same VRF.

  Conditions: This symptom occurs when configuring a secondary address on an interface, which has already one secondary IP address in the same subnet. This applies to VNET capable interfaces.

  Workaround: There is no workaround.

- CSCtj21696

  Symptoms: The virtual access interface remains down/down after an upgrade and reload.

  Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different, the problem does not happen):

  Router1#sho inv

  NAME: “chassis”, DESCR: “2801 chassis” PID: CISCO2801 , VID: V04 , SN: FTX1149Y0KF

  NAME: “motherboard”, DESCR: “C2801 Motherboard with 2 Fast Ethernet” PID: CISCO2801 , VID: V04 , SN: FOC11456KMY

  NAME: “VIC 0”, DESCR: “2nd generation two port EM voice interface daughtercard” PID: VIC2-2E/M= , VID: V , SN: FOC081724XB

  NAME: “WIC/VIC/HWIC 1”, DESCR: “4 Port FE Switch” PID: HWIC-4ESW , VID: V01 , SN: FOC11223LMB

  NAME: “WIC/VIC/HWIC 3”, DESCR: “WAN Interface Card - DSU 56K 4 wire” PID: WIC-1DSU-56K4= , VID: 1.0, SN: 33187011

  NAME: “PVDM 1”, DESCR: “PVDMII DSP SIMM with one DSP with half channel capcity” PID: PVDM2-8 , VID: NA , SN: FOC09123CTB

  Workaround: Do a shut/no shut the serial interface.

- CSCtj24453

  Symptoms: The following traceback is observed when **clear ip bgp *** is done:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 5905A0A8
  chunkmagic 120000 chunk_freemagic 4B310CC0
  -Process= "BGP Scanner", ipl= 0, pid= 549 with call stack
  0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
  0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
  0x403A4E84:bgp_scanner(0x403a4c50)+0x234
  ```

  Conditions: It is rarely observed, when **clear ip bgp *** is done with lot of routes and route-map-cache entries.

  ```
  Router# show ip bgp sum
  BGP router identifier 10.0.0.1, local AS number 65000
  BGP table version is 1228001, main routing table version 1228001 604000
  network entries using 106304000 bytes of memory
  604000 path entries using 31408000 bytes of memory
  762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
  ```

```
381 BGP AS-PATH entries using 9144 bytes of memory
382 BGP community entries using 9168 bytes of memory
142685 BGP route-map cache entries using 4565920 bytes of memory
```

The **clear ip bgp *** command is not a very common operation in production network.

Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj28747

  Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an “Exit Mismatch” message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

  Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

  Workaround: There is no workaround.

- CSCtj30155

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload

  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCtj32574

  Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

  ```
  router eigrp 1
    redistribute connected
    no redistribute connected
  ```

  The **no redistribute connected** command is not being backed up to the standby.

  Conditions: The symptom is observed with any redistribute-related commands.

  Workaround: There is no workaround.

- CSCtj32769

  Symptoms: Data path fails with Layer-2 Virtual Private Network (L2VPN)on ACR interface when asynchronous mode is enabled.

  Conditions: This issue occurs when a VPN is configured on ACR interface in asynchronous mode with cellpacking configurations. This issue does not occur in normal synchronous mode or Layer-2 Virtual Circuits (L2VCs).

  Workaround: Configure the same Maximum Number of Cells Packed (MNCP) value for local and remote provide edge (PE) devices.

- CSCtj36521

  Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

  Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

  Workaround: Make sure IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj38606

  Symptoms: The following error message is seen:

  ```
  %SYSTEM_CONTROLLER-3-MISTRAL_RESET: System Controller is reset:Normal Operation
  continues
  ```

  The **show ibc** exec command reports increments of the following counter:

  Hazard Illegal packet length = 7580

  Conditions: The symptom is observed on a Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCtj40564

  Symptoms: Cisco ASR 1000 router disallows incoming Internet Key Exchange (IKE) connection that matches a keyring. This issue occurs after the router is reloaded.

  Conditions: This symptom occurs when a crypto keyring, which has a local- address defined as an interface, is used.

  ```
  crypto keyring keyring_test
    pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted>
    local address Loopback2104
  ```

  Workaround: Use an IP address.

  ```
  crypto keyring keyring_test
    pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted>
    local address <ip address>
  ```

- CSCtj46297

  Symptoms: Ping fails when performing a shut/no shut on the outgoing interface in an FRR setup.

  Conditions: The symptom is observed in an FRR setup when performing a shut/no shut on the outgoing interface.

  Workaround: Perform a shut/no shut on the tunnel interface.

- CSCtj47736

  Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

  Conditions: The symptom is observed when the neighbor is learned, then you add a max-service limit on an address family. Then do a shut/no shut on the interface.

  Workaround: There is no workaround.

- CSCtj48629

  Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtj50072

  Symptoms: High CPU interrupt level caused by IPv4 unicast or multicast traffic received via GREoIP or GREoMPLS tunnel if rate is high. If ingress interface is tunnel and egress is tunnel (MDT included) as well, then outer IP ToS of egress packet will be reset to 0x0.

  Conditions: The symptom is observed after a reload (under 10% probability), GRE tunnel must be in VRF:

```
#show running-config interface tunnel 513
interface Tunnel513
 vrf forwarding REN
 ip address 10.0.2.1 255.255.255.0
 ip pim sparse-mode
 tunnel source Loopback513
 tunnel destination 10.0.113.2 (via IP or MPLS interface)
 tunnel vrf REN
end
```

  To confirm hit:

```
#show vlan internal usage | include Tunnel513
4074 Tunnel513

#remote command switch show mls vlan-ram 4074 4074
```

  (If there is 256, the defect is present)

  Workaround: Reload the router.

- CSCtj52865

  Symptoms: Unable to utilize 16 queues per lowq port.

  Conditions: If you remove any QoS policy on subtargets of lowq port, because of stale lowq count on the **show platform lowq** command, we will not be able to use maximum number of queues per lowq port.

  Workaround: Only reloading the router resolves the issue.

- CSCtj53299

  Symptoms: Met corruption issue is observed.

  Conditions: This symptom occurs during OIF churn.

  Workaround: Use the **clear ip mroute** command for the problematic entry.

- CSCtj58943

  Symptoms: Standby RP reloads due to line by line sync failure for **encapsulation dot1q 1381** command:

```
encap dot1Q 1381
due to parser return error

rf_reload_peer_stub: RP sending reload request to Standby. User: Config-Sync,
Reason: Configuration mismatch
```

  Conditions: Symptom occurs when issuing a configuration command under a sub-interface mode.

  Workaround: There is no workaround.

- CSCtj65553

  Symptoms: Static route that is installed in default table is missing.

  Conditions: Static route is missing after Route Processor (RC) to Line Card (LP) to Route Processor transition on Cisco Catalyst 3000 series switching module.

  Workaround: Configure the missing static route.

- CSCtj72148

  Symptoms: A Cisco 7600 router might face an SP crash upon first reload after upgrade from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2. After successive reloads, the system functionality is restored.

  Conditions: This symptom is observed when upgrading from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2.

  Workaround: There is no workaround.

- CSCtj72730

  Symptoms: If an Enhanced Interior Gateway Routing Protocol (EIGRP) **address-family** configuration command is removed, any redistribution commands that refer to that address-family should also be removed. This defect documents a case where the redistribution command is not removed.

  Conditions: This issue occurs when the redistribution command is not removed after removing the corresponding EIGRP address-family configuration command.

  Workaround: Manually remove the redistribution commands that remain after the **address-family** command is removed.

- CSCtj77004

  Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

  Conditions: The symptom is observed when “archive log config” is configured.

  Workaround: There is no workaround.

- CSCtj79085

  Symptoms: Multicast Forwarding Information Base (MFIB) entries are struck in NP HW_ERR MET-FULL:5, NP HW_ERR MET-ALLOC:6.

  Conditions: The above issue occurs during slot 7 reload, UUT-CE1 interface Flap, and UUT reload with traffic.

  Workaround: There is no workaround.

- CSCtj79750

  Symptoms: Multicast responses are not obtained.

  Conditions: After a Multicast Listener Discovery (MLD) join, multicast responses are not obtained.

  Workaround: There is no workaround.

- CSCtj79992

  Symptoms: Receiver end flooded in an MVPN scenario.

  Conditions: The symptom is observed even after stopping traffic.

  Workaround: There is no workaround.

- CSCtj82292

  Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

  Conditions: This issue occurs when summary address is advertised as follows:

  ```
  ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
  ```

  Workaround: There is no workaround.

- CSCtj82401

  Symptoms: After rebooting Cisco ASR 1000 router, all adjacencies get detached and all calls fail.

  Conditions: If the configured default call-policy contains “na-carrier-id- table”, it will be converted to “na-dst-carrier-id-table”. During reboot, the “na-dst-carrier-id-table” is detected as an unrecognized command, therefore, that part of the config is rejected. This leaves the SBC in a state where all adjacencies are detached until the problem is corrected.

  Workaround: Manually add back “na-carrier-id-table” to the configuration after reloading the router. Deactivate and reactivate the SBC.

- CSCtj85858

  Symptoms: Coexistance of flat class-default shape policy-map (port level shape) and QoS on sub-targets (sub-interface, service instance, sessions and so on) is not supported on LowQ ES+.

  Conditions: This symptom occurs only on LowQ ES+.

  Workaround: There is no workaround.

- CSCtj86464

  Symptoms: Bundling does not occur with Distributed Link Fragmentation and Interleaving (dLFI) over ATM.

  Conditions: Bundle keeps flapping with dLFI over ATM.

  Workaround: There is no workaround.

- CSCtj87180

  Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of “SSS Manager Disconnected Session”.

  Conditions: The symptom is observed when the LAC router receives an incorrect “Error code(9): Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID” from the multihop peer.

  Workaround: There is no workaround.

- CSCtj88825

  Symptoms: Fabric utilization goes high and drops are seen.

  Conditions: The symptom is observed when egress replication is configured with multicast. Global ICROIF index (0x02006) is programmed which causes high fabric utilization.

  Workaround: There is no workaround.

- CSCtj89941

  Symptoms: IOSd crashes when using the command **clear crypto session** on an EzVPN client.

  Conditions: Testbed setup:

  1. RP2+ESP20 worked as the EzVPN simulator, which is configured with over 1000 clients. Then simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured.
  2. Use IXIA to generate 1Gbps traffic.
  3. Wait until all the SAs have been established and traffic is stable.
  4. Use CLI **clear crypto session** on EzVPN simulator.

  Workaround: There is no workaround.

- CSCtj94297

  Symptoms: “F” flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

  Conditions: The symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRF.

  Workaround: Use the **clear ip mroute** in the affected mroute.

- CSCtj94358

  Symptoms: SIP400 will pass the traffic through a previously configured VLAN on reconfiguring the **bridge-domain** command.

  Conditions: This symptom is seen with the egress interface that is a SIP400 with MPB configured.

  Workaround: Remove the “bridge-domain” configuration and then add the new “bridge-domain”.

- CSCtj94490

  Symptoms: Route Processor (RP) reloads after 30 RP switchovers.

  Conditions: This symptom occurs after 30 RP switchovers during 28000 PPPoEoA sessions while traffic is flowing.

  Workaround: There is no workaround.

- CSCtj94835

  Symptoms: Spurious memory access and tracebacks are seen on router reload.

  Conditions: The symptom is observed when the router is reloaded.

  Workaround: There is no workaround.

- CSCtj95032

  Symptoms: PIM packets are dropped at SIP400. As a result PIM neighborship is not formed between the CEs.

  Conditions: This symptom is seen when the egress interface is on SIP400 with bridging configured on it.

  Workaround: There is no workaround.

- CSCtj96489

  Symptoms: In a CISCO 7600 router, a freshly provisioned interface, or an interface which has been administratively no shut, belonging to non-default VRF, may fail to forward traffic.

  Conditions: This is a race condition and hence timing sensitive.

  Workaround: Another interface **shut/no shut** may help restore service.

- CSCtj96915

  Symptoms: LNS router hangs up at interrupt level and goes into an infinite loop.

  Conditions: Unknown. See Further Problem Description below.

  Workaround: There is no workaround. Only power cycle can remove the symptom.

  Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtj97360

  Symptoms: Punted datapaths are multicast flows GREoIP->DefaultMDT and GREoMPLS->Default MDT.

  Conditions: This symptom occurs with device bootup with IPv4-only VRF. After bootup IPv6 is enabled for VRF, which triggers the problem.

  Workaround: Do not have IPv6 AF and the mcast configurations in the same VRF.

- CSCtj97823

  Symptoms: The 32-byte topology names are not handled correctly on bootup.

  Conditions: This symptom occurs when 32-byte topology names are not handled correctly on bootup.

  Workaround: Use topology names shorter than 32 characters.

- CSCtk00398

  Symptoms: When receiving DHCPv6 SOLICIT from two clients with same DUID, DHCPV6 binds the Delegated-Prefix to incorrect client.

  Conditions: This symptom occurs when two clients are sending SOLICIT with same DUID.

  Workaround: There is no workaround.

- CSCtk00976

  Symptoms: File descriptor reaches the maximum threshold limit. You will be unable to save the configuration or do any file system related operation as file descriptors are exhausted. You will get "File table overflow" error.

  Conditions: The symptom is observed when running the **dir/recursive <>** command periodically using the ANA tool.

  Workaround: Do not run **dir/recursive <>** command if leaks are detected. Also, if it is running through ANA server polling, disable it.

- CSCtk02155

  Symptom: Attachment to the CHOC3 SPA console fails after seeing VC configuration command failures.

  Conditions: This symptom is seen with CHOC3 SPA on SIP200 or SIP400.

  Workaround: Reset the line card.

  Further Problem Description: The periodic process resyncs the IPC between the host and CHOC3 SPA. As this is not happening, we are not able to attach to the SPA console.

- CSCtk02661

  Symptoms: Bundles stop forwarding any traffic.

  Conditions: The symptom is observed when you move the SPA to a different bay on a SIP-400 and apply configurations on the new bay.

  Workaround: Reload spa on both ends.

  Alternate workaround: Unconfigure multilink before moving the SPA out.

- CSCtk02647

  Symptoms: On an LNS configured for L2TP aggregation, it may be that per-user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

Conditions: This symptom is seen when LNS multilink is configured and negotiated for PPP/L2TP sessions per-user ACL downloaded for PPP users via radius.

Workaround: There is no workaround.

- CSCtk05652

  Symptoms: UDLD, that uses end-to-end across an AToM link, causes the CE link on one side to be put in err-disabled state.

  See the following topology:

  SW1 (CE) <-- PE-1 <-> MPLS cloud <-> PE-2 (7600 running 12.2(33)SRE2 --> SW2 (CE)

  UDLD err-disabling the port on SW2 is seen though the link is not unidirectional.

  Conditions: This issue is observed on Cisco IOS Release 12.2(33)SRE2.

  Workaround: Run Cisco IOS Release 12.2(33)SRD5.

- CSCtk06750

  Symptoms: IP-directed broadcast packets do not get forwarded by downstream router.

  Broadcast-source----R1---serial----R2-------rcr

  Conditions: When the serial link encapsulation is set to High-Level Data Link Control (HDLC), which is the default encapsulation, the layer2 HDLC frames are sent out with an incorrect address type in HDLC header. The downstream router does not recognize the payload as a broadcast packet and it does not forward it further as a directed broadcast packet.

  Workaround: Change the encapsulation to Point-to-Point Protocol (PPP) on the affected serial interfaces.

- CSCtk07369

  Symptoms: The buginf statement “draco2_fastsend: PAK_BUF_ON_OBL processing vlan” appears on the console.

  Conditions: This is displayed in certain cases, such as multicast replication.

  Workaround: There is no workaround.

- CSCtk07632

  Symptoms: Even with the filter option, traffic on a different VLAN on trunk port is getting spanned.

  Conditions: The symptom is observed when the filter vlan specified is not configured on the box.

  Workaround: Configure the vlan on the box, then configure it as SPAN filter vlan.

- CSCtk12252

  Symptoms: Priority 1, valid SONET controller network clock source does not get picked as an active clock source. Instead, the clock remains as FREERUN.

  Conditions: This issue occurs after reloading the router, when there is a valid but not present, priority 2 network clock source.

  Workaround: Perform a shut/no shut on the near-end Prio1 clock source SONET controller.

- CSCtk12608

  Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, 15.1 (2)T and Release 15.1(01)S and with the following configurations:

  Router 1:

```
interface Ethernet0/0
 ip address 10.0.12.1 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.1 255.255.255.0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 201.0.0.1 remote-as 200
 neighbor 201.0.0.1 ebgp-multihop 255
 no auto-summary
!

ip route 0.0.0.0 0.0.0.0 200.0.0.1
ip route 201.0.0.1 255.255.255.255 10.0.12.2
ip route 201.0.0.1 255.255.255.255 10.0.120.2
```

Router 2:

```
interface Loopback200
 ip address 200.0.0.1 255.255.255.0
!
interface Loopback201
 ip address 201.0.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.12.2 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.2 255.255.255.0
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 200.0.0.0
 neighbor 10.0.12.1 remote-as 100
 neighbor 10.0.12.1 update-source Loopback201
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.12.1
!
```

Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes”.

- CSCtk12708

  Symptoms: Router crashes when holdover clock source is deleted.

  Conditions: This symptom occurs when the holdover clock source is deleted.

  Workaround: There is no workaround.

- CSCtk13364

  Symptoms: Traffic is blackholed over EVC bridge domain interfaces on the port.

  Conditions: The symptom is observed when a subinterface is deleted and an EVC with the same encapsulation dot1q is created and configured with a bridge domain. The traffic over all the other EVCs on the interface is blackholed.

  Workaround: After the configuration, perform a shut/no shut on the interface.

- CSCtk30807

  Symptoms: A box that acts as a DHCP relay/server crashes when the DHCP service is toggled (no service dhcp/service dhcp).

  Conditions: This issue occurs when the box is also configured as ISG.

  Workaround: There is no workaround.

- CSCtk31340

  Symptoms: Cisco route processor (RP) crashes when a port-channel is removed and the member link is defaulted.

  Conditions: When a port-channel is removed (no int port-channel 200) and the member link is defaulted, the port-channel does not automatically remove the configurations on the member link. This crashes the route processor.

  Workaround: There is no workaround.

- CSCtk33682

  Symptoms: Storm control stops working.

  Conditions: The symptom is observed after a shut/no shut of the interface on an ES-20.

  Workaround: Remove/add the storm control command on the interface.

- CSCtk33821

  Symptoms: When polling VidMon metrics through SNMP during MSE intervals, no metric values are returned.

  Conditions: This symptom is observed when the MSE interval is being polled.

  Workaround: There is no workaround.

  Further Problem Description: When we get a MSE interval, the Cisco 7600 does not export the interval data to SNMP. During the MSE interval MRV will be - 100, CMM uses this value to determine the Media stop event. So it is critical to export the MSE interval to SNMP.

- CSCtk34026

  Symptoms: Adding, deleting and re-adding an access subinterface may sometimes cause loss of data path.

  Conditions: The symptom is observed when the configuration sequence involves an add-delete-add sequence.

  Workaround: Create access subinterfaces from scratch.

- CSCtk36029

  Symptoms: The **match protocol** *icmp* command is not available under class map configuration.

  Conditions: This symptom is seen on the Cisco 7600 with ISG CoPP.

  Workaround: There is no workaround.

- CSCtk36064

  Symptoms: QoS policy-map with set CoS is applied on switchport interface of ES+ LC in ingress. CoS value is not copied to EXP while adding label in L3VPN/VPLS scenarios.

  Conditions: This symptom is seen on a Cisco 7600 router. ES+ LC, QoS policy- map with set CoS is applied on switchport interface in ingress. CoS value is not copied to EXP while adding label in L3VPN/VPLS scenarios.

  Workaround: There is no workaround.

- CSCtk36090

  Symptoms: Router crash at draco2_inband_dma_pak after a router reload with the following SRE image:

  s72033-adventerprisek9_dbg-mz.nightly_sre_2010-11-20

  Conditions: The symptom is observed following a router reload.

  Workaround: There is no workaround.

- CSCtk36377

  Symptoms: VRF ping fails for some of the VRFs after deleting and adding MVRFs.

  Conditions: This symptom is seen when adding and deleting MVRFs using a script.

  Workaround: Delete VRF and add it back.

- CSCtk37068

  Symptoms: Policing is not happening.

  Conditions: This symptom occurs when CoPP is enabled.

  Workaround: There is no workaround.

- CSCtk39301

  Symptoms: Tracebacks such as the following can appear on the RP:

  ```
  %C6K_MPLS_RP-STDBY-3-INFINITE_OCE: In label: 17 Invalid OCE  previous oce
  type: 29 prev
  ptr: 0x5648A2B0, next oce type: 29 next oce ptr: 0x0
  -Traceback= 42319368z 42322E68z 42BA0EF0z 438DCE10z 438D17F0z 405A209Cz
  405AC198z 405A7900z
  405EA768z 405EA9E0z 438D06B4z 438D0EE4z 438DAF98z 438FFE40z 422200D0z
  4222123Cz
  ```

  Conditions: The symptom is observed if there are more than eight or 10 ECMP paths for any prefix (i.e.: when there is a loadbalance object in the forwarding OCE chain).

  Workaround: Reduce the number of paths and do a **clear ip route** to re-initiate hardware programming.

- CSCtk47891

  Symptoms: Traffic might be blackholed when LC is reset, if Fast Reroute (FRR) is in use.

  Conditions: This symptom occurs when FRR is configured and it is in active state when the LC is reset.

  Workaround: There is no workaround.

- CSCtk47960

  Symptoms: Large CLNP packets may be dropped when forwarded over SIP- 200/Flexwan2 module. Header Syntax errors may be recorded on receiving host.

  Remote side will generate the following:

  ```
  %CLNS-3-BADPACKET: ISIS: L1 LSP, packet (902) or wire (896) length invalid
  ```

  Conditions: This symptom is seen on Cisco 7600 switch with SIP-200 line card that is running Cisco IOS 12.2(33)SRD3 and later releases.

  Issue is seen when packets larger than 911 bytes are sent (Payload and Header).

  Workaround: If CLNS is only used for ISIS neighborships “no isis hello padding” can be configured to establish ISIS neighborship. For the LSP packets, configure lns-mtu 903 under router isis on the Cisco 7600 to make this work.

- CSCtk53463

  Symptoms: For configuring the **shape average** *cir value bc value* command currently across all platforms, *bc value* is limited by 4ms * *cir value*. The 4ms here represents minimum interval time for bursts. ES+ LC however can support interval value that is faster (smaller) than 4ms. This has been expected behavior with exception of ES+ LC.

  Conditions: Currently all platforms restrict interval time for shape from going below 4ms.

  Workaround: There is no workaround.

- CSCtk54318

  Symptoms: VC creation fails on disabling and re-enabling the card for SIP-400 with 4XT3E3 SPA with below messages on console:

  ```
  SLOT 2: %NP_CLIENT-3-INITFAIL: NP Client Initialization Failed -
  fr_npc_vc_add: vc creation failure, np: 0, hwidb: 0x4ACA3500, dlci: 0
  SLOT 2: %NP_CLIENT-3-INITFAIL: NP Client Initialization Failed -
  fr_npc_vc_add: vc creation failure, np: 0, hwidb: 0x4ACA3500, dlci: 1023
  ```

  Condition: This issue is seen when the below commands are executed on a T3 serial interface of the SPA 4XT3E3 configured as DTE with frame relay encapsulation:

  no card type t3 *slot bay*
  card type t3 *slot bay*

  Then unconfigure and reconfigure frame relay enacapsulation.

  Workaround: Reload the SPA.

- CSCtk54431

  Symptoms: When a Cisco ASR 1000 BRAS receives SOLICIT IA-PD from CPE, but no Delegated-IPv6-Prefix has been received from Radius, currently, NO reply is sent to the CPE. An Advertise with option “NoPrefixAvail” should be sent instead (RFC 3633).

  Conditions: This symptom is seen when CPE requests IA-PD, but BRAS does not have any Delegated-IPv6-Prefix.

  Workaround: There is no workaround.

- CSCtk55382

  Symptoms: A SPA-OC192POS-VSR or SPA-OC192POS-XFP may fail boot diagnostic test.

  Conditions: The symptom is observed when Control Plane Policing (CoPP) is configured on the system. The diagnostic test that fails is the “TestACLPermit” test displayed in “show diagnostic result”. The output of “show module” will indicate a “Minor error” on the subslot.

  Workaround: Before a system reload or module reset, disable the CoPP feature. After the module is booted, CoPP can be enabled again.

- CSCtk57049

  Symptoms: After access interface flap on encap PE in MVPN setup, the traffic is not sent over data MDT even though the VRF selects the data MDT for encap.

  Conditions: This symptom is seen after access interface flap on encap PE in MVPN setup, the traffic is not sent over data MDT even though the VRF selects the data MDT for encap.

  Workaround: There is no workaround.

- CSCtk59347

  Symptoms: CPU is busy and console is locked up for minutes after entering the **clear counter** command.

Conditions: This symptom occurs with a large scale configuration with hundreds of interfaces and service groups configured on the system.

Workaround: Instead of clearing all counters of all interfaces, clear the counters of specific interfaces as needed.

- CSCtk67658

  Symptoms: Traceback and infrequent crash of the new active are seen when SSO is performed on a router.

  Conditions: This symptom occurs when SSO is performed on a router.

  Workaround: There is no workaround.

- CSCtk68647

  Symptoms: DMVPN stops allowing connections after operating for some time (based on number of connections). The **show crypto socket** command shows sockets are leaking and never decrease even when the SA is inactive.

  Conditions: This symptom occurs on Cisco ASR code prior to Cisco IOS Release XE 3.2.0. Multiple DMVPN tunnels are configured with tunnel protection shared.

  Workaround: Upgrade to Cisco IOS Release XE 3.2.0. Remove other DMVPN tunnels (or shutdown tunnels).

- CSCtk75389

  Symptoms: PFR fallback interface on Cisco ASR 1000 platform fails to remain in inpolicy.

  Conditions: The issue is seen on Cisco ASR 1000 platform and only with ATM interface.

  Workaround: There is no workaround if ATM interface is used on the Cisco ASR 1000 platform.

- CSCtk76190

  Symptoms: The RSP/SUP fails to switchover automatically when the “TestSPRPInbandPing” fails for more than 10 instances.

  Conditions: The symptom is observed when the “TestSPRPInbandPing” fails for more than 10 instances.

  Workaround: There is no workaround.

- CSCtk83760

  Symptoms: Met updates from SUP are reaching Cisco 67xx DFC cards.

  Conditions: This symptom is observed during OIF churn. This is not reproduced locally, and the fix is put in as a sort of preventive mechanism.

  Workaround: There is no workaround.

- CSCtk98030

  Symptoms: After replacing an ES20 line card with an ES+ line card or vice versa in the same slot, some service groups reject new members to join if the old line card had ethernet service instances in these groups. Similarly, a named EVC rejects new ethernet service instances if it had association with the old line card. The named EVC cannot be deleted, complaining that it still has service instances.

  Conditions: The symptom is observed if an ES20 line card has been replaced with an ES+ line card or vice versa in the same slot. The old line card had ethernet service instance members in some service groups and/or named EVCs. The old associations between ethernet service instances and service groups or named EVCs are not cleaned up properly, blocking new association to these groups and EVCs.

Workaround: Configure new service groups and named EVCs with same configuration as the problematic ones. Abandon the use of the old groups and EVCs. Assign ethernet service instances from the new line card to the new groups and EVCs.

- CSCtl03100

  Symptoms: Router crashes due to severe memory fragmentation.

  Conditions: This symptom occurs with the following configuration:

  - 6000 series scalable EoMPLS
  - 500 sw-based EoMPLS
  - 2.5k VPLS instances
  - 100 vrfs(50 L3VPN, 30 MVPN, and 20 6VPE)
  - QOS policies on around 1600 interfaces.

  Workaround: There is no workaround.

- CSCtl05926

  Symptoms: Packets of size exceeding MTU are dropped with the following error messages:

  ```
  %CONTROLLER-3-TOOBIG: An attempt made to send giant packet on  \
  GigabitEthernet7/3/1 (1491 bytes from 10010046, max allowed 1476
  ```

  Conditions: This symptom is observed when the outgoing interface is on SIP400.

  Workaround: There is no workaround.

- CSCtl05979

  Symptoms: In SSO mode, PPPoE sessions with PAC2 ISG service are replicated to Standby RP, with policy-maps missing on Standby RP. PAC2 service should poison the PPPoE session.

  Conditions: This symptom is observed in SSO mode, when PPPoE sessions with PAC2 ISG service are established.

  Workaround: Use dummy ISG service applied from RaBaPol to force poisoning.

- CSCtl08014

  Symptoms: Router crashes with memory corruption symptoms.

  Conditions: This symptom occurs when performing switchover or Online Insertion and Removal (OIR), while MLP sessions are initiating.

  Workaround: There is no workaround.

- CSCtl08601

  Symptoms: Unconfiguring DHCP pool hangs the console.

  Conditions: This symptom is observed when “no service dhcp” is issued prior to unconfiguring the pool.

  Workaround: There is no workaround.

- CSCtl10395

  Symptoms: Control Plane Policing (CoPP) stops dropping packets in hardware on a Cisco 7600 series router after double switchover.

  Conditions: This symptom occurs on the Cisco 7600 platform when CoPP is configured on the router and SSO (HA Switchover) is done twice.

  Workaround: Remove and reconfigure the CoPP.

- CSCtl18652

  Symptoms: After replacing an ES20 with an ES+ line card on the same slot, or vice versa, adding ethernet service instance members from the new line card to an existing service group that was associated with the old line card may cause a reload of the standby RP in SSO mode. This is due to stale configuration on the standby RP.

  Conditions: An ES20 line card has been replaced by a different type of line card or vice versa, on the same slot. New members are assigned to a service group that had members from the old line card. There is a standby RP in SSO mode.

  Workaround: Create a new service group with the same configuration as the existing group and assign new members to the new group. Abandon the use of the old group.

- CSCtl19347

  Symptoms: On configuring additional bundles, LC crashes. This occurs with SIP- 400 when copying the dLFI configurations from a disk to the running configuration to bundle up.

  Conditions: This symptom occurs when copying the dLFI configurations from a disk to the running configuration to bundle up.

  Workaround: There is no workaround.

- CSCtl20993

  Symptoms: Router crashes during IPsec rekey.

  Conditions: The conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtl41921

  Symptoms: There is a traffic duplication.

  Conditions: This symptom occurs with bootup with scale having 2000 sLSPs.

  Workaround: Do a shut/no shut on the tunnel.

- CSCtl42358

  Symptoms: A Cisco ASR 1000 series router crashes after “no atm sonet overhead j1” command on an ATM interface.

  Conditions: This symptom occurs on a Cisco ASR 1000 series router on an ATM interface.

  Workaround: There is no work around.

- CSCtl46703

  Symptoms: T1/E1 tributary on Prowler SPA stays down occasionally after LC/SPA is reloaded.

  Conditions: This symptom occurs after LC/SPA is reloaded.

  Workaround: Reconfigure clock configuration (e.g. vtg 1 t1 1 clock source line/internal) on the affected T1/E1.

- CSCtl46903

  Symptoms: VLAN mapping or translation feature does not work on ES+, when the port is configured as L2 switchport.

  Conditions: This symptom occurs when the port is configured on L2 switchport.

  Workaround: Configure the feature under EVC framework or L2 switchport on LAN cards.

- CSCtl50930

Symptoms: For some sip messages (for example, OPTION), SBC will assert failure when call goes through VRF.

Conditions: This symptom only happens on 1001/1002/1004 non-redundant mode.

Workaround: Configure redundant mode SSO.

- CSCtl55828

  Symptoms: LDP/OSPF PDUs get dropped when line rate traffic is running on the Interface in case the link is over subscribed.

  Conditions: This symptom occurs with the following Hardware and software:

  Hardware - ES+ LC

  Software - Cisco IOS Releases 15.0(1)S, 15.0(1.1)S, 15.1(1)S Link over subscription, output drops at the MPLS interface.

  Workaround: There is no workaround.

- CSCtl58623

  Symptoms: MCP XE32 build breaks.

  Conditions: This symptom occurs in all conditions.

  Workaround: There is no workaround.

- CSCtl69609

  Symptoms: When bringing down the shortest route, traffic blackholing occurs in MLDP on one of the OIF.

  Conditions: This condition occurs in MLDP and branch point combination.

  Workaround: There is no work around.

- CSCtl74301

  Symptoms: INBOX Stateful Switch Over (SSO) does not work on Cisco ASR 1006 routers in RLS 3.2(8). When this occurs, SSO drops signaling and RTP.

  Conditions: This symptom occurs for INBOX SSO. This happens when SIP binds with the loopback address for control.

  Workaround: There is no workaround. Unless required by your network architecture, do not use loopback address for control bind.

- CSCtl83053

  Symptoms: Unable to change the shaper rate with ANCP port up messages.

  Conditions: This symptom occurs with the Cisco ASR 1000 series router with QoS and ANCP enabled.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.1(1)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(1)S. All the caveats listed in this section are open in Cisco IOS Release 15.1(1)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCth08313

  Symptoms: The following is seen during online operations:

  ```
  : %SYS-SP-2-GETBUF: Bad getbuffer, bytes= 24616
  -Process= "IPC Periodic Timer", ipl= 0, pid= 24
  -Traceback= 81745F8 81D19E8 8BEAD94 8BEB5C4 853BAD4 8527704 854CE24 82AE1B0 82AE2E8
  855E454 835AFD0 83552E8
  ```

  Or

  ```
  IPC: Sending Big IPC msg to Driver MSG: ptr: 0x152CDAC8, flags: 0x14328, retries: 1,
  seq: 0x2016C68, refcount: 2, rpc_result = 0x0, data_buffer = 0x14FB3084, header =
  0x78730658,
  data = 0x78730678 || HDR: src: 0x216001E, dst: 0x2010000, index: 0, seq: 27752, sz:
  1808,
  type: 14209, flags: 0x1608, ext_flags: 0x0, hi: 0x1B622B, lo: 0x36C456 || DATA: 00 00
  00 06
  0E 19 00 08 00 00 00 00 00 00 03 12 00 00 00 00 89 00 00 00 00 00 00 00 00 00 06 E8 00
  00 00 01 11 9E 04 34 04 60 08 00 00 01 00 20 6E 00 67 05 EF E8 00 06 00 00 00 20 00 00
  00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16
  ```

  Conditions: This symptom is seen either after boot of the router or after failover on a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRE.

  Workaround: There is no workaround.

- CSCth08800

  Symptoms: Multicast traffic gets replicated to EVCs, which have not joined a multicast feed.

  Conditions: This symptom is seen when we have multiple EVCs under a single bridge-domain service with active multicast receivers spread across the EVCs. Upon disabling and re-enabling snooping on bridge-domain VLAN, multicast gets wrongly replicated by NP on Excalibur.

  Workaround: Reconfigure the physical interface carrying the EVCS.

- CSCti08301

  Symptoms: The SPA gets reloaded due to Semaphore hog and heartbeat failures.

  Conditions: This symptom occurs when member links of a multilink bundle is added/removed or moved across multilink bundles while sending traffic at bigger frame size and higher rate.

  Workaround: There is no workaround.

- CSCti08740

  Symptoms: When network payload loopback is followed by remote line fdl ansi loopback, the remote fdl ansi fails.

  Conditions: This symptom happens when network payload loopback is followed by remote line fdl ansi loopback.

  Workaround: Do the remote line fdl ansi alone.

- CSCti17802

  Symptoms: The following log message may be incorrectly displayed to prompt the user to issue the **issu runversion** command in cases where the ISSU upgrade has been aborted due to an error.

  ```
  "ISSU_PROCESS-SP-7-DEBUG: Peer state is [ STANDBY HOT ]; Please issue the runversion
  command"
  ```

  Conditions: Wrong message is shown when ISSU is aborted after issuing the **issu loadversion** command. This behavior has no functional impact.

  Workaround: There is no workaround.

- CSCti20319

  Symptoms: After ISSU, the LTL entry corresponding to L3 receiver on CFC in egress replication mode does not have the OIF slot programmed in platform entry on SP.

  Conditions: This symptom is seen after ISSU runversion. It is not seen after SSO.

  Workaround: Do a module reset of the egress CFC card.

- CSCti22462

  Symptoms: On adding more than 18 slaves with delay request rate at 32 PPS to a master session, existing slaves start flapping.

  Conditions: This symptom occurs with a setup with more than 18 slaves connected to a master session with delay request rate at 32 PPS.

  Workaround: Reduce the delay request rate on the slave side. Keep number of slave sessions connected to a master of less than 18.

- CSCti23169

  Symptoms: Redistribution of EIGRP into BGP at the PE creates an external route at the CE at the other end.

  Conditions: When we redistribute EIGRP into BGP at the PE and the EIGRP has a network that is actually a loopback interface on this PE, we see the other end CE shows it as an external route. The specific condition for this is only when this network is the first network statement applied in the EIGRP. For example, see the following:

  ```
  net 10.0.0.0 is the subnet for the loopback interface on the PE and net
  192.168.0.0 is the other interface network address which has a neighbor at
  the other end. We have EIGRP redistributed into BGP and we are now
  configuring EIGRP as
  router eigrp
  network 10.0.0.0
  network 192.168.0.0
  ```

  In this condition we see an external route created for 10.0.0.0 network at the other CE. If we reverse the network statement order, we do not see this issue. Also when we use the **no network** *10.0.0.0* command and reenter the network statement, we do not see the issue.

  In any live network, such configuration will never occur. The customers will never try to add the loopback address of a PE and send it to the other CE over EIGRP PE-CE network.

  Workaround:

  1. Reverse the network statements
  2. Do a **no network** and **network** for that network.

- CSCti27214

  Symptoms: BFD/Routing flaps, and packet loss is seen.

  Conditions: This symptom is seen when Standby RP is coming up to life.

  Workaround: Disable both QoS (containing NBAR) and NBAR protocol discovery from under all interfaces.

- CSCti40325

  Symptoms: Radius retransmit timeout happens (roughly) at half the timeout configured by the **radius-server timeout** *timeout* command. For example, for the default timeout value of 5 seconds, timeout happens at 2 to 3 seconds. For higher values, for example 20, timeout happens at around 10 seconds.

  Conditions: This symptom is seen when radius server is used for AAA.

Workaround: There is no workaround.

- CSCti47426

  Symptoms: NAT address is consistently added in the FIB table as a receive adjacency. This results in packet getting incorrectly routed.

  Conditions: This issue is seen with static NAT such that NAT source address is same as destination address.

  Workaround: There is no workaround.

- CSCti66996

  Symptoms: SIP400 crash is seen on reloading the chopper SPA, which has MLP bundles configured.

  Conditions: This symptom is seen when swapping the member links across bundles and reloading the SPA. The crash is seen sometimes.

  Workaround: There is no workaround.

- CSCti78950

  Symptoms: Traffic is sent to RP for unresolved entries.

  Conditions: This symptom occurs when the remote is not responding to ARP.

  Workaround: There is no workaround.

- CSCti81076

  Symptoms: PVC creation fails on controller with the following message:

  ```
  ACRPVCADD : PVC creation fails
  ```

  Conditions: This issue is seen with the following steps:

  1. Add working and protect controller to ACr group.
  2. Configure virtual controller for ATM and create L2VP on ATM-ACR interface.
  3. Shut the working controller.
  4. Remove atm config from virtaul controller and configure again.
  5. Do “no shut” on the working controller.

  Workaround: Configure when controllers are UP.

- CSCti82670

  Symptoms: An RSP will crash when the CFM automated test script (consisting of 53 tests) is run twice in succession.

  With SUP720, the crash is seen with a single run.

  Conditions: The automated test script must be run on 3 connected routers.

  Workaround: Adding a **no shut** on UUT interface with UP- MEPS before doing the LeakConfig seems to prevent the crash and provide a clean run.

  Further Problem Description: Other problems observed are:

  - The CFM MIB will return infinite results for getmany.
  - A **show** command will crash the router.

- CSCti87639

  Symptoms: Standby RP reloads due to config out of sync or keepalive failure in RPR mode.

  Conditions: This issue is observed while running NBAR scripts or sometimes with no activity on box. It cannot be reproduced manually.

Workaround: Operate in SSO mode.

- CSCti87947

  Symptoms: All the police profiles applied on Service groups on a port-channel interface do not get cleared on deleting the port-channel interface.

  Conditions: This symptom occurs with scale configurations and ingress policers applied on SG on port-channel interface.

  Workaround: Line card online insertion and removal (OIR) solves the problem.

- CSCtj05670

  Symptoms: When doing SSO with scaled mLDP configuration, path set for some of the VRFs are not configured.

  Conditions: This issue only occurs when configuring mLDP on 100 VRFs with 100 receivers.

  Workaround: There is no workaround.

- CSCtj19150

  Symptoms: Service policy applied on VP not seen on standby RP after doing APS switchover Issue is seen only in scale environment and when Both Active and protect controllers are on different LCs.

  Conditions: The issue will be seen under the following conditions:

  1. Configure ACR on both working and protect controllers (on different LCs).
  2. Configure virtual controller for ATM.
  3. Configure 100 ATM PVPs and apply service policy.
  4. Do APS switchover.

  Workaround:

  1. Have both working and protect controller on same LC.
  2. After APS switchove remove and again apply service policy.

- CSCtj22784

  Symptoms: A service-group is not getting configured.

  Conditions: This symptom is seen when a service-group is not getting configured on scaled configurations.

  Workaround: There is no workaround.

- CSCtj24811

  Symptoms: A Cisco ASR 1000 router may crash when RSVP aggregation feature is configured and FLR is triggered.

  Conditions: This symptom is seen when usage of RSVP aggregation feature and FLR is triggered.

  Workaround: There is no workaround.

- CSCtj30238

  Symptoms: WRED counters are wrongly updated. The default counter should be 0, but the counter is wrongly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there is not traffic match in the class.

Conditions: This issue is seen on Cisco 7600 router with ES+ card only. Es+ line card does not support per WRED class based counters. There was a recent breakage due to which transmit packets/bytes column started showing up for Es+ card, which is wrong. As ES+ writes same value to WRED transmit count (not the per subclass base count, but total count), this value does not make sense.

Workaround: Do not use WRED subclass transmit packets/bytes counters for ES+ line card on Cisco 7600 router.

- CSCtj32574

  Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

  ```
  router eigrp 1
    redistribute connected
    no redistribute connected
  ```

  The **no redistribute connected** command is not being backed up to the standby.

  Conditions: The symptom is observed with any redistribute-related commands.

  Workaround: There is no workaround.

- CSCtj35914

  Symptoms: In a setup with primary CEM PW and a backup configured, the traffic flows in the backup path when the primary is still up.

  Conditions: Reload the module on the peer PE, when the primary path/controller is down. Allow the backup path to come up when primary path is still down. Bring up the primary path now, the traffic will not be switched to the primary path. The traffic still flows in the backup path, though the primary path is up. The traffic does not switchover to primary, even if the backup path goes down.

  Workaround: Reset the module on the peer PE again when the primary controller/path is up.

- CSCtj44160

  Symptoms: The “failed to reparent member to new group” error message is seen as soon as flat SG is applied on subifs and after that, it gets rejected.

  Conditions: This symptom is seen in bringup sessions from subifs having HQoS policy applied on session control policy and attach flat SG to the subifs.

  Workaround: There is no workaround.

- CSCtj47086

  Symptoms: If a connected route that is also owned by EIGRP or OSPF is replicated from one routing table to another, any route-map that is applied when redistributing the route into EIGRP will not work properly if the source specified during redistribution is anything other then connected (for example EIGRP or OSPF).

  Workaround: Make sure to specify the source as EIGRP or OSPF instead of connected when redistributing the replicated routes.

- CSCtj52865

  Symptoms: Unable to utilize 16 queues per lowq port.

  Conditions: If you remove any QoS policy on subtargets of lowq port, because of stale lowq count on the **show platform lowq** command, we will not be able to use maximum number of queues per lowq port.

  Workaround: Only reloading the router resolves the issue.

- CSCtj52969

  Symptoms: The following message may be observed when issuing the **show issu state detail** command after performing an **issu loadversion** operation:

  ```
  %ISSU_PROCESS-3-IPC_AGENT: Failed to send; error code [ timeout ]
  ```

  Conditions: This message may be observed when issuing the **show issu state detail** command after performing an **issu loadversion** operation. This message may also be observed if the **show issu state detail** command is given while the standby is reloading for any other reason.

  Workaround: When the standby is booting up after issuing the **issu loadversion** command, do not use the **show issu state detail** command until the standby is completely up. There is no functional impact, except that for a small period of time (a few seconds), the standby information is temporarily unavailable.

- CSCtj58686

  Symptoms: Difference is seen in subclassification for Kazaa over http and Kazaa over non80 traffic.

  Conditions: This symptom is seen with difference in subclassification for Kazaa over http and Kazaa over non80 traffic.

  Workaround: There is no workaround.

- CSCtj64755

  Symptoms: Console hangs for 4 to 5 minutes when IMA configurations are removed from the virtual controller with scale.

  Conditions: This issue is seen when IMA interface is configured for scale. Console hangs when IMA configuration is removed from virtual controller by “no vtg 1 t1 ima-group”.

  Workaround: There is no workaround.

- CSCtj93845

  Symptoms: Memory leak in ACL is observed with PBR configuration.

  Conditions: This memory leak is observed when 200 application traffic classes are configured using PfR, and traffic is left running on the testbed for sometime.

  Workaround: There is no workaround.

- CSCtj94188

  Symptoms: After LC OIR the red AIE peer and AIE Peer id become the same. This causes the PWs to go down.

  Conditions: LC OIR causes the red AIE peer id and AIE peer id to become same.

  Workaround: Clear xconnect all reprovisions the PWs and the issue is not seen.

- CSCtk05205

  Symptoms: FMAN-FP crashes with scaled traffic.

  Conditions: This symptom is seen with a plain firewall and is receiving scaled SMTP traffic that is sent by Avalanche tool with different source ip addresses in the same subnet.

  Workaround: Using the **parameter-map type inspect** command and restricting the maximum scaling numbers, we can avoid the crash, but scaling number will be less.

- CSCtk10381

  Symptoms: Met3 is being set to 0 on doing SSO with mLDP intranet configurations.

  Conditions: This symptom is seen with MVPN session in data MDT mode and doing SSO switchover.

Workaround: Clear ip mroute of the affected steams.

- CSCtk13121

  Symptoms: Router crashes inconsistently when doing pings.

  Conditions: This symptom is seen with router crashing inconsistently when doing pings.

  Workaround: There is no workaround.

- CSCtk13169

  Symptoms: Ping does not pass through in dLFI over ATM with sip-200+sip-400.

  Conditions: This symptom is seen when ping does not pass through in dLFI over ATM with sip-200+sip-400.

  Workaround: There is no workaround.

- CSCtk13364

  Symptoms: Traffic is blackholed over EVC bridge domain interfaces on the port.

  Conditions: When a sub-interface is deleted and an EVC with the same encapsulation dot1q is created and configured with a bridge-domain, the traffic over all the other EVCs on the interface is blackholed.

  Workaround: After the configuration, performing a **shut/no shut** on the interface restores all traffic.

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 15.1S. These documents include hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, and feature modules.

Documentation is available online on Cisco.com.

Use these release notes with the resources described in the following sections:

Platform-Specific Documents

Platform-specific information and documents for the Cisco 7200 series routers, Cisco 7300 series routers, and Cisco 7600 series routers are available at the following locations:

Cisco 7200 series home page on Cisco.com at
http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_series_home.html

Cisco 7300 series home page on Cisco.com at
http://www.cisco.com/en/US/products/hw/routers/ps352/tsd_products_support_series_home.html

Cisco 7600 series home page on Cisco.com at
http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS and Catalyst OS 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.

Cisco Feature Navigator is updated regularly and 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://www.cisco.com/go/cfn

Cisco IOS Software Documentation Set

The Cisco IOS Release 15.1S documentation set consists of configuration guides, command references, and other supporting documents and resources. For the most current documentation, go to the following URL:

http://www.cisco.com/en/US/products/ps11280/tsd_products_support_series_home.html

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 and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 343.
