



# Release Notes for Cisco IOS Release 15.0S

---

**First Published: July 30, 2010**

**Last Updated: June 29, 2012**

**Release: Cisco IOS Release 15.0(1)S6**

**Part Number: OL-23223-01 Rev. H0**

These release notes support Cisco IOS Release 15.0S for the Cisco 7600 series routers up to and including Cisco IOS Release 15.0(1)S6. These release notes are updated as needed to describe new features, caveats, and related documents.

Use these release notes with the appropriate platform documentation. See the [“Related Documentation” section on page 212](#).

For more information, see the [“Introduction” section on page 2](#).

## Contents

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 6](#)
- [MIBs, page 16](#)
- [Limitations and Restrictions, page 16](#)
- [Important Notes, page 17](#)
- [Caveats, page 25](#)
- [Troubleshooting, page 211](#)
- [Related Documentation, page 212](#)
- [Notices, page 213](#)
- [Obtaining Documentation and Submitting a Service Request, page 215](#)



---

**Americas Headquarters:**

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

© 2010–2012 Cisco Systems, Inc. All rights reserved.

# Introduction

Cisco IOS Release 15.0S initiates a consolidated support strategy to provide greater consistency in new feature release and rebuild schedules and to simplify the software selection process. The release numbering has changed from 12.2SR to 15.0S to support this strategy and simplified software selection process.

Cisco IOS Release 15.0S aggregates feature inheritance from Cisco IOS Release 12.2SR.

Cisco IOS Release 15.0(1)S is the first in a series of individual Cisco IOS Release 15S releases, each of which will deliver aggregate functionality through its predecessor. Cisco IOS Release 15.0(1)S, the latest release of Cisco IOS software for the Cisco 7600 series routers, builds on the proven capabilities of Cisco IOS Release 12.2SR.

More than 40 new features for mobile, video, business, and residential services are introduced in Release 15.0(1)S. Leading features and benefits include:

- *Inline Video Monitoring*—Improve service-level agreements (SLAs) for production video delivery
- *IEEE 1588-2008*—Converge to all Ethernet 3G & 4G mobile networks including time of day
- *SyncE ESMC & SSM*—Integrate synchronization management on Ethernet 3G & 4G mobile platforms
- *mVPN Extranet*—Deliver on-demand multicast services for Virtual Private Network (VPN) business customers
- *Static PW over P2MP TE*—Improve multicast resiliency and simplify network designs
- *IEEE 802.1ad Full Compliance*—Improve interoperability for multivendor environments
- *2-Port Gigabit Synchronous Ethernet SPA Support*—Create clocking solutions for circuit emulation and native Ethernet
- *Tunable DWDM Optics*—Improve operations and scale with simplified selection of wavelengths
- *ATMv2 SPA Support*—Save money with better density for legacy interfaces

For information on new features and Cisco IOS commands that are supported by Cisco IOS Release 15.0(1)S, see the [“New and Changed Information” section on page 6](#).

## System Requirements

This section describes the system requirements for Cisco IOS Release 15.0S and includes the following sections:

- [Supported Hardware, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Support, page 4](#)
- [Memory Recommendations, page 5](#)

## Supported Hardware

Cisco IOS Release 15.0S supports the following platforms, including the following models and supervisor engines:

- Cisco 7600 series routers (Cisco 7603-S, Cisco 7604, Cisco 7606, Cisco 7606-S, Cisco 7609, Cisco 7609-S, and Cisco 7613)
- Supervisor Engine 32, Supervisor Engine 720, Route Switch Processor 720
- RSP720-10GE

## 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 Release 15.0S*:

[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/15_0s/7600_hwd.html)

For information about the new hardware features, see the “New and Changed Information” section on page 6.

## 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-ip-services_wan-mz), Version 12.2(33)SRD, EARLY DEPLOYMENT
RELEASE SOFTWARE
```

## Upgrading to a New Software Release

For information about selecting 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](http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml)

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

To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to 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 by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features that are 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:

<http://www.cisco.com/go/cfn>

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

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

## 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](mailto: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](http://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](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.
- 

## New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.0S and contains the following subsections:

- [New Hardware Features in Cisco IOS Release 15.0\(1\)S2, page 6](#)
- [New Software Features in Cisco IOS Release 15.0\(1\)S2, page 6](#)
- [New Hardware Features in Cisco IOS Release 15.0\(1\)S, page 7](#)
- [New Software Features in Cisco IOS Release 15.0\(1\)S, page 7](#)

### New Hardware Features in Cisco IOS Release 15.0(1)S2

There are no new hardware features in Cisco IOS Release 15.0(1)S2.

### New Software Features in Cisco IOS Release 15.0(1)S2

This section describes new and changed features in Cisco IOS Release 15.0(1)S2. Some features may be new to Cisco IOS Release 15.0S 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 15.0(1)S2. Links to feature modules are included below. If a feature listed below 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 below.

#### Label Switched Multicast (LSM) Multicast Label Distribution Protocol (mLDP) Based Multicast VPN (mVPN) Support

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

[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/routers/7600/ios/15S/configuration/guide/7600_15_0s_book.html)

## MLDP-Based MVPN

The MLDP-based MVPN feature provides extensions to Label Distribution Protocol (LDP) for the setup of point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) label switched paths (LSPs) for transport in the Multicast Virtual Private Network (MVPN) core network.

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

[http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc\\_mldp\\_mvpn.html](http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_mldp_mvpn.html)

## New Hardware Features in Cisco IOS Release 15.0(1)S

This section describes new and changed features in Cisco IOS Release 15.0(1)S. Some features may be new to Cisco IOS Release 15.0S 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 15.0(1)S. Links to feature modules are included below. If a feature listed below 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 below.

### Addition of ES Transport Line Cards for Cisco 7600

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/Hardware/Module\\_and\\_Line\\_Card\\_Installation\\_Guides/ES40\\_Line\\_Card\\_Installation\\_Guide/es40\\_pref.html](http://www.cisco.com/en/US/docs/routers/7600/Hardware/Module_and_Line_Card_Installation_Guides/ES40_Line_Card_Installation_Guide/es40_pref.html)

### SPA-1x0C3-ATM-V2, SPA-3x0C3-ATM-V2 and SPA-1x0C12-ATM-V2 Support on Cisco 7600 SIP-400 and SIP-200

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/7600wsip.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/7600wsip.html)

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/install\\_upgrade/7600series/7600sov.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/7600series/7600sov.html)

[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/15_0s/7600_hwd.html)

## New Software Features in Cisco IOS Release 15.0(1)S

This section describes new and changed features in Cisco IOS Release 15.0(1)S. Some features may be new to Cisco IOS Release 15.0S 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 15.0(1)S. Links to feature modules are included below. If a feature listed below 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 below.

## 802.1ad Full Compliance

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES20\\_config\\_guide/baldfc.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldfc.html)

## 802.3ad Link Aggregation with Weighted Load Balancing

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce\\_lnkbnld.html](http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_lnkbnld.html)

## ATM AC: VC Signalling and Provisioning

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm\\_ac\\_vc\\_sig\\_prov.html](http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_ac_vc_sig_prov.html)

## BFD Control Channel over VCCV-Support for ATM Pseudowire

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/76cfgsip.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgsip.html)

[http://www.cisco.com/en/US/docs/ios/iproute\\_bfd/configuration/guide/irb\\_bfd.html](http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html)

## BGP—Remove/Replace Private AS Filter

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/iproute\\_bgp/configuration/guide/irg\\_remove\\_as.html](http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_remove_as.html)

## BGP Dynamic Neighbors

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/iproute\\_bgp/configuration/guide/irg\\_neighbor.html](http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor.html)

## BGP Nonstop Routing with Stateful Switchover

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/iproute\\_bgp/configuration/guide/irg\\_nsr\\_sso.html](http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_nsr_sso.html)



## BGP Slow Peer

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/iproute\\_bgp/configuration/guide/irg\\_slow\\_peer.html](http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_slow_peer.html)

## Broadcast Storm Control on Switchports and Ports Having EVCs

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES20\\_config\\_guide/baldfcfg.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldfcfg.html)

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES20\\_config\\_guide/es20-config-guide.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/es20-config-guide.html)

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES40\\_config\\_guide/es40\\_chap4.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html)

[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/install_config/ES40_config_guide/es40_sw_config.html)

## CISCO-SWITCH-HARDWARE-CAPACITY-MIB

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/technical\\_references/7600\\_mib\\_guides/MIB\\_Guide\\_ver\\_6/7600mib3.html](http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/7600mib3.html)

## CLASS-Based-QoS-MIB for EVC

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/technical\\_references/7600\\_mib\\_guides/MIB\\_Guide\\_ver\\_6/7600mib3.html](http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/7600mib3.html)

## CWDM-SFP-xxxx on RSP720 GE

Platform: Cisco 7600

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

[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/15_0s/7600_hwd.html)

## DHCP Radius Proxy Enhancement

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad\\_dhcp\\_rad\\_proxy.html](http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rad_proxy.html)

## DHCP Server Radius Proxy

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad\\_dhcp\\_rad\\_proxy.html](http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rad_proxy.html)

## DWDM-SFP-xxxx 40x Wavelengths on RSP720

Platform: Cisco 7600

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

[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/15_0s/7600_hwd.html)

## DWDM-SFP-xxxx on SUP32 and 67xx-SFP on Cisco 7600 (8x Additional Wavelengths)

Platform: Cisco 7600

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

[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/15_0s/7600_hwd.html)

## GLC-GE-100FX for 1GE SFP MAC on Cisco 7600

Platform: Cisco 7600

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

[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/15_0s/7600_hwd.html)

## GTP-SLB IPv6 Support

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp\\_slb.html](http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_slb.html)

## IEEE 802.1ag-2007 Compliant CFM—Bridge Domain Support

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

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/sipsasw.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipsasw.html)

[http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce\\_cfm-ieee.html](http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee.html)

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES20\\_config\\_guide/baldfg.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldfg.html)

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES40\\_config\\_guide/es40\\_chap4.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html)

## Ingress Policing Support on EVC on Port-Channel

Platform: Cisco 7600

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

[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/bald_qos.html)

## Inline Video Monitoring on the Cisco 7600 Router

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES40\\_config\\_guide/es40\\_chap13.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html)

## IPv6 Services: DNS Lookups over an IPv6 Transport

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg\\_bsc\\_con.html](http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html)

## MPLS Point-to-Multipoint Traffic Engineering: Support for Static Pseudowires

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp\\_te\\_p2mp\\_static.html](http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_p2mp_static.html)

## MPLS VPN—BGP Local Convergence for 6VPE/6PE

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp\\_vpn\\_pece\\_lnk\\_prot.html](http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_pece_lnk_prot.html)

## Multicast MIB VRF Support

The Multicast MIB VRF Support feature is an enhancement to help manage Cisco devices in a multicast VPN (MVPN) environment using SNMP. This feature enhances the Cisco suite of supported multicast MIBs by making the following multicast MIBs VRF aware:

- CISCO-IPMROUTE-MIB
- CISCO-PIM-MIB
- IGMP-STD-MIB
- IPMROUTE-STD-MIB
- MSDP-MIB
- PIM-MIB

Multicast VRF (MVRF) awareness enables the MIB objects associated with these multicast MIBs to be queried and set for the individual MVRFs configured. In addition, MVRF awareness provides the capability to detect conditions for a trap inside of an MVRF and look up the correct information for that MVRF; the traps would then be sent to the SNMP manager that is configured for that MVRF.

For detailed information about these MIBs, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at <http://www.cisco.com/go/mibs>.

## Multicast VPN Extranet Support

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc\\_mc\\_vpn\\_extranet.html](http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_mc_vpn_extranet.html)

[http://www.cisco.com/en/US/products/ps5845/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps5845/products_installation_and_configuration_guides_list.html)

## Non-Aggregate WRED Support with 6 Profiles on OC3 and OC12 ATM SPAs

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/76cfgatm.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html)

## Non-Aggregate WRED 6 Queues on ATM and STM1 SPA

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/76cfgatm.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html)

## NSF/SSO: MPLS Point-to-Multipoint Traffic Engineering

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp\\_te\\_p2mp.html](http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_p2mp.html)

## Private Host on Pseudoport on CWAN Cards

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/flexwan\\_config/features.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html)

## Product Security Baseline: Password Encryption and Complexity Restrictions

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html)

## QoS on Port-Channel Member-Link

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES40\\_config\\_guide/es40\\_chap7.html#wp1430479](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html#wp1430479)

## REP Configurable Timers aka REP Fast Hellos

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES20\\_config\\_guide/baldfc.html#wp1710575](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldfc.html#wp1710575)

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES40\\_config\\_guide/es40\\_chap4.html#wp1520539](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1520539)

[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/routers/7600/ios/15S/configuration/guide/7600_15_0s_book.html)

[http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw\\_book.html](http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_book.html)

## SPA-1xOC3-ATM-V2, SPA-3xOC3-ATM-V2 and SPA-1xOC12-ATM-V2 Support on Cisco 7600 SIP-400 and SIP-200

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/76ovwsip.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwsip.html)

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/install\\_upgrade/7600series/7600sov.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/7600series/7600sov.html)

[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/15_0s/7600_hwd.html)

## SSO—Synchronous Ethernet (SyncE)

Platform: Cisco 7600

The SSO—Synchronous Ethernet (SyncE) feature makes the SyncE feature High Availability Stateful Switchover (SSO) compliant.

SyncE provides high-quality clock synchronization over Ethernet ports at the physical level and SSO synchronizes state information for SyncE between an active route processor and a standby route processor.

The SSO—Synchronous Ethernet (SyncE) feature is available only on Cisco 7600 series routers that are running Cisco IOS Release 15.0(1)S or later.

There are no configuration tasks associated with this feature. On a Cisco 7600 series router that is running Cisco IOS Release 15.0(1)S or later, the SyncE function will automatically be a part of the High Availability feature if you configure your router for High Availability.

For information about the SyncE feature on the Cisco 7600 series routers, see the Overview of the Ethernet SPAs document at the following location:

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/760veth.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/760veth.html)

For information about the SyncE: ESMC and SSM feature, see the Synchronous Ethernet (SyncE): ESMC and SSM document at the following location:

[http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir\\_synce.html](http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_synce.html)

## STM1E-SFP Support

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/sipsasw.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipsasw.html)

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/install\\_upgrade/7600series/SIP-SSC-SPA-HW-Install.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/7600series/SIP-SSC-SPA-HW-Install.html)

[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/15_0s/7600_hwd.html)

## Storm Control Action—Port Disable

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES40\\_config\\_guide/es40\\_chap4.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html)

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES20\\_config\\_guide/baldfcg.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldfcg.html)

## Support for IEEE 1588-2008 Precision Clock Synchronization Protocol

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/sipsasw.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipsasw.html)

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/install\\_upgrade/7600series/SIP-SSC-SPA-HW-Install.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/7600series/SIP-SSC-SPA-HW-Install.html)

[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/15_0s/7600_hwd.html)

[http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce\\_book.html](http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_book.html)

[http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir\\_book.html](http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_book.html)

## Synchronous Ethernet (SyncE): ESMC and SSM

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES40\\_config\\_guide/es40\\_chap4.html#wp1555644](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1555644)

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/760veth.html#wp1056831](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/760veth.html#wp1056831)

## TE-FRR Support on VPLS LAG NNI

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES20\\_config\\_guide/baldfg.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES20_config_guide/baldfg.html)

[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/install_config/ES40_config_guide/es40_chap6.html)

## Tunable DWDM-XFP on All ES+ 10GE

Platform: Cisco 7600

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

[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/15_0s/7600_hwd.html)

## Video Monitoring MIB Support for Medianet Video Monitoring

Platform: Cisco 7600

This feature provides support for the use of the industry-standard Simple Network Management Protocol (SNMP) to monitor media streams. This support is implemented with the addition of the following Cisco proprietary SNMP Management Information Base (MIB) modules:

- CISCO-FLOW-MONITOR-TC-MIB—Defines the textual conventions common to the following MIB modules.
- CISCO-FLOW-MONITOR-MIB—Defines the framework that describes the flow monitors supported by a system, the flows that it has learned, and the flow metrics collected for those flows.
- CISCO-MDI-METRICS-MIB—Defines objects that describe the quality metrics collected for media streams that comply to the Media Delivery Index (MDI) [RFC 4445].
- CISCO-RTP-METRICS-MIB—Defines objects that describe the quality metrics collected for RTP streams, similar to those described by an RTCP Receiver Report packet [RFC 3550].
- CISCO-IP-CBR-METRICS-MIB—Defines objects that describe the quality metrics collected for IP streams that have a Constant Bit Rate (CBR).

For detailed information about these MIBs, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at <http://www.cisco.com/go/mibs>.

This feature also includes two new command-line interface (CLI) commands and one modified CLI command. The commands are as follows:

- **snmp-server host**—Enables the delivery of flow monitoring SNMP notifications to a recipient.
- **snmp-server enable traps flowmon**—Enables flow monitoring SNMP notifications. By default, flow monitoring SNMP notifications are disabled.
- **snmp mib flowmon alarm history**—Sets the maximum number of entries maintained by the flow monitor alarm history log.

For more information about these commands, see the *Cisco IOS Master Command List*.

## WANPHY and OTN Support on ES+XC Combination Line Card

Platform: Cisco 7600

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

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES40\\_config\\_guide/es40\\_chap10.html](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap10.html)

## XFP-10G-MM-SR on 10GE Ports for Cisco 7600

Platform: Cisco 7600

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

[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/15_0s/7600_hwd.html)

## MIBs

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

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

If 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 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](mailto: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>

## Limitations and Restrictions

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.



# Important Notes

The following sections contain important notes about Cisco IOS Release 15.0S.

- [Cisco IOS Behavior Changes, page 17](#)
- [Important Notes for Cisco IOS Release 15.0S, 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 stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in this section.

- [Cisco IOS Release 15.0\(1\)S6, page 17](#)
- [Cisco IOS Release 15.0\(1\)S5, page 18](#)
- [Cisco IOS Release 15.0\(1\)S4, page 19](#)
- [Cisco IOS Release 15.0\(1\)S3a, page 20](#)
- [Cisco IOS Release 15.0\(1\)S2, page 21](#)
- [Cisco IOS Release 15.0\(1\)S1, page 24](#)

## Cisco IOS Release 15.0(1)S6

The following behavior changes are introduced in Cisco IOS Release 15.0(1)S6:

- 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/mppls/command/mp-m4.html#GUID-B64630A1-3CD7-42DE-8E86-6CD47AC8981A>

- Better optimization is possible for ACL TCAM entry consumption on Cisco 7600 platforms for Policy Based Routing (PBR).

Old Behavior: When configuring multiple PBR sequences (or a single PBR sequence with multiple ACLs) in which more than one PBR ACL contains DENY entries, the result of the merge is suboptimal in terms of the number of TCAM entries and masks used.

New Behavior: Entering the new **platform ipv4 pbr optimize tcam** command allows better optimization.

Additional Information:

<http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/layer3.html#wp1027016>

- PfR syslog levels have been added to minimize the number of messages.  
 Old Behavior: Too many PfR syslog messages are generated.  
 New Behavior: PfR syslog levels have been added to minimize the number of messages displayed, and a syslog notice has been 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>

## Cisco IOS Release 15.0(1)S5

The following behavior changes are introduced in Cisco IOS Release 15.0(1)S5:

- 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 the 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/ipv6-addrg-bsc-con.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).
- 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.
- Chopper: State of MLP bundles is not synced to stdby after SPA OIR.  
 Old Behavior: Prior to Cisco IOS Release 15.1(3)S and Cisco IOS Release 12.2(33)SRE04, the SPA-1xCHOC12/DS0 SPA boots up with the old controller status. If it was not admin down, it would start with no admin down and the interfaces come up as soon as the SPA boots up.  
 New Behavior: Effective from Cisco IOS Release 15.1(3)S and Cisco IOS Release 12.2(33)SRE05, the SPA-1xCHOC12/DS0 boots up with admin down status and the original SPA status is restored after one second of the SPA bootup. Please 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/760vwsr.html#wp1058053](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/760vwsr.html#wp1058053)
- Doc: CLI to tune ratelimit parameter for RP based LI mode.  
 Old Behavior: The command was not present in the command reference guide.

New Behavior: Updated the command reference guide with the **li-slot rp rate** command.

Additional Information: The updated guide is available here:

<http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-11.html>

## Cisco IOS Release 15.0(1)S4

The following behavior changes are introduced in Cisco IOS Release 15.0(1)S4:

- BGP no longer activates IPv6 peers in the IPv4 address family automatically.

Old Behavior: By default, both IPv6 and IPv4 capability is exchanged with a BGP peer that has an IPv6 address. When an IPv6 peer is configured, that neighbor is automatically activated under the IPv4 unicast address family.

New Behavior: Starting with new peers being configured, an IPv6 neighbor is no longer automatically activated under the IPv4 address family. You can manually activate the IPv6 neighbor under the IPv4 address family if you want. If you do not want an existing IPv6 peer activated under the IPv4 address family, you can manually deactivate the peer with the **no neighbor ipv6-address activate** command. Until then, existing configurations that activate an IPv6 neighbor under the IPv4 unicast address family will continue to try to establish a session.

Additional Information:

[http://www.cisco.com/en/US/docs/ios/iproute\\_bgp/configuration/guide/irg\\_basic\\_net.html](http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_basic_net.html)

[http://www.cisco.com/en/US/partner/docs/ios/ios\\_xe/iproute\\_bgp/configuration/guide/irg\\_basic\\_net\\_xe\\_ps11174\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/partner/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_basic_net_xe_ps11174_TSD_Products_Configuration_Guide_Chapter.html)

- The **ipv6 nd ra suppress** command is updated.

Old Behavior: The **ipv6 nd ra suppress** command only suppresses periodic unsolicited RAs. It does not suppress RAs sent in response to a router solicitation.

New Behavior: The **all** keyword was added to the command. Use of the **all** keyword with the **ipv6 nd ra suppress** command suppresses all RAs, including those sent in response to a router solicitation.

- Disable ISG on the ES+ lowQ line card.

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

New Behavior: The following restriction has been added: 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](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1554396)

- M:N LAG support provided on the port-channel access type subinterface.

Old Behavior: Only two members can be added to the port-channel access type subinterface.

New Behavior: Multiple members can be added 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](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](http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_policies_agg.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 **vcv 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 **vcv bfd template** command has no effect. Only raw BFD is used.

- MLS QoS protocol ARP police does not work with the ES+ switchport/SVI interface.

Old Behavior: Behavior on L2 interfaces is trust cos by default.

New Behavior: For switchport and SVI instances, the default port behavior is trust dscp. The cos value is now derived from the dscp value.

Additional Information:

[http://www.cisco.com/en/US/docs/routers/7600/install\\_config/ES40\\_config\\_guide/es40\\_chap7.html#wp1346147](http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap7.html#wp1346147)

- A change has been made in the **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.

- A change has been made in the **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.

## Cisco IOS Release 15.0(1)S3a

The following behavior changes are introduced in Cisco IOS Release 15.0(1)S3a:

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

Old Behavior: The DHCP server sends an 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.

- There is a new BGP error message.  
 Old Behavior: No error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels (via the **neighbor send-label** command or via a template). Sending MPLS labels to IPv6 peers is not supported.  
 New Behavior: An error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels. An example of the error message is as follows:  

```
%BGP-4-BGP_LABELS_NOT_SUPPORTED: BGP neighbor 2001:DB8:1::2 does not support sending labels.
```
- 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 MTU and TTL rate limiters are enabled by default.  
 Old Behavior: The MTU and TTL rate limiters are 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>
- Disable NP crashinfo for all Network Processor exceptions.  
 Old Behavior: A fix is required to reduce the Network Processor reload time.  
 New Behavior: Network Processor crashinfo is disabled for all Network Processor exceptions by default.  
 Impact to Customer: This fix disables crashinfo generation for all SIP400 Network Processor exceptions, which helps in improving the Network Processor reload time.  
 Additional Information:  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/7600series/760vwsip.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/760vwsip.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](http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html#wp1013065)

## Cisco IOS Release 15.0(1)S2

The following behavior changes are introduced in Cisco IOS Release 15.0(1)S2:

- ISG can be configured to not update subscriber sessions with data from reauthentication profiles.  
 Old Behavior: 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](http://www.cisco.com/en/US/docs/ios/isg/command/reference/isg_m1.html)

- Command functionality and output change.

Old Behavior: Client notification timer was not displayed in output of the **show redundancy states** command.

New Behavior: The output now includes configuration for the client notification timer.

```
router# show redundancy states
my state = 13 -ACTIVE
peer state = 4 -STANDBY COLD
Mode = Duplex
Unit = Secondary
Unit ID = 2

Redundancy Mode (Operational) = RPR
Redundancy Mode (Configured) = RPR
Redundancy State = RPR
Maintenance Mode = Disabled
Manual Swact = enabled
Communications = Up

client count = 53
client_notification_TMR = 240000 milliseconds <=====New output
keep_alive TMR = 9000 milliseconds
keep_alive count = 0
keep_alive threshold = 18
RF debug mask = 0x0
```

- The **show ip multicast rpf tracked** command is no longer supported.

Old Behavior: The **show ip multicast rpf tracked** command is available for use. However, it is not recommended that customers use this command.

New Behavior: The **show ip multicast rpf tracked** command is removed.

Additional Information:

[http://www.cisco.com/en/US/docs/ios/ipmulti/command/reference/imc\\_06.html](http://www.cisco.com/en/US/docs/ios/ipmulti/command/reference/imc_06.html)

- Specific BGP show commands display dampening information on an individual VRF basis.

Old Behavior: The following commands display flap-statistics, dampened-paths, and dampening parameters of VRFs under the VPNv4 or VPNv6 address family identifier:

- **show ip bgp all dampening**
- **show ip bgp vpnv4 all dampening**
- **show ip bgp vpnv6 unicast all dampening**

New Behavior: Because VRFs can have dampening enabled independently of other VRFs and the global VPNv4 and VPNv6 topologies, the following commands display flap-statistics, dampened-paths, and dampening parameters of individual VRFs under that VRF name:

- **show ip bgp all dampening**
- **show ip bgp vpnv4 all dampening**
- **show ip bgp vpnv6 unicast all dampening**

If dampening is not enabled for a VRF, that is stated under the VRF name.

For more information, see the Cisco IOS IP Routing: BGP Command Reference.

- The **ipv6 access-class** command has been changed.

Old Behavior: A crash occurs when removing an IPv6 access list that is still applied to a vty.

New Behavior: The phrase “Identical restrictions should be set on all the virtual terminal lines because a user can connect to any of them” has been added so users can avoid this problem.

Additional Information:  
[http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6\\_05.html](http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_05.html)
- Prevent ARP packet drop by setting ARP packet priority.

Old Behavior: Network congestion causes ARP packets to drop because the ARP packet priority is not enabled.

New Behavior: A new command **arp packet-priority enable** was added. Use the **arp packet-priority enable** command when a network congestion causes ARP packets to drop. Enabling ARP packet priority significantly reduces the number of ARP packet drops.

Additional Information:  
[http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad\\_arp.html](http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_arp.html)
- Rate limit SIP200\_MP-4-PAUSE message to avoid console flooding

Old Behavior: In scaled scenario, SIP200\_MP-4-PAUSE messages take on a lot of logging space and in the process other important logs might get missed.

New Behavior: SIP200\_MP-4-PAUSE message to avoid console flooding.

Impact to customer: 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.
- 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 BGP address families do not come up. This is because the router is receiving messages from a neighbor that the AFI or SAFI is not supported, and the router does not retry those AFIs. The output of show ip bgp all 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 simply 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.

## Cisco IOS Release 15.0(1)S1

The following behavior changes are introduced in Cisco IOS Release 15.0(1)S1:

- WRED: CLI-configured qlimit does not affect WRED min/max threshold

Old Behavior: If no queue-limit is configured, the queue-limit for the current class is based on the parent values for available buffers and current class allocated bandwidth. In the implicit WRED min/max scenario, thresholds were calculated from the available buffers.

For random-detect behavior, in the implicit WRED min/max scenario, thresholds are calculated from the available buffers.

New Behavior: The queue-limit is always calculated from the parent queue-limit and allocated bandwidth in the current class. When you use the **queue-limit** command to explicitly configure the values, these values are used as the definition of the queue-limit.

For random detect behavior, thresholds are calculated from the available aggregate queue-limit for that class.

Additional Information:

[http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos\\_q1.html](http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_q1.html)

- Active Flow Counts in NetFlow

Old Behavior: The total number of active NetFlow flows in a module obtained from an SNMP query is always instantaneous value.

New Behavior: A new keyword, **cache**, is added to the **mls netflow** command. When the **mls netflow cache** command is executed, the command returns a cached value of the total active flow count. The cached value is updated every 30 seconds.

Additional Information:

[http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf\\_02.html#wp1136217](http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_02.html#wp1136217)

- PPPoA sessions fail to sync up with stand-by after SSO in a scaled setup

Old behavior: Documentation for the **show checkpoint** command was missing in the BBDSL Command Reference

New behavior: Added the **show checkpoint** command to the BBDSL Command Reference at the following location:

[http://www.cisco.com/en/US/docs/ios/bbds/command/reference/bba\\_03.html#wp1045985](http://www.cisco.com/en/US/docs/ios/bbds/command/reference/bba_03.html#wp1045985)

- ISG can be configured to use the SSG format for the ssg-control-info accounting attribute.

Old Behavior: ISG reverses the inbound and outbound data values in the ssg-control-info attribute.

New Behavior: The **subscriber accounting ssg** command allows ISG to use the same format as SSG for the ssg-control-info attribute.

Additional Information:

[http://www.cisco.com/en/US/docs/ios/isg/command/reference/isg\\_m1.html](http://www.cisco.com/en/US/docs/ios/isg/command/reference/isg_m1.html)

## Important Notes for Cisco IOS Release 15.0S

This section describes important issue that you should be aware of for Cisco IOS Release 15.0S.

### DECNET MOP

The advipservices images do not support DECNET MOP in Cisco IOS Release 15.0S.



## 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/public/sw-center/sw-content.shtml>

## Field Notices and Bulletins

For general information about the types of documents listed in this section, see the following document:

- **Field Notices**—We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account with Cisco.com, you can find field notices at [http://www.cisco.com/en/US/customer/support/tsd\\_products\\_field\\_notice\\_summary.html](http://www.cisco.com/en/US/customer/support/tsd_products_field_notice_summary.html). If you do not have a Cisco.com login account, you can find field notices at [http://www.cisco.com/en/US/support/tsd\\_products\\_field\\_notice\\_summary.html](http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html).
- **Software Center**—Visit the Software Center/Download Software page on Cisco.com to subscribe to Cisco software notifications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Software Center/Download Software page at <http://www.cisco.com/cisco/web/download/index.html>.

## Caveats

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.

Because Cisco IOS Release 15.0S is based on Cisco IOS Release 12.2SR, many caveats that apply to Cisco IOS Release 12.2SR also apply to Cisco IOS Release 15.0S. For information on severity 1 and 2 caveats in Cisco IOS Release 12.2SR, see the *Caveats for Cisco IOS Release 12.2SR* document located on Cisco.com.

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](http://www.cisco.com) and go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](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 15.0(1)S6**, page 26
- **Resolved Caveats—Cisco IOS Release 15.0(1)S5**, page 35

- [Resolved Caveats—Cisco IOS Release 15.0\(1\)S4a, page 62](#)
- [Open Caveats—Cisco IOS Release 15.0\(1\)S4, page 63](#)
- [Resolved Caveats—Cisco IOS Release 15.0\(1\)S4, page 63](#)
- [Resolved Caveats—Cisco IOS Release 15.0\(1\)S3a, page 85](#)
- [Resolved Caveats—Cisco IOS Release 15.0\(1\)S2, page 119](#)
- [Resolved Caveats—Cisco IOS Release 15.0\(1\)S1, page 135](#)
- [Open Caveats—Cisco IOS Release 15.0\(1\)S, page 153](#)
- [Resolved Caveats—Cisco IOS Release 15.0\(1\)S, page 165](#)

## Resolved Caveats—Cisco IOS Release 15.0(1)S6

Cisco IOS Release 15.0(1)S6 is a rebuild release for Cisco IOS Release 15.0(1)S. The caveats in this section are resolved in Cisco IOS Release 15.0(1)S6 but may be open in previous Cisco IOS releases.

- CSCth96200

Symptoms: A continuous traceback is seen:

```
%FRR_OCE-STBY-3-GENERAL: un-matched frr_cutover_cnt.
-Traceback= 7021958 70217D4 7021A34 7034130 4686294 4671348 4A2E548 4682AA4 4683524
4F69DA4 4F63664
```

Conditions: This symptom is seen with the FRR feature configured and possibly under scale conditions.

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.

- CSCti04788

Symptoms: High CPU utilization upon flapping of the core-facing interface being used by EoMPLS.

Conditions: Scale > 1000 VCs.

Workaround: There is no workaround. The CPU will return to normal after a brief period of high CPU utilization. However, other routing protocols may flap.

- CSCti62936

Symptoms: The router crashes when a situation is created with bandwidth 0 on an EVC and then the queue limit is modified.

Conditions: This symptom occurs when bandwidth 0 is created on an EVC and then the queue limit is modified.

- Workaround: There is no workaround.
- CSCtj29754
 

Symptoms: Different behavior between static IPv6 and IPv4 routes is seen.

Conditions: A default IPv6 route and an IPv6 static route with an IPv6 address as the next hop must be configured. When the interface of the next hop goes down, the next hop will be resolved via the default route and the route will still be seen as active in the routing table. This is not the case with IPv4. With IPv4, the static route would be removed from the routing table.

Workaround: Use a fully specified static route where the interface and the next hop address are configured.
  - 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.
  - CSCto86079
 

Symptoms: Continuous diag failure and CRC errors are seen.

Conditions: This symptom is observed upon entering the **no mls switching** command, followed by the **mls switching** command, bus stall is called.

Workaround: Fix description: Disable the DDR sync between argos and SSA before the superman is configured for mls switching, and re-enable the DDR sync after the config is made on superman. Re-sync is done twice in the fix, since with one resync we are still facing diag failures on this card.
  - 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.
  - 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”.
  - 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.

- 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.

- CSCtr87070

Symptoms: Enable login failed with error “% Error in authentication”.

Conditions: The symptom is observed with TACACS single-connection.

Workaround: Remove TACACS single-connection.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCtu90140

Symptoms: A chunk memory leak is observed.

Conditions: A chunk memory leak is seen after configuring the IP source guard.

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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(01.16)S.

Workaround: There is no workaround.
- 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 exist.
  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.
- 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.
- 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.

- 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
```
- 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.
- 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.
- CSCtx94279
 

Symptoms: A line card crashes.

Conditions: This symptom is observed in switch traffic and flood traffic (line rate and less than 128-byte packet size) with more than one port in the egress path flood.

Workaround: There is no workaround.
- 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.

- 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.

- 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.

- 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.
- 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).
- 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.
- CSCtz30983

Symptoms: Crash on ES+ line card upon issuing the **show hw-module slot X tech- support** or **show platform hardware version** command. This is similar to CSCti78408.

Conditions: This symptom occurs on an ES+ line card.

Workaround: Do not issue the **show hw-module slot X tech-support** or the **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 than 2M to avoid blocking of the BPDU PW.
- 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: This symptom is seen when service policies less than 128 kb are added or removed.

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: This symptom is seen in Cisco IOS SREx and RLSx releases.

Workaround: Use ingress replication.

## Resolved Caveats—Cisco IOS Release 15.0(1)S5

Cisco IOS Release 15.0(1)S5 is a rebuild release for Cisco IOS Release 15.0(1)S. The caveats in this section are resolved in Cisco IOS Release 15.0(1)S5 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 router 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.

- 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.

- 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.

- CSCso46409

Symptoms: mbrd\_netio\_isr and crypto\_engine\_hsp\_hipri traceback log messages are produced.

Conditions: This symptom is observed while using WebVPN on a Cisco 3845 router with an AIM-VPN/SSL-3.

Workaround: There is no workaround.

- CSCsq02771

Symptoms: DHCP relay may hang when a request for an IP address is received from a DHCP client on an unnumbered MPLS and VPN setup.

Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Interim Release 12.4(19.16)T1.

Workaround: There is no workaround.

- 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.

- 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.
- 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](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html)

Workaround: There is no workaround.
- CSCtf35224
 

Symptoms: When using Cisco IOS Release 12.2(33)SRD3, UDP broadcast traffic cannot be forwarded correctly through flexwan line card of the Cisco 7600 series router. There are some count values that are increasing on serial interface of brand router, but there was no output from the **debug ip packet** command on brand router.

Conditions: When using Cisco IOS Release 12.2(33)SRD3 based on below topology, UDP broadcast traffic cannot be forwarded correctly using the **ip helper-address x.x.x.x** command.

```
2800-4 (Pagent) [F0/0] <-----> [Gi6/2] 7600-2 [S4/0/0:1] <----Serial back-
to-back-----> [S0/3/0:1] 2800-5
```

Traffic Pattern from Pagent is below.

  - tgn L3-src-addr 10.1.1.2
  - tgn L3-dest-addr 192.168.234.255
  - tgn L4-src-port 1234
  - tgn L4-dest-port 1234

Workaround: When using Cisco IOS Release 12.2(33)SRC1, UDP broadcast traffic can be forwarded correctly using the **ip helper-address x.x.x.x** command.
- 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.
- CSCth10764
 

Symptoms: PPP Negotiation not working correctly between Cisco GSR XR router and Cisco 7200 series router.

Conditions: Max-header size different on both ends, PPP not negotiating lower size.

- Workaround: There is no workaround.
- 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.
  - CSCti04919
 

Symptoms: While unconfiguring and reconfiguring the VRF, PIM neighborship goes down in a specific scenario.

Conditions: This symptom occurs if the PIM MDT GRE tunnel takes more time to come up compared to other interfaces in the VRF.

Workaround: Toggle the default MDT.
  - 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.
  - 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.
  - 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: This symptom is observed when the automated test script is run on three connected routers.

Workaround: Adding a **no shut** on the UUT interface with UP- MEPS before doing the LeakConfig seems to prevent the crash and provide a clean run. Do not run the automated script.

Further Problem Description: Other problems observed are as follows:

    - The CFM MIB will return infinite results for getmany.
    - A **show** command will crash the router.
    - Stale Earl Adjacency entries remain while adding or removing EVCs. Reload the LC to resolve the issue.
  - 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.

- CSCtj56551

Symptoms: The Cisco 7600 series router crashes in a very rare case.

Conditions: This symptom is observed very rarely when route-churn/sessions come up.

Workaround: There is no workaround.

- 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 Policy Based Routing (PBR) using the second next-hop.

Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are policy based routed 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.

- 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 series router. Preferably it should not take any action. For example, it should not affect any other working features.

Workaround: Unconfigure the command by typing the **no ip cef accounting non- recursive** command.

- 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.

- CSCtk62763

Symptoms: A Cisco 7600 series 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.

- CSCtl09030
 

Symptoms: The Cisco ASR 1000 series router configured to function as ISG and DHCP relay/server crashes in the ARP input process or IP inband session initiator process in dhcpd\_find\_binding function.

Conditions: This symptom is observed when the Cisco ASR 1000 series router is configured with DHCP relay or server and DHCP initiated IP sessions are configured. This issue is seen when the ISG inband IP session initiator is configured and an ARP request is received from a client whose DHCP IP session has timed out or cleared.

Workaround: Disable ISG DHCP session initiator.
- CSCtl86141
 

Symptoms: Data traffic is switched over BPDU PW. This issue can result in MAC-FLAPs over the multiple MST rings configured to be part of MST 0 instances (configured along with RL2GP) as BPDU PW acts as a loop in the network connectivity for those MST rings.

Conditions: This symptom is observed when data traffic is received on the access VLAN on which BPDU PW is configured.

Workaround: There is no workaround. This issue is not expected to be seen on the customer VLAN as data traffic is not expected over the native VLAN.
- 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.
- 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.

- 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.
- CSCtn22523
 

Symptoms: IPSLA udp-jitter probes may crash at saaAddSeqnoDupQ in Cisco IOS Release 12.4T/15.0M. There is no impact to other releases.

Conditions: This symptom is observed when the network experiences delay, and reordered and duplicate packets can trigger this problem when IPSLA udp-jitter is scheduled.

Workaround: Disable udp-jitter probes.
- CSCtn25681
 

Symptoms: The following error messages may be displayed in the log on the Cisco Catalyst 6500 series switches:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x41634A64 reading 0x110
%ALIGN-3-TRACE: -Traceback= 41634A64 41636CB4 41637CB0 41637EDC 4162E65C
416690F0 416690DC 00000000
```

Conditions: This symptom is observed when TACACS+ is configured on the switch.

Workaround: There is no workaround.
- CSCtn52529
 

Symptoms: After the TE tunnels are recovered and resignaled, a timer is started to wait for the RESV to come in. If the RESV does not arrive, the timer is restarted and the PATH is sent out again. In this DDTs, the PATH was not being sent out after the timer expired.

Conditions: This symptom occurs after the TE tunnels are recovered and resignaled and the RESV does not arrive after the timer is started.

Workaround: There is no workaround.
- CSCtn58128
 

Symptoms: BGP process in a Cisco ASR 1000 series router that is being used as a route reflector may restart with a watchdog timeout message.

Conditions: This issue may be triggered by route-flaps in a scaled scenario where the route reflector may have 4000 route reflector clients and might be processing more than a million routes.

Workaround: Ensure “no logging console” is configured.
- 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 Cisco IOS Release 12.2(33)SRB and later. The earlier versions are not affected.

This can only happen for some prefixes with different mask length, e.g. 10.0.0.0/24 and 10.0.0.0/26, but not for 10.0.0.0/24 and 10.0.0.1/32, because 10.0.0.0 is not the same prefix as 10.0.0.1.

1. Assume there is a prefix, 10.0.0.0/24, is imported from vpnv4 to vrf. It has been allocated a label of 16.
2. If the allocated label changes from 16 to 17, e.g. due to interface flapping or BGP attribute change.
3. However, before BGP import happens, if there is a more specific prefix, e.g. 10.0.0.0/26, is added to the BGP radix tree, but it is denied for importing due to, e.g. RT policy.

Workaround: Remove RT or import map and re-added it back. However, please note, if the above condition happens again, the issue could be seen again.

- 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.

- CSCto43868

Symptoms: Traffic loss is seen for MVPN streams.

Conditions: This symptom is observed during the following triggers in both per-prefix/per-vrf mode with traffic:

Triggers: slot 7 reload on UUT, clear ip bgp \* on UUT,uut reload, core router reload.

Workaround: There is no workaround.

- CSCto52194

Symptoms: With the P2MPTE scenario, some of the met3 entries are not programmed properly.

Conditions: This symptom occurs with shut/no shut of the interface.

Workaround: There is no workaround.

- CSCto64188

Symptoms: The Cisco ASR series router may unexpectedly reload if WCCP mask assignment changes while the **show ip wccp service detail** command is in progress.

Conditions: This symptom occurs when WCCP mask assignment is in use. The **show ip wccp service detail** command displays a WCCP client mask assignment table while, at the same time, the service group mask assignments are changed.

Workaround: Do not use the **detail** keyword while WCCP redirection assignments may be changing. Instead, use the **clients** and **assignment** keywords.

For example, if mask assignments may be changing, use the following two commands:

- **show ip wccp web-cache clients**
- **show ip wccp web-cache assignment**

instead of the following command:

**show ip wccp web-cache detail**

- 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.

- CSCto71004

Symptoms: Router crashes with high scale and a lot of BGP routes and scaled mpls l3 vpns enabled. 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. Setup had scaled mpls l3 vpns enabled.

Following messages were seen when this issue was hit:

```
%COMMON_FIB-SP-6-FIB_RECURSION_VIA_SELF:
10.173.30.125/32 is found to resolve via itself during setting up
switching info
%COMMON_FIB-SP-6-FIB_RECURSION_VIA_SELF:
10.173.19.16/30 is found to resolve via itself during setting up
switching info
%COMMON_FIB-SP-6-FIB_RECURSION_VIA_SELF:
10.173.19.17/32 is found to resolve via itself during setting up
```

switching info

Workaround: There is no workaround.

- CSCto72629

Symptoms: A MAXAGE LSA is repeatedly retransmitted bringing down the OSPFv3 adjacency.

Conditions: This symptom occurs when the unadjusted age of the LSA in the OSPFv3 database (as opposed to the advertised age, which includes time spent in the database) is less than MAXAGE. Note that the age of the LSA in the database is not updated once it is installed unless maxaging is initiated by OSPFv3 process.

Workaround: Use the **clear ipv6 ospf process** command to clear the OSPF state based on the OSPF routing process ID.

- CSCto79174

Symptoms: A Cisco 7600 series 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.

- CSCto84267

Symptoms: PRE crashes after CPU hogs (due to PPP Event) are observed.

Conditions: This symptom occurs several seconds before the reload, when the following message is seen in the logs:

```
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
(20/17),process = PPP Events.
```

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.

- CSCto90656

Symptoms: The 24CT1/E1 card sends a packet with errors. (The inbound interface indicates frame and CRC errors.)

Conditions: This symptom occurs when connected with a simulator and only occurs on port 0 and 1 on ESR-24CT1/E1. The reported tested release and combination is as follows:

- PRE4 Cisco IOS Release 12.2(33)SB10 -> NG
- PRE2 Cisco IOS Release 12.2(33)SB10 -> NG
- PRE2 Cisco IOS Release 12.2(31)SB5 -> NG
- PRE1 Cisco IOS Release 12.0(27)S4 -> Good

Workaround: Reconfigure the **clock source** command in the following order:

1. Type **clock source line** in controller configuration mode.
2. Type **clock source internal** in controller configuration mode.
3. Type **clock source line** in controller configuration mode.

After this configuration, the symptom is cleared. However, after reloading the chassis, the issue recurs.

- 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.

- CSCtq21234

Symptoms: Label is not freed.

Conditions: The symptom is observed after shutting down the link.

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 than 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.

- 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.

- CSCtq57709

Symptoms: LC crash is observed.

Conditions: This symptom occurs when the encapsulation is changed.

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.

- 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.

- CSCtq64072

Symptoms: A DHCP release received on a different member link of a PC other than the one on which it was requested is considered as fake and dropped.

Conditions: This symptom occurs with the DHCP client release/decline message. The binding interface must match before the binding entry is removed to prevent someone from faking these messages to delete others' valid binding.

Workaround: There is no workaround.

Further Problem Description: In case of a port-ch, the stored hwidb for a binding is that of the bridge interface. When a release is received on the other member-links, the hwidb does not match.

- CSCtq67680

Symptoms: A 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.

- 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.

- 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.

- 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.

- 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.

- CSCtq96329

Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. This could also result in memory corruption or 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.

- 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.

- 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.

- CSCtr14852  
Symptoms: A Cisco 7600 series 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.

- CSCtr22007

Symptoms: A Cisco 7600 series router that is configured with RSVP crashes.

Conditions: MPLS-TE Tunnel Flap.

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>

- CSCtr33918

Symptoms: Convergence is observed in the order of 1-6 seconds of multicast/video traffic on a Cisco 7600 series router 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.

- 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.

- 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 series router 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: 00000000 . . .

```

```

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.

- CSCtr37073

Symptoms: WS-X6196-RJ-21 and WS-X6148X2-RJ-45 may fail to come online on the Cisco 7600 series router when running SRC or higher images.

Conditions: This symptom occurs when SRC or higher images are run on a Cisco 7600 series 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.
- 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>
- 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 series 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.

- CSCtr79347

Symptoms: A Cisco ASR1006 router 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.

- 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.

- CSCtr88739
 

Symptom 1: The 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: These symptoms are only observed with routes with the same prefix, but a different mask length. For example, 15.0.0.0/32, 15.0.0.0/31, 15.0.0.0/30 ..... 15.0.0.0/24, 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.
- 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>
- 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.
- CSCts12193
 

Symptoms: With the single hop MPLS TE tunnel from the core router to the PE router, removing the MDT default configuration may cause some control planes to go down (like LDP, BGP). This is due to misprogrammed adjacency in the hardware.

Conditions: This symptom occurs when unconfiguring the MDT default configuration.

Workaround: Restore the configuration.
- CSCts13255
 

Symptoms: Standby SUP crash is observed on the Cisco 7609 router after upgrade to 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 7609 router after upgrade to c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is also seen with Cisco IOS Release 12.2(33)SRE.

Workaround: There is no workaround.

- CSCts15072

Symptoms: Multicast traffic in the MVPN solution is dropped.

Conditions: This symptom is observed on a Cisco 7600 series router 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.

- 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.

- 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.

- CSCts37435

Symptoms: MVPN groups are not populated in the VRF.

Conditions: This symptom is observed in MVPN with an ACL.

Workaround: There is no workaround.

- CSCts38429

The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.





```
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.

- CSCts48540

Symptoms: PXF drop occurs on the MPLS-enabled interface due to “acl denied” on the Cisco 10000 series router configured with LI targets.

Conditions: This symptom occurs when all the uplinks are MPLS-enabled and the aggregate or default route for the LI target prefix is advertised via MP-BGP from RR or PE routers.

Workaround 1: Make sure that LI tap is applied to a non-MPLS interface only.

Workaround 2: Remove the LI tap configuration.

Workaround 3: If the LI target prefix flaps, make sure to avoid it, if possible.

- 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.

- 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.

- 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 router 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.

- CSCts63737

Symptoms: LI intercepts traffic from all L3 MPLS VPNs that have the target IP address in RIB.

Conditions: This symptom is observed with L3 MPLS VPNs with a duplicate IP addressing scheme and when LI tap is applied to one of the duplicate addresses. This issue is seen when the target route is flapped.

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 disable-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**.
- CSCts66808
 

Cisco IOS Software contains a queue wedge vulnerability that can be triggered when processing IP tunneled packets. Only Cisco IOS Software running on the Cisco 10000 Series router has been demonstrated to be affected.

Successful exploitation of this vulnerability may prevent traffic from transiting the affected interfaces.

Cisco has released free software updates that addresses this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-c10k-tunnels>
- CSCts81327
 

Symptoms: On a Cisco 10000 series router that has LI done with a session brought up via radius and that is using SNMP session ID taps, LI is not working.

Conditions: This symptom is observed only when using session ID taps in SNMP and bringing up sessions via radius.

Workaround: There is no workaround.
- CSCts81427
 

Symptoms: With a scaled dLFloATM 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.
- 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.
- 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: V11 : 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: V11 : 1
1013: NDE_1013 : 1013
1015: NDE_1015 : 1015

```

Workaround: Reload the device.

- CSCtt1787

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.

- CSCtt19442
 

Symptoms: A 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.
- CSCtt25612
 

Symptoms: The router crashes with traceback error messages and the standby takes over. After this, the router is stable.

Conditions: There is no known trigger or changes that were made as per the user update.

Workaround: There is no workaround.
- 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.
- CSCtu00150
 

Symptoms: When “oam-ac emulation” is configured on xconn, OAM is not received on the AC, indicating that the oam-ac is down on both the Cisco 10000 series PE routers.

Conditions: This symptom is observed with Cisco IOS Release 15.0(1)S. This particular issue is not seen in the Cisco IOS 33SB image, but only in the Cisco IOS Release 12.2(33)XNG (v150\_1\_s\_xe31\_throttle) image.

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 00000000 .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.

- 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 or reconfigure local connect.

- 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.

- 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**

## Resolved Caveats—Cisco IOS Release 15.0(1)S4a

Cisco IOS Release 15.0(1)S4a is a rebuild release for Cisco IOS Release 15.0(1)S. The caveats in this section are resolved in Cisco IOS Release 15.0(1)S4a 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.

- CSCtr22007

Symptoms: A Cisco 7600 router that is configured with RSVP crashes.

Conditions: This symptom occurs with MPLS-TE tunnel flap.

Workaround: There is no workaround.

## Open Caveats—Cisco IOS Release 15.0(1)S4

Cisco IOS Release 15.0(1)S4 is a rebuild release for Cisco IOS Release 15.0(1)S4. The caveat in this section is open in Cisco IOS Release 15.0(1)S4. This section describes only select open caveats.

- 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.

## Resolved Caveats—Cisco IOS Release 15.0(1)S4

Cisco IOS Release 15.0(1)S4 is a rebuild release for Cisco IOS Release 15.0(1)S. The caveats in this section are resolved in Cisco IOS Release 15.0(1)S4 but may be open in previous Cisco IOS releases.

- CSCtb24959

Symptoms: The router may crash while clearing a large number of RP mappings.

Conditions: This symptom occurs when you configure the router as an RP agent and candidate RP for a large number of RPs. This issue is seen when you run the **clear ip pim rp-map** command several times.

Workaround: Do not run the **clear ip pim rp-map** command several times in succession.

- CSCtf81249

Symptoms: Memory leaks occur while configuring Cisco IOS commands.

Conditions: This symptom is observed only when configuring from tclsh.

Workaround: Use the **end** command specifically to avoid any leaks.

- CSCth90147

Symptoms: The router will respond to an RS with an RA.

Conditions: The symptom is observed when you configure the **ipv6 nd ra suppress** command. This command is only intended to suppress periodic mcast RAs. The router will still respond to unicast RS (that is intended behavior).

Workaround: Use an ACL to block the reception of RS packets.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCti70931

Symptoms: The VTY performing the configuration hangs. The console is still alive, but is not very responsive. The **show processes cpu** command output shows high CPU utilization.

Conditions: This symptom occurs when configuring 200 call policy sets with a large number of entries.

Workaround: Around 100 entries seems to work. Thus, limit the number of entries.

- 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.

- CSCti92812

Symptoms: After physical interface flap, the GRE tunnel for VRF does not come up correctly.

Conditions: This symptom occurs when the GRE tunnel is configured for the default (global) routing table.

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCtj20776

Symptoms: Accounting-stop record is sent for radius proxy session when reauthentication happens for that session.

Conditions: This symptom is seen in the following scenarios:

1. The authentication request comes from AP.
2. The accounting request comes from AZR and the session on ISG is associated to AZR.
3. ISG receives a reauthentication 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls>

- CSCtj44374

Symptoms: The VTY performing the configuration hangs. The console is still alive, but is not very responsive. The **show processes cpu** command output shows high CPU utilization.

Conditions: This symptom occurs when configuring 200 call policy sets with a large number of tables.

Workaround: Around 100 tables seems to work. Thus, limit the number of tables.

- CSCtj58672

Symptoms: MallocLite memory leak occurs at function `vlan_bl_util_process_bitlist`.

Conditions: This symptom occurs when loading the Cisco IOS Release 15.1(1)S image with the L3vpn and BFD profile configuration.

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 the 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 temporarily, but it can reappear. The issue is specific to policers. If possible, shapers can be used instead of policers to avoid the issue.

- 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 a backup.

Workaround: Do shut/no shut on PfR master or PfR border.

- CSCtj92247

Symptoms: Standby reloading occurs due to configuration synchronization.

Conditions: This symptom occurs when you try to modify the parameters, for example, Peak value, of a vp that is already created.

Workaround: There is no workaround.

- 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: This symptom occurs when a member link of L2 port-channel that is passing traffic is removed from the port-channel.

Workaround: Remove and add the port-channel configurations 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 would resolve this issue.

- 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. The 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 multilink group** <> command.

Workaround: There is no workaround.

- CSCtl67150

Symptoms: PPP multilink interfaces fail to come up on the serial interface in Cisco ASR 1000 series routers.

Conditions: This symptom occurs under the following conditions:

1. When you create one or more than one t1 channel groups in a CT3 interface.
2. When you create a multilink interface.
3. When you create one link per channel group.
4. When the encapsulation for every link is PPP, authentication CHAP.
5. When the multilink interfaces fail to come up.

Workaround: There is no workaround.

- 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.

- 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.

- CSCtl93514

Symptoms: QoS configurations do not get applied on the interfaces when the router is upgraded from ES20 to ES+.

Conditions: This symptom occurs 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.

- 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.

- 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.

- 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**

- 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 an 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.

- 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.

- CSCtn42029

Symptoms: PXF CPU CEF memory leak at HW Mac rewrite component.

```
#sh pxf cpu cef memory
FP CEF/MFIB/TFIB XCM Type usage:
Type  Name  Col  Total  Alloc  Size  Start      End      BitMap  Error
...
   6  Mac   5    524279  383641  8     30800000  30C00000  CB394174  0          <===
HW Mac rewrite memory allocation level
...
C10K CEF/MFIB/TFIB PXF allocations:
Types      Alloc  Failed
Leaves     65598   0
Nodes      21205   0
Loadinfo   2047    0
Adjacency  87576   0
Rewrite    383642  0          <=== HW Mac rewrite allocated memory
```

Conditions: This symptom is observed when lawful intercept taps are configured on the router.

Workaround: Use the following workarounds:

1. Switchover.
2. Reload.
3. Remove all LI taps.

- 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.

- 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.

- CSCtn56526

Symptoms: In the present XE32 software, MBS is being calculated based on the MTU value always. The user-defined MBS value is not shown in the **show atm pvc** command output.

Conditions: This symptom occurs under the following conditions:

1. When you configure the MBS from the CLI.
2. When you use the **show atm pvc** command.
3. When MBS does not reflect the configured value. Its value is always based on MTU size.

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 symptom 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.

- CSCtn65599

Symptoms: Some multicast streams from CE are not forwarded to the Data MDT by PE.

Conditions: This symptom is observed only after SSO or PRE crash.

Workaround: There is no workaround.

- 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 Cisco 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.

- 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

- 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 bypass the policer and cause high CPU.

Conditions: This symptom is observed on an ES+ switchport/SVI interface with “mls qos protocol arp police <>” enabled on the router.

Workaround 1: Broadcast storm control could be used to rate-limit arp broadcast packets.

Workaround 2: The following policy can be configured on the interfaces (applicable only after Cisco IOS Release 12.2(33)SRE3, 15.0(01)S2, 15.1(01)S01, and 15.1(2)S onwards):

```
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

```

Then, dscp-transparency enabled using the following CLI:

```
no mls qos ip rewrite dscp slot <module>
```

- 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.

- 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
!

ROUTER2:
-----
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

ROUTER3:
-----
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

```

Crash reproduce steps are as follows:

1. Traffic travel from ROUTER3 to ROUTER2.
2. “clear bgp ipv4 unicast 10.1.1.1” on ROUTER2.

Workaround: There is no workaround.

- CSCtn98642

Symptoms: The Cisco ASR RP crashes with the following message:

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Ether-SPA background process
```

Conditions: This symptom occurs if a large-scale configuration has QinQ and QinQ-Any with the same outer vlan on SPA. This issue can occur during router reload. Note that QinQ (min 50+) and QinQ-Any with the same outer vlan must be present for this issue to occur.

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 SRE2 and SRE3 with MLACP deployment.

Workaround: There is no workaround.

- CSCtn99440  
Symptoms: LC CPU high is due to the mfib-const-ic process.  
Conditions: This symptom is observed for scaled mypn gre configs when more gre mdt tunnels come up.  
Workaround: There is no workaround.
- CSCtn99858  
Symptoms: Crashinfo is seen.  
Conditions: This symptom is observed during an 8k session.  
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.
- 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:
  1. Create an IOS image that does not IPV6 enabled.
  2. Enable BFD on an interface.
  3. 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 ReloadCisco has released free software updates that address these vulnerabilities.  
Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls>

- 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.
- 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.
- CSCto15040
 

Symptoms: When configuring a service instance under the physical interface, the service instance may not be programmed properly on the Switch Processor or the line card, leading to loss of connectivity.

Conditions: This symptom is observed when configuring the service instance under the physical interface of an ES+/ES20/SIP-600 card. This issue is seen with Cisco IOS Release 12.2(33)SRE or later releases.

Workaround: Configure the port in a channel-group and move the service instance configuration under the port-channel interface.
- CSCto15361
 

Symptoms: MF: Active Supervisor crashes after removing the “router eigrp” configuration.

Conditions: This symptom occurs when the Active Supervisor crashes while disabling the Ipv6 router eigrp because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.

Workaround: Modify the igrp2\_procinfo\_free function to kill the EIGRP Hello process prior to cleaning up the peer list.
- 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/readd 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.

- 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.

- CSCto43154

Symptoms: A Cisco device 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 a Cisco device running Cisco IOS.

Workaround: There is no workaround.

- CSCto44396

Symptoms: If a 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 later updated as MDI flow.

Workaround: Remove and reattach 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 the client side.

- 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.

- CSCto46877

Symptoms: Multicast and unicast stream recovery over ATM link into core after a pxf crash takes more time with XNG2. After a pxf crash, multicast convergence takes more time.

Conditions: This symptom is observed when a pxf crash occurs on the Cisco 10000 platform.

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 should be running Cisco IOS Release 15.1(1)S1.

Workaround: There is no workaround.
- CSCto52235
 

Symptoms: The MAC address accounting CLI is missing on the Cisco ASR 1000 series router.

Conditions: This symptom occurs on the Cisco ASR 1000 series router.

Workaround: There is no workaround.
- 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.
- 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.
- 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.
- 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.

- 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.

- CSCto64240

Symptoms: Unable to configure port-channel access sub-interface with three member-links.

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.

- CSCto71075

Symptoms: High CPU usage is seen on changing root node multiple times in an MLDP setup. Loss of pim neighborhood 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.

- 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.

- 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.
- 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.
- 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 the --more-- prompt, the CLI can end up referencing wrong data, resulting in router reset.

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 few multicast-related configurations of PTP are configured on the Cisco 7600 router.
- 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.

- CSCto83789  
Symptoms: When mem-link flaps, this CLI will not be inherited to all the EFPs configured under PC.  
Conditions: This symptom occurs when the CLI to disable control-packets on the hi-p queue is configured on the PC main interface with EVCs and the member-link flap or PC shut/no shut.  
Workaround: Remove the CLI “platform control-packet use-priority-q disable” and reapply it on the PC interface.
- 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.
- 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 running the c7200-adventerprisek9-mz.122-33.3.13.SRE image.  
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.
- 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.
- 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.
- 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.
- CSCtq49179

Symptoms: Packets are not matched in the user-defined classes that are classifying traffic based on the DSCP markings on the physical interface.

Conditions: This symptom is observed only if the call is an MLPPP call over L2tp. The issue is not seen with a non-MLPPP call.

Workaround: There is no workaround.
- 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.
- 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.
- 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 Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.
- 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 the 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.

- CSCth87458

Symptoms: Memory leak is detected in `ssh_buffer_get_string`

Conditions: Use test tool Codenomicon to test SSH verification against UUT (SSH-Server test). After the test, the memory leak will be seen in `ssh_buffer_get_string`

Workaround: There is no workaround.

- CSCti98219

Symptoms: The router crashes upon transmission of an mpls-labeled packet.

Conditions: This symptom with Cisco IOS Release 12.4(24)T3 or Cisco IOS Release 15.0(1)M3. Others may be affected. The router acts as MPLS/VPN PE with VRF-NAT. This issue occurs due to SIP packets sent on the MPLS-facing interface.

Workaround: Filter SIP traffic inbound on the IP-facing interface or configure “no ip nat service sip udp port 5060”.

- CSCtk02814

Symptoms: The **show pppoe throttled subinterfaces** command output is truncated, and does not show throttled ATM VC or QinQ subinterfaces during throttling.

Conditions: This symptom occurs when pppoe throttling is configured and active.

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.

- 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.

- CSCtn93891

Symptoms: Multicast traffic is getting blocked.

Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

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.

- 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.

- 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.

- 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.

- 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 l 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.

- CSCtq32896

Symptoms: LSM entries stop forwarding traffic.

Conditions: This symptom is observed after Stateful Switchover (SSO).

Workaround: There is no workaround.

- 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”.

- 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:

```
*Apr 18 15:38:47.704: %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.

- CSCtq94418

Symptoms: Adding, deleting, and readding 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.

- CSCtr06097

Symptoms: The shape average configuration is rejected while alternating from valid “shape average kbps” to valid “shape average percent”. This results in policy modification failure, which could result in wrong throughput.

Conditions: This symptom is observed when a class-map with “shape average” is modified with “shape average percent”.

Workaround: Use the **no shape average** command before issuing the **shape average percent** command.

- CSCtr11268

Symptoms: Traffic duplication is seen during reopt at the receiver node when the tunnel between the mid-point and tail-end is TE FRR-protected.

Conditions: This symptom is observed if active and backup are on different slots. When FRR is active, swap adj on the primary slot should be set to drop. Otherwise, at the time of reopt, packets will be sent out from both active and backup slots.

Workaround: There is no workaround.

Further Problem Description: Even with the fix present, in large-scale scenarios, there is a chance that momentary duplication may occur upon reopt. In case traffic duplication is seen even after this fix is present, increase the primary interface delay timer to 4 seconds or higher to avoid this problem.

## Resolved Caveats—Cisco IOS Release 15.0(1)S3a

Cisco IOS Release 15.0(1)S3a is a rebuild release for Cisco IOS Release 15.0(1)S. The caveats in this section are resolved in Cisco IOS Release 15.0(1)S3a but may be open in previous Cisco IOS releases.

- CSCsl63149

Symptoms: If you repeatedly use the **test mcast ltl** command on a switch processor, a buffer leak is introduced and SP may finally run out of buffers, and the system crashes.

Conditions: This symptom occurs when the **test mcast ltl** command is used repeatedly on a switch port.

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.

Conditions: This symptom occurs on a router running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCsy61302

Symptoms: A chunk header corruption and a router crash with the BADMAGIC error message is seen for either a free or in-use chunk.

Conditions: This 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323>.

- CSCtd59027

Symptoms: The device crashes due to a bus error.

Conditions: This 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.

- CSCtd72318  
Symptoms: Cisco ASR1004 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 the 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 message is 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`.
- CSCte15193  
Symptoms: The **`no spanning-tree vlan [vlan]`** command is not removed on standby alone.  
Conditions: This symptom is observed under the following conditions:
  - The **`no spanning-tree vlan vlan`** command is configured first.
  - The **`default spanning-tree vlan vlan- range`** command is entered next.
  - The `vlan` 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 vlan`** command to remove it.
- CSCte36327  
Symptoms: On a dual-IOSD system, the standby gets rebooted at startup. This might cause delay in 2RU at startup.  
Conditions: This symptom occurs on a dual-IOSD system.  
Workaround: There is no workaround.
- 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.
- CSCtf11309  
Symptoms: The MFR interface flaps continuously on shut and no shut, when a policy-map is attached to it.

Conditions: This symptom is observed with Cisco routers that have c7200-adventerprisek9 images.

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 the single connection option.

- CSCtf72328

Symptoms: BFD IPv4 Static does not fully support AdminDown.

Conditions: This 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 on the interface on which the BFD session is configured.

- CSCtf83711

Symptoms: Memory leak is observed after testing PPPoE sessions. The following is the chunk leak at sg\_rule\_map\_action\_create:

```
461778CC 148 148CDC9C 0 *Dead* SSS PM rule action
```

Conditions: This symptom is observed after testing PPPoE sessions.

Workaround: There is no workaround.

- CSCtf90182

Symptoms: When one subinterface-based PW (EoMPLS) is configured on SIP400, an SSO switchover causes a traffic drop of 80 seconds. The VC on the peer router does not come up quickly. It goes to down state and then after 80 seconds, it comes up. Both LDP GR and OSPF NSF AWARE are configured.

Conditions: This symptom occurs with SSO.

Workaround: Configure a larger hello holdtime using the following command:

```
Router(config)# mpls ldp discovery hello holdtime 30
```

Note that the actual value of hello holdtime that is required may depend on the environment.

- CSCtf91692

Symptoms: When a WS-X6708-10GE module or a WS-X6716-10GE module is inserted into a 6509 or 6513 chassis, it may cause the module in slot N - 8 to reload. For example, inserting the module into slot 9 may reset the module in slot 1, inserting the module into slot 10 may reset the module in slot 2, inserting the module into slot 13 may reset the module in slot 5, and so on.

Conditions: This symptom occurs with the following conditions:

1. The 6708/6716 module is inserted in slots 9 to 13.
2. Module insertion is done slowly.

Workaround: This problem has been fixed.

- 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.

- CSCtg41606

Symptoms: With Reverse Route Injection (RRI) configured with the **reverse-route** command, if the crypto map is applied to a multiaccess interface (e.g.: ethernet), then egress traffic may fail when the router cannot populate an ARP entry for the crypto peer address.

Conditions: This 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**.

- 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 command **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 renegotiation 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.

- CSCtg78106

Symptoms: The router shows SNMP ports as open and/or responds to SNMP requests even though the device has no SNMP configuration.

Conditions: This symptom occurs if there is a specific sequence of configuration events that are configured and unconfigured.

To confirm if the device is affected, the output of **show ip sockets** or **show control-plane host open-ports** would show SNMP ports UDP 161 and UDP 162 as open and listening, even though the output of **show running-config | include snmp** returns no output.

Any SNMP requests that are made to the device would have to match SNMP community names that were previously configured on the device.

Workaround:

1. Firstly, configure any SNMP community string, for example, **snmp-server community workaround**. This allows you to view the existing snmp community names with the **show snmp community** command.
2. Remove each of the snmp community names, with the **no snmp-server community "community name"** command.
3. Then, shut down the snmp agent with the **no snmp-server** command. This will close the ports.

Example of workaround once in the vulnerable state:

```
Router# show run | include snmp
Router# configure terminal
Router(config)# snmp-server community workaround
Router(config)# exit
Router# show snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only active

Community name: private
Community Index: cisco22
Community SecurityName: private
storage-type: nonvolatile active
Community name: workaround
Community Index: cisco23
Community SecurityName: workaround
storage-type: nonvolatile active

Router(config)# no snmp-server community private
Router(config)# no snmp-server community workaround
Router(config)# no snmp-server
Router(config)# exit
Router# show udp
Proto Remote Port Local Port In Out Stat TTY OutputIF 17 --listen-- 10.68.32.17 1975 0
0 1000001 0
Router#
```

- CSCtg85402
 

Symptoms: Multicast packet software switching MFIB platform flags “NP RETRY RECOVERY HW\_ERR HAL” after reloading.

Conditions: This symptom is seen with reloading, SSO, and ISSU.

Workaround: There is no workaround.
- 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 (the 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 bidirectional 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>.
- 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: This symptom is observed when you have a bandwidth statement on a multilink bundle.

Workaround: Avoid bandwidth statements on multilink bundle interfaces.
- CSCth25634
 

Symptoms: The password is prompted for twice for authentication.

Conditions: This symptom occurs when login authentication has the line password as fallback and RADIUS as primary, for example, when you configure the **aaa authentication login** command as follows:

```
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, users providing the wrong password at the password prompt will be granted access if the following is configured:

```
aaa new-model
aaa authentication login MYMETHOD line none
line con 0 login authentication MYMETHOD password <some password>
```

- CSCth37580

Symptoms: Dampening route is present even after removing “bgp dampening”.

Conditions: This 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 the route advertised by RTRA.

In this scenario, when DUT learns the route, it will perform the 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.

- CSCth45731

Symptoms: PPPoE sessions get synced partially to the standby RP and later never get cleaned up. The **show** command for the sessions looks on a standby RP like the following:

```
Sby# show ppp all Interface/ID OPEN+ Nego* Fail- Stage Peer Address Peer Name
-----
0xB400008A LCP+ CHAP+ IPV6CP+ Undefine 0.0.0.0
Peer address is 0 and interface will show the PPP handle instead of the virtual
interface of PPP.
```

Conditions: This symptom is observed when IPCP is getting renegotiated and terminated before the full session sync is done for the upcoming PPPoE session.

Workaround: There is no workaround.

- CSCth45774

Symptoms: The Cisco IOS ASR router crashes when **no ip policy routemap** is configured in the config term mode.

Conditions: This symptom is observed because routemap does not exist.

Workaround: Remove the policy configuration prior to removing routemap.

- 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.

- 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw>.

- 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, and then perform the switchover.

- CSCth99366

Symptoms: Multicast streams are displayed as active, when they are not in active state, while executing the **show ip mroute vrf VRF act** and **show ip mfib vrf VRF act** commands.

Conditions: This symptom is observed with the following conditions:

- One primary path (1st PE - CE) and one backup path (2nd PE - CE) are present for multicast traffic and the CE routers are on the same LAN as the multicast source.
- When a switchover from primary path to backup path and again back to primary path occurs, the traffic also switches from primary to backup and then back to primary path.

Backup shows the streams as active although they are flowing through the primary path

Workaround: 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 on the affected interfaces.

- CSCti25339

Symptoms: A Cisco IOS device may experience a device reload.

Conditions: This symptom 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](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

- CSCti34396

Symptoms: The router distributes an unreachable next hop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

Conditions: This symptom is observed 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 next hop 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: This symptom is observed after an FPD upgrade.

Workaround: Perform a **no shut**, and then shut the interface on the active to sync it properly.

- 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

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>.

- CSCti61949
 

Symptoms: Unexpected reload with “SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header” and “chunk name is BGP (3) update” messages.

Conditions: This 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.
- CSCti67429
 

Symptoms: An 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: This symptom is observed with an 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.
- CSCti81177
 

Symptoms: Features like Videomon do not work on a routed port.

Conditions: This symptom occurs when an interface is configured as a switchport and reconfigured to a routed port.

Workaround: Reload the line card.
- CSCti85446
 

Symptoms: A next hop static route is not added to RIB even though the next hop IP address is reachable.

Conditions: This symptom is observed with the following conditions:

  1. Configure a next hop static route with a permanent keyword.
  2. Make the next hop IP address unreachable (e.g.: by shutting the corresponding interface).
  3. Change the configuration in such a way that the next hop is reachable.
  4. Configure a new static route through the same next hop IP address used in step 1.

Workaround: Delete all the static routes through the affected next hop and add them back.
- CSCti97759
 

Symptoms: IPSG configuration with DHCP snooping entry configuration causes the RP to crash.

Conditions: This symptom is observed when a 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.
- CSCtj08533
 

Symptoms: QoS classification fails on egress PE if the route is learnt via BGP.

Conditions: This symptom is observed when there are redundant paths to the CPE.

Workaround: Use only one path between PE and CPE.

- 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: This 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
```

- CSCtj21696

Symptoms: The virtual access interface remains down/down after an upgrade and reload.

Conditions: This symptom 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: "PVDMMII DSP SIMM with one DSP with half channel capacity" PID:
PVDM2-8 , VID: NA , SN: FOC09123CTB
```

Workaround: Perform a shut/no shut on the serial interface.

- CSCtj24453

Symptoms: The following traceback is observed when you use the **clear ip bgp \*** command:

```
%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: This symptom is rarely observed, when you use the **clear ip bgp \*** command 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.

- CSCtj30462

Symptoms: Subscriber detail shows incorrect user/service profiles.

Conditions: This symptom is observed with the following conditions:

- For session 1, a user profile or service profile called Profile\_1 has been downloaded.
- For session 2, another user profile or service profile called Profile\_2, whose content is very similar to Profile\_1, has been downloaded. The services/features inside the profile have been installed correctly; however, in the show command of session 2, Profile\_1 content is displayed.

This does not impact the functionality.

Workaround: There is no workaround.

- CSCtj37698

Symptoms: Cisco IOS 10000 Series routers that are acting as VPDN multihop reset the TOS value to 0 when **ip tos reflect** command is applied to the VPDN tunnel to LAC. This occurs downstream from LNS to the LAC.

Conditions: This symptom occurs under normal VPDN configuration.

Workaround: There is no workaround.

- CSCtj46297

Symptoms: Ping fails when performing a shut/no shut on the outgoing interface in an FRR setup.

Conditions: This 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.

- 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: This symptom is observed in Cisco IOS Release 15.0(1)M2.

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, you 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.



- 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.
- CSCtj58943
 

Symptoms: Standby RP reloads due to line-by-line sync failure for the **encapsulation dot1q 1381** command:

```
Config Sync: Line-by-Line sync verifying failure on 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: This symptom occurs when issuing a configuration command in subinterface mode.

Workaround: There is no workaround.
- 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.
- CSCtj65553
 

Symptoms: The static route that is installed in the default table is missing.

Conditions: This symptom is observed after Route Processor (RC) to Line Card (LP) to Route Processor transition on a 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 Cisco IOS 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 Cisco IOS Release 12.2(33)SRE2.

Workaround: There is no workaround.
- CSCtj74542
 

Symptoms: The router crashes.

Conditions: This symptom is observed on a Cisco 10000 Series router when you configure more than 33 QinQ subinterfaces, all having the same outer VLAN and at least one of them with a second dot1q configured as “any”. Bring up a PPP session through the subinterface that has the second dot1q configured as “any”. Delete all other subinterfaces. Then, try to clear the PPP session or delete the last subinterface.

Workaround: There is no workaround.

- 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: This symptom is observed when “archive log config” is configured.

Workaround: There is no workaround.
- CSCtj79769
 

Symptoms: LC crashes.

Conditions: This symptom is observed in the unconfiguration part.

Workaround: There is no workaround.
- CSCtj82292
 

Symptoms: The EIGRP summary address with AD 255 should not be sent to the peer.

Conditions: This symptom occurs when the 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.
- 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: This 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.
- CSCtj89941
 

Symptoms: IOSd crashes when using the command **clear crypto session** on an EzVPN client.

Conditions: This symptom is observed in the following 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.
- CSCtj91764
 

Symptoms: A UC560/UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to CPU.

Conditions: This symptom is observed during a complete SNMP MIB walk.

Workaround: The CISCO-CALL-APPLICATION-MIB can be excluded via configuration.
- CSCtj94141
 

Symptoms: While sending SNMP queries in MPLS script, a memory leak is observed at saaMplsOperSnmpGet.

Conditions: This symptom is observed while sending SNMP queries in MPLS script.

- Workaround: There is no workaround.
- CSCtj94555
 

Symptoms: After Cisco IOS ASR 1000 routers are reloaded, they fail to re-register to the KS.

From the debugs, it is observed that the attempt to register is generated too early before the GDOI is ON. This attempt is made before the interface, through which GDOI registration traffic with the KS passes, goes to state UP.

Conditions: This symptom is observed on Cisco IOS ASR routers that run Cisco IOS Release 15.0(1)S1.

Workaround: Use the **clear crypto gdoi** command.
  - CSCtj94835
 

Symptoms: Spurious memory access and tracebacks are seen on router reload.

Conditions: This 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 neighborhood is not formed between the CEs.

Conditions: This symptom is observed when the egress interface is on SIP400 with bridging configured on it.

Workaround: There is no workaround.
  - CSCtj96915
 

Symptoms: The 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 that this is a timing issue. While this is a rare event, the probability of it occurring increases with the load and number of sessions.
  - 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 the “File table overflow” error.

Conditions: This symptom is observed when running the **dir/recursive <>** command periodically using the ANA tool.

Workaround: Do not run the **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 observed 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: This 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.

- 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 symptom is observed in Cisco IOS Release 12.2(33)SRE2.

Workaround: Run Cisco IOS Release 12.2(33)SRD5.

- CSCtk07632

Symptoms: Even with the filter option, traffic on a different VLAN on trunk port is getting spanned.

Conditions: This symptom is observed when the filter vlan specified is not configured on the box.

Workaround: Configure the VLAN on the box, and 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 symptom 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 the client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

Conditions: This symptom is observed in Cisco IOS Releases 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”.

- CSCtk12708

Symptoms: The 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: This 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 symptom 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: This symptom is observed 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.

- CSCtk32104

Symptoms: PPPoE data traffic gets process switched.

Conditions: This symptom occurs on PPPoE data traffic.

Workaround: There is no workaround.

- CSCtk33682

Symptoms: Storm control stops working.

Conditions: This 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.

- CSCtk34026

Symptoms: Adding, deleting, and re-adding an access subinterface may sometimes cause loss of data path.

Conditions: This symptom is observed when the configuration sequence involves an add-delete-add sequence.

Workaround: Create access subinterfaces from scratch.

- 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 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 observed 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. The CoS value is not copied to EXP while adding label in L3VPN/VPLS scenarios.

Conditions: This symptom is observed on a Cisco 7600 router. ES+ LC, QoS policy-map with set CoS is applied on switchport interface in ingress. The 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: This 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 observed 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: This symptom is observed if there are more than eight or ten 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 reinitiate 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 the 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 observed on a Cisco 7600 switch with an SIP-200 line card that is running Cisco IOS 12.2(33)SRD3 and later releases.

This 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 `lsp-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  $4\text{ms} * \text{cir value}$ . The 4ms here represents the minimum interval time for bursts. ES+ LC, however, can support an interval value that is faster (smaller) than 4ms. This has been expected behavior with the exception of ES+ LC.

Conditions: Currently, all platforms restrict the interval time for shape from going below 4ms.

Workaround: There is no workaround.

- CSCtk53657

Symptoms: WCCP blackholes 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 IOS 7600 and the hardware is still programmed, WCCP blackholes the traffic.

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 symptom is observed 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 encapsulation.

Workaround: Reload the SPA.

- CSCtk55382

Symptoms: A SPA-OC192POS-VSR or SPA-OC192POS-XFP may fail the boot diagnostic test.

Conditions: This 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.
- 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.
  - 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.
  - CSCtk62453
 

The Cisco 10000 Series Router is affected by a denial of service (DoS) vulnerability where an attacker could cause a device reload by sending a series of ICMP packets.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are also available.

This advisory is posted at <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-c10k>.
  - 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/default 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 in 3CXL PFC mode.

Workaround: There is no workaround.
  - 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.
  - CSCtk67768
 

Symptoms: RP crash is observed in DHCPD receive process.

Conditions: This symptom occurs on the Cisco IOS DHCP server that is used on Cisco IOS ASR routers and acting as ISG.

Workaround: There is no workaround.

- CSCtk68647

Symptoms: DMVPN stops allowing connections after operating for some time (based on the number of connections). The **show crypto socket** command shows that 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).

- CSCtk74970

Symptoms: TE autoroute announced tunnel is not installed in the routing table.

Conditions: This 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”.

- CSCtk75389

Symptoms: The PFR fallback interface on the Cisco ASR1000 platform fails to remain in inpolicy.

Conditions: This symptom is observed on the Cisco ASR1000 platform and only with the ATM interface.

Workaround: There is no workaround if the ATM interface is used on the Cisco ASR1000 platform.

- CSCtk76190

Symptoms: The RSP/SUP fails to switchover automatically when the “TestSPRPInbandPing” fails for more than ten instances.

Conditions: This symptom is observed when the “TestSPRPInbandPing” fails for more than ten instances.

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.

- CSCtk98030

Symptoms: After replacing an ES20 linecard with an ES+ linecard or vice versa in the same slot, some service groups reject new members to join if the old linecard had ethernet service instances in these groups. Similarly, a named EVC rejects new ethernet service instances if it had association with the old linecard. The named EVC cannot be deleted, complaining that it still has service instances.

Conditions: This symptom is observed if an ES20 linecard has been replaced with an ES+ linecard or vice versa in the same slot. The old linecard 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 linecard to the new groups and EVCs.

- 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>** output of that interface.

This symptom is observed on the following devices:

- Cisco IOS Catalyst 6500 router that is running Cisco IOS Releases 122- 33SXH and 12-33SXI.
- Cisco IOS Catalyst 7600 router that is running Cisco IOS Releases 122- 33SRA7, 122-33SRB, 122-33SRC, 122-33SRD, and 122-33SRE.
- Cisco IOS Catalyst 4500 router that is running Cisco IOS Release 122-40SG.

The output is indicated correctly when it is enabled on Cisco IOS Release 122- 18.SXF17a.

Workaround: There is no workaround.

- 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.

- CSCtl04285

Symptoms: After a BGP flap or provisioning a new session, the BGP route reflector will not advertise new IPv4 MDT routes to PEs.

Conditions: This symptom is observed with BGP session flap or when provisioning a new session.

Workaround: Enter the **clear ip bgp \*** command.

- 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.

- CSCtl06259

Symptoms: On a Cisco IOS 10000 series router running Cisco IOS Release 12.2 (33)SB08e, the **show ip cef vrf <vrf> platform** command might show incomplete output, which may include only the following fields:

```
c10k_label_data = 0xCFEE3D80
tag_elt_addr = 0x0
```

```
ipv6_tag_elt_addr = 0x0
```

Conditions: This symptom occurs on a Cisco IOS 10000 series router running Cisco IOS Release 12.2(33)SB08e.

Workaround: Use the **clear ip route vrf <vrf>** command to display the correct output.

- CSCt107955

Symptoms: The 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.

- CSCt108014

Symptoms: The 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.

- CSCt108601

Symptoms: When the DHCP authorization pool is removed, the console stops responding.

Conditions: This symptom occurs if you use the **no service dhcp** command before the DHCP pool is removed.

Workaround: There is no workaround.

- CSCt110395

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.

- CSCt118652

Symptoms: After replacing an ES20 with an ES+ linecard on the same slot or vice versa, adding ethernet service instance members from the new linecard to an existing service group that was associated with the old linecard may cause a reload of the standby RP in SSO mode. This is due to stale configuration on the standby RP.

Conditions: An ES20 linecard has been replaced by a different type of linecard or vice versa, on the same slot. New members are assigned to a service group that had members from the old linecard. 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.

- CSCt119347

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.

- CSCt121884
 

Symptoms: When enabling auto-summary under the BGP process, a BGP withdraw update is not sent even though the static route goes down.

Conditions: This 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.
- CSCt122071
 

Symptoms: After performing SSO, all BFD sessions on the HA router is removed after doing SSO.

Conditions: This symptom is observed when performing SSO after shutting down a BFD-enabled active ATM interface.

Workaround: Reset the HW module to activate the BFD sessions.
- CSCt122871
 

Symptoms: The 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.
- CSCt142358
 

Symptoms: A Cisco ASR 1000 series router crashes after the **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 workaround.
- CSCt146903
 

Symptoms: The 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.
- CSCt154033
 

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.
- CSCt155828
 

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.

- CSCtl67195

Symptoms: The following three BGP debug commands are not allowed to enable:

- **debug ip bgp vpv4 unicast**

- **debug ip bgp vpv6 unicast**

- **debug ip bgp ipv6 unicast**

Conditions: This 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.

- 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.

- CSCtl82922

Symptoms: Fast memory leak occurs on the 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, the standby SP crashes and the system operation recovers.

The “Holding” number in the 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 observed 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.

- CSCt183053
 

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.
- CSCt183736
 

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.
- CSCt188066
 

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: This 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 multitopology routing. All versions of Cisco IOS that include multitopology routing or that are derived from versions that included multitopology routing, and where this fix is not integrated are impacted.

The fix prevents the issuing of commands beginning with **show ip bgp all attr**.
- CSCt190890
 

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.
- CSCt198270
 

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: This 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 in check syntax mode:

- **config check syntax**
- **route-map hello**
- **match local-preference**
- **no match local-preference**

Conditions: This symptom is observed with the commands given above.

Workaround: There is no workaround.

- CSCtn03930

Symptoms: System error log may show up.

Conditions: This symptom is observed on a Cisco IOS ASR1000 series router when it functions as an IP Security (IPSec) termination and aggregation router, and when Route Processor (RP) Switchover happens with running traffic.

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 symptom is observed 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.

- 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 issues in a couple of instances.

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.

- CSCtn62767

Symptoms: The service policy fails to install on the tunnel interface.

Conditions: This symptom is observed when you configure the 3Lvl policy and apply it to the tunnel interface.

Workaround: There is no workaround.

- CSCtf34720

Symptoms: DR will not send a periodic join for an SSM group with a “static-group” configuration on the RPF interface. This will result in the S,G states expiring in the upstream routers and may result in traffic loss.

Conditions: This symptom is observed when the static-group join is configured on the RPF interfaces and the output interface list of the mroute is NULL.

Workaround: Add a local join by using **ip igmp join-group** for the same group and source so that it adds a local interested receiver and sends a periodic join upstream.

- CSCtg85402

Symptoms: Multicast packet software switching MFIB platform flags “NP RETRY RECOVERY HW\_ERR HAL” after SSO/ISSU.

Conditions: This symptom is observed only with CFC cards and not with DFC, and is specific to the mVPN configuration with egress CFC cards. This symptom occurs under rare conditions with SSO/ISSU.

Workaround: Remove and add the default MDT configuration.

- CSCtg91572
 

Symptoms: A router with an SSM (S,G) entry consisting of a NULL outgoing list sends a periodic PIM Join message to the upstream RPF neighbor, thereby pulling unnecessary multicast traffic.

Conditions: This symptom is observed when the router has a NULL outgoing list for an SSM (S,G) entry either due to PIM protocol action (Assert) or when the router is not the DR on the downstream access interface receiving IGMPv3 reports.

Workaround: There is no workaround.
- CSCth84370
 

Symptoms: The Standby Supervisor gets reloaded when **write memory** is run from one VTY, and then later, **show configuration** is run from another VTY. No particular configuration needs to be done prior to **write memory**.

Conditions: This symptom occurs when the Dual Supervisor is used and the configuration file is quite long.

Workaround: Do not run the **write memory** and **show configuration** commands simultaneously.
- CSCth84714
 

Symptoms: With scaled number of MLP bundles on Sip200 with DLFi enabled, Sip200 crashes.

Conditions: This symptom occurs with the following conditions:

  1. Reload the SPA that has MLP bundles.
  2. Shut/no shut the controller.
  3. Flap the links by any other means.

Workaround: This issue is not seen without high traffic and without LFI enabled.
- CSCti80519
 

Symptoms: The following error message is displayed:

```
%ATM: PVP 15 removal failed
```

Conditions: This symptom is seen when there is no service policy applied to VP.

Workaround: VP can be deleted after adding a dummy service policy.
- CSCtj79769
 

Symptoms: LC crashes.

Conditions: This symptom is observed in the unconfiguration part.

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.
- 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.
- CSCtl05785
 

Symptoms: Connectivity is broken on the Cisco 7600 L3 subinterfaces upon reconfiguration of the assigned VRF. Directly connected devices are no longer reachable, and the 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.
  - CSCtl06259
 

Symptoms: On a Cisco IOS 10000 series router running Cisco IOS Release 12.2 (33)SB08e, the **show ip cef vrf <vrf> platform** command might show incomplete output, which may include only the following fields:

```
c10k_label_data = 0xCFEE3D80
tag_elt_addr = 0x0
ipv6_tag_elt_addr = 0x0
```

Conditions: This symptom occurs on a Cisco IOS 10000 series router running Cisco IOS Release 12.2(33)SB08e.

Workaround: Use the **clear ip route vrf <vrf>** command to display the correct output.
  - CSCtl44112
 

Symptoms: mls adjacencies get corrupted for few labels.

Conditions: This symptom occurs at redundancy switchover.

Workaround: Perform shut/no shut on the associated tunnel.
  - 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.
  - 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.

- CSCt198270
 

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: This symptom is observed in Cisco IOS Release 15.1(2)T2 and later releases.

Workaround: Execute a shut/no shut to fix the issue.
- CSCtn16899
 

Symptoms: PIM neighborship is lost between source node and receiver nodes.

Conditions: This symptom is observed 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.
- 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.
- CSCtn38711
 

Symptoms: A router crashes.

Conditions: This symptom occurs during SSO on a heavily loaded Cisco 7600 router.

Workaround: There is no workaround.
- CSCtn41662
 

Symptoms: The 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.

- 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 **pim mode** command if possible when it is only present on a single interface.

- 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’s 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**.

- CSCtn60353

Symptoms: In subpackage ISSU, some OM objects on the standby RP may be missing.

Conditions: This symptom occurs with ISSU between two releases and a new release that adds a new TDL message type.

Workaround: Force a reload of the standby RP before a final RP switchover.

- 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.

- CSCtn62767

Symptoms: The service policy fails to install on the tunnel interface.

Conditions: This symptom is observed when you configure the 3Lvl policy and apply it to the tunnel interface.

Workaround: There is no workaround.

- 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 the global routing table (no MVPN).

Workaround: Disable IGMP snooping for the VLAN.
- CSCtn73566
 

Symptoms: Not all of the tunnel interfaces are up as PIM neighbors.

Conditions: This symptom is observed during mvpnv extranet testing.

Workaround: There is no workaround.
- 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 the LC.
- 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.

## Resolved Caveats—Cisco IOS Release 15.0(1)S2

Cisco IOS Release 15.0(1)S2 is a rebuild release for Cisco IOS Release 15.0(1)S. The caveats in this section are resolved in Cisco IOS Release 15.0(1)S2 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).

- CSCta69213

Symptoms: A Cisco router configured for NHRP may crash due to a bus error.

Conditions: This symptom is observed on a Cisco router configured for NHRP and DMVPN.

Workaround: There is no workaround.

- 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.

- CSCte95396

Symptoms: A subscriber cannot enable the SSS session due to DPM not finding the binding in the DPM table although the DHCP binding exists as shown by performing the **show ip dhcp server binding** command.

Debug sss policy event/err would show “SG-DPM: DHCP Binding does not exist to query session”.

Conditions:

- Subscriber has dhcp binding when doing “show ip binding ...” note: also check the vrf (if any).
- Subscriber has no entry in the dpm policy.
- Session trigger needs to be l2-connect dhcp

## Workarounds:

- If this is a “low lease time and relay dhcp case”, make sure subscriber does not send a DHCP packet: waiting for the DHCP binding to disappear (i.e., expire), re-enable the user’s dhcp forwarding path.
  - If this is a “dhcp server” case, clear dhcp binding on the ISG.
  - Reload the router
- CSCte98144  
Symptoms: The standby reloads with spurious memory access during resource policy configuration.  
Conditions: The symptom is observed on a Cisco 7600 series router.  
Workaround: There is no workaround.
  - CSCtf05827  
Symptoms: A Cisco 10000 router crashes with chunk error.  
Conditions: This symptom occurs due to memory corruption longevity and stress test.  
Workaround: There is no workaround.
  - CSCtf19902  
Symptoms: For some clients, relaying of DHCP Discover packets is not triggered following session authentication. For a single ISG, this results in the client never receiving an address. For redundant ISGs, where one is affected by this issue and one is not, this results in the affected ISG never clearing the session, even though it sees the request from the client accepting the other ISG’s offer.  
Conditions: This symptom is seen when service-start event under control- policy is configured to unapply all possible services (including the desired service), then apply the new service.  
Workaround: Change the service-start event configuration to only unapply other services, then apply the new service. However, this will require a separate event configuration for each service type.
  - CSCtf32348  
Symptoms: Router crashes.  
Conditions: The symptom is observed when you apply “ip security dedicated topsecret sci nsa” on any of the interfaces.  
Workaround: Remove “ip security dedicated topsecret sci nsa” configuration.
  - 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.
  - 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.
- CSCtf64375
 

Symptoms: Memory corruption and router crash are seen with overlapping mac- addresses.

Conditions: This symptom is seen when bringing up Cisco 10000 router sessions with overlapping mac-addresses at 40CPS each set of 10 sessions having the same mac-address.

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.
  - 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.
  - 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.
  - CSCtg60065
 

Symptoms: DLFioATM back-to-back ping fails for AAL5MUX encapsulation.

Conditions: The symptom is observed when you configure DLFioATM with encapsulation AAL5MUX.

Workaround: There is no workaround.

Further Problem Description: Issue is not seen when you configure for AAL5SNAP.
  - CSCtg73456
 

Symptoms: Bulk sync fails due to applying the **tx-ring- limit** command on the main interface, which is not supported.

Conditions: This symptom occurs when applying the **tx-ring- limit** command on the main interface and doing an SSO.

Workaround: There is no workaround.

- CSCtg73798
 

Symptoms: After one or more linecard 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.
- 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 linecard.

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 linecard on configuration of the port-channel.
- CSCth01394
 

Symptoms: On a Cisco 7606 router that is running Cisco IOS Release 12.2(33) SRD3 with SIP200/SPA-4XCT3/DS0, when you have ppp multilink interface(s) configured with member links from same SPA (software based multilink) and you physically remove SPA, you will see that upon executing the **show ppp multilink** command, the multilink interface still has reference for member links. If you do the **sh run int serialx/y** command, you will get message interface not found.

Conditions: This issue is consistently reproducible.

Workaround: There is no workaround.
- CSCth05476
 

Symptoms: On router bootup, the SIP200 linecard 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.
- CSCth05778
 

Symptoms: Router is showing memory leaks.

Conditions: The symptom is observed when the remote end is sending LCP conf\_req messages to a Cisco 10000 series router a lot frequently (1 per 4 msec) than the normal scenario (1 per 2 seconds).

Workaround: Shut down the PPP link that is flapping.

- 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.

- 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.

- CSCth33500

Symptoms: NAS port is reported as zero on LNS.

Conditions: This symptom occurs when “vpdn aaa attribute nas-port vpdn-nas” is configured.

Workaround: There is no workaround.

- 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.

- CSCth45540

Symptoms: Device crashes in SSH Process.

Conditions: SSH process has to fail to allocate memory for the new connection. This would only occur in extremely low memory conditions.

Workaround: None.

- CSCth46888

Symptoms: When the ARP entry is refreshed due to timeout or use of the **clear arp** command, the router sends ARP request for cached MAC address. However, the request message does not use virtual MAC for Source (Sender) MAC.

Conditions: The symptom is observed when the router is VRRP master and VRRP IP is configured the same as the interface IP.

Workaround: There is no workaround.

- CSCth47907

Symptoms: HQF-related traceback seen while stacking a multilink frame-relay configuration with QoS configurations.

Conditions: It is seen if the QoS configuration is applied first and then the DLCI is created, and the policy is applied through the frame-relay map.

Workaround: The issue is not seen if the DLCI is created first and then policy-map is applied; or if the policy-map is directly applied instead of frame-relay map.

- CSCth55689

Symptoms: If you do a **clear xconnect** before the primary VC has come up, the system erroneously brings up PW on the backup VC.

Conditions: The symptom is observed if you do a **clear xconnect** before PW establishment.

Workaround: Use the following command:

**clear xconnect peer** *peer-ip* **vcid** *vcid-id*.

- CSCth57687

Symptoms: A router crashes with the *c7200-adventerprisek9-mz\_final\_hotice\_pi15* image.

Conditions: The symptom is observed with the parser syntax check.

Workaround: There is no workaround.

- CSCth59593

Symptoms: Spurious memory access is seen.

Conditions: The symptom is observed when issuing the command **show pxf cpu isg ip-session mtrie no**.

Workaround: There is no workaround.

- CSCth67811

Symptoms: Acct-Terminate-Cause is set as “nas-error” in Tunnel stop record when admin clear.

Conditions: This symptom is seen with admin clear tunnel using the **clear vpdn tunnel l2tp all** command.

Workaround: There is no workaround.

- CSCth71095

Symptoms: DHCP binding table is not completely synced to standby RP.

Conditions: This symptom occurs when box is acting as DHCP Relay and ISG is configured.

Workaround: Use unnumbered multiservice interface instead of numbered one.

- 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.

- CSCth72290

Symptoms: Traffic over PPPoMPLS drops continuously on a SIP400 with microcode reload.

Conditions: The symptom is observed when PPPoMPLS is configured over any interface on a channelized SPA on SIP400 and following a microcode reload of the linecard.

Workaround: Reload the SPA.

**Further Problem Description:** When PPPoMPLS is configured on a channelized interface the encapsulation for that interface on the linecard is PPP where as the SPA encapsulation is HDLC as the SPA just tunnels the packets through. After the microcode reload, the linecard queries the SPA for a connection ID for the channelized interface with encapsulation as PPP but as the SPA encapsulation set is HDLC the SPA does not give any connection ID to the SIP400 and hence the traffic starts to drop after a reload.

- CSCth82486

**Symptoms:** A SIP600 crashes.

**Conditions:** The symptom is observed following an OIR of the active supervisor.

**Workaround:** There is no workaround.

- 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”.

- 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.

- 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.

- CSCti04754

**Symptoms:** PPPoE sessions are stuck at attempting state forever.

**Conditions:** This symptom is seen when sessions are triggered during SSO time, which get stuck at attempting state.

**Workaround:** Clear attempting state sessions by the **clear** command from box.

- 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.
- CSCti08115  
Symptoms: The removal of a port-channel interface associated with **mpls ldp advertise-labels interface Port-channelN** can cause a “config sync” error upon an SSO.  
Conditions: The symptom is observed after doing an SSO following the removal of the port-channel interface.  
Workaround: Before the SSO, remove the offending advertise-labels command when removing the port-channel command with:  
**no interface Port-channelN**  
**no mpls ldp advertise-labels interface Port-channelN**
- 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.
- CSCti24657  
Symptoms: New settings for fabric channel preemphasis are for sip600/esm20 card for Cisco 7609, Cisco 7609S, and Cisco 7613 chassis.  
Conditions: There are no conditions.  
Workaround: There is no workaround.

- 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.
- CSCti30665
 

Symptoms: On issuing the **issu runversion** command the standby reloads with the following message:

```
%ISSU-3-DEBUG_ERROR:
  There is no session control block with session_id = 0
-Traceback= 426E3B14z 417C7154z 417C56B4z 417C58A8z 43D79674z 417C8F00z
417CA120z
-Traceback= 426E3B1Cz 417C7154z 417C56B4z 417C58A8z 43D79674z 417C8F00z
417CA120z
-Traceback= 426E3B1Cz 417C71A8z 417C56B4z 417C58A8z 43D79674z 417C8F00z
417CA120z
%RED_MODE-3-RED_MODE_START_NEGO_FAILED: Red Mode ISSU start nego session
failed (ISSU_RC_INVALID_MSG_SES_CTX)
```

Conditions: The symptom is observed when issuing the **issu runversion** command.

Workaround: There is no workaround.
- 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.
- 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+ linecards, some of the ACEs do not work, while others work as normal.

Conditions: The symptom is observed when the linecard or router is reloaded with the ACL configuration present.

Workaround: Remove and add ACL on the EVC.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>.

- 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.
- 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”.
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 12.2(33)SB based releases if the 12.2(33)SB router is the one not reloading.

- 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.

- 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.

- 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 seen 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).

- 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.

- 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.

- 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 linecard, 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.

- CSCti77521

Symptoms: Policy-map is not attached to a DLFloATM 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.

- 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 linecard.

Workaround: There is no workaround.

- 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.

- CSCti88062

Symptoms: Traffic stops flowing through ports configured with REP over EVC BD when an ES20 linecard 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.

- 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**.
- 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.
- 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.
- 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.
- 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.
- 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 seen on P router when MLDP neighbors go down.

Workaround: There is no workaround.

- 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 linecard.

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.
- 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.
- 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.
- 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.
- 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.
  - CSCtj44237
 

Symptom: High CPU observed in RP.

Conditions: The symptom is observed with MVPN configurations.

Workaround: There is no workaround.
  - 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.
  - 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.
  - 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.
  - 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 not add or configure class names which are sub-strings of other classes on the router.

- CSCtj63285  
Symptoms: Build breakage.  
Conditions: There are no conditions.  
Workaround: There is no workaround.
- CSCtj74611  
Symptoms: Active supervisor in the Cisco 7600 series router reloads.  
Conditions: The symptom is observed after a linecard 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.
- CSCtj79992  
Symptoms: Receiver end flooded in an MVPN scenario.  
Conditions: The symptom is observed even after stopping traffic.  
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.
- 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.
- 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.

## Resolved Caveats—Cisco IOS Release 15.0(1)S1

Cisco IOS Release 15.0(1)S1 is a rebuild release for Cisco IOS Release 15.0(1)S. The caveats in this section are resolved in Cisco IOS Release 15.0(1)S1 but may be open in previous Cisco IOS releases.

- CSCsm26063

Symptoms: Router crashes following a **shut/no shut** on the main interface.

Conditions: This symptom is observed 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.

- CSCso20810

Symptoms: A buffer leak may occur when a router is configured with the combination of NAT, multicast and encryption. The leak occurs when multicast subsequently flows out a crypto-enabled interface.

Conditions: This symptom will effect only those users whose routers are part of a multicast group. They must also have NAT and crypto configured on one or more of the interfaces in the multicast group.

Workaround: Multicast traffic can be forwarded via a GRE tunnel instead of in the clear.

- CSCsv70157

Symptoms: On a Cisco 7609 router that is running Cisco IOS Release 12.2(33)SRD, after configuring any interface with any carrier-delay value other than 0 (the default), upon entering **wr mem** you get an unexpected warning message:

```
"Warning: Overriding existing carrier delay value to 0"
```

Conditions: There appears to be no special conditions to reproduce this defect. Simply configure any interface with a carrier delay and execute **wr mem**:

```
Router#conf t Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f2/12
Router(config-if)#carr
Router(config-if)#carrier-delay 2
Router(config-if)#end Router#wr Building configuration... Warning: Overriding existing
carrier delay value to 0
%SYS-5-CONFIG_I: Configured from console by console[OK]
Router#
```

Workaround: There is no workaround.

Further Problem Description: This warning should come when Asymmetric Carrier Delay (ACD) is configured on an interface and you then attempt to configure Standard Carrier Delay via the **carrier-delay delay** interface command. However, the message is coming when ACD is not configured.

- CSCtb58282

Symptoms: A device running Cisco IOS may reload when the **show tcp brief** command is issued.

Conditions: This symptom is observed under the following conditions:

1. "Ip domain lookup" is configured (it is on by default).
2. The ip address of the foreign host in the tcp session has a very long domain name associated with it (on the order of 70 characters) .
3. The port number of the foreign host is 5 digits long.

If **ip domain lookup** is disabled, the problem could still happen if the host has a static entry configured via the **ip host** command.

Workaround: Configure “no ip domain lookup.” Or, avoid using the **show tcp brief** command on the device.

- CSCtd47834

Symptoms: After a large number of RP switchovers, Standby RP does not come up for around 35 minutes and is then rebooted due to “Standby EHSA fsm watchdog timer expired, standby reloading . . . .”

Conditions: This symptom is observed after the following sequence of events:

1. NTT 3Play Setup with traffic. (8K DHCPv4, 8kDHCPv6, 16k PPPoE, 18000 SBC Pinholes & 800 BHCA)
2. Bring up all the blocks (PPPoX, DHCPv4 etc.)
3. Try to bring up additional 1k sessions, but the sessions are blocked due to the limit and are unable to come up
4. Start Traffic on all the sessions
5. Do an RP switchover repeatedly.

Workaround: No workaround other than restarting the standby from the active.

- CSCtf05408

Symptoms: IP address on a loopback interface is lost.

Conditions: The conditions are currently under investigation.

Workaround: Reconfigure the loopback interface.

- CSCtf90970

Symptoms: TX CPU might crash on a Cisco 7600 SIP-200 due to a particle chain corruption.

Conditions: This symptom is observed when “ppp multilink interleave” is configured on a multilink PPP bundle.

Workaround: Disable the “ppp multilink interleave” feature on the multilink PPP bundle.

- CSCtf92354

Symptoms: Traceback seen when doing a shut/no shut under heavy traffic (100Mbps).

Conditions: The following steps cause this issue:

1. 256 dLFioATM interfaces on a single PA.
2. Traffic is flowing through all the bundles which is above NDR (100 Mbps) but less than interface bandwidth (155Mbps). This 100 Mbps traffic includes 20 Mbps of 64 byte + 40 Mbps of TCP + 40 Mbps of UDP.
3. Do a shut/no shut
4. Tracebacks will be seen.

Workaround: There is no workaround.

- CSCtg11344

Symptoms: A few PPPoA sessions fail to sync up with the standby.

Conditions: The symptom is observed after an SSO switchover in a scaled scenario.

Workaround: There is no workaround.



- CSCtg35298  
Symptoms: Traffic drops are seen between two PEs after re-optimization.  
Conditions: The symptom is observed with 16k VPLS VC, 4k scalable EoMPLS, 1K software EoMPLS, 600 primary tunnels to nPE1 and one tunnel to nPE2 from nPE3.  
Workaround: There is no workaround.
- 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.
- 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.
- 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.
- CSCtg60201  
Symptoms: Unconfiguring the **maximum-path** command does not trigger a backup path calculation.  
Conditions: This symptom is observed if “addition-path install” is configured along with the **maximum-path** command.  
Workaround: Reconfigure “bgp additional-path install.”
- CSCtg65989  
Symptoms: Only the first user is able to get authenticated successfully and browse the internet. All subsequent users are constantly redirected to the web portal after successful authentication. The **show sss sess uid xxx** command shows that the internet service is not applied to the account even though the session is authenticated.  
Conditions: The symptom is observed with customers using web logon with a session applying an auto service.  
Workaround: Remove “autoservice” and apply static service at account logon.
- CSCtg74946  
Symptoms: QoS counters are stuck at “0.”  
Conditions: This symptom is observed with SSO and when DLF1 is configured over ATM.

Workaround: Detach and re-attach the service policy.

- CSCtg84969

Symptoms: The output of **show ip mfib vrf vrf name verbose** may show the following line “Platform Flags: NP RETRY RECOVERY HW\_ERR” and multicast traffic may not be hardware switched.

Conditions: The symptom is observed on a dual RP Cisco 7600 series router with line cards after multiple reloads or SSO switchovers. When the issue occurs the output of the **show ip mfib vrf vrf name verbose** command on the standby SP will show some lines preceded with “###” where an interface name is expected.

Workaround: There is no workaround.

- CSCtg88216

Symptoms: Packets are being flooded on the wrong line cards associated to some BRIDGE DOMAINS that have interested receivers on other line cards.

Conditions: This symptom is observed with egress ports on multiple DFCs.

Workaround: There is no workaround.

- CSCtg89555

Symptoms: No forwarding interface is seen in the mfib output on a DFC.

Conditions: This symptom is observed when configuring an ip address after multicast has been configured on a dot1Q interface.

Workaround: Performing a **shut/no shut** of the interface will fix the problem.

- CSCtg94250

Symptoms: Removing **address-family ipv4 vrf vrf** (in router BGP) followed by **no ip vrf vrf** (where “vrf” is the same) could result in a crash.

Conditions: The symptom is observed in a large VPNv4 scale setup, when applying the following commands to the same VRF back-to-back:

1. **no address-family ipv4 vrf vrf**
2. **no ip vrf vrf**
3. **ip vrf vrf**

The trigger of the BGP crash is a result of a racing condition between event 1 and event 2.

Workaround: Since this is a racing condition, the workarounds are:

1. Not applying (1) before (2).
2. Give sufficient time for (1) to complete before applying (2).

- CSCtg98501

Symptoms: Memory leak is seen with an EAP component every time the EAP system times out and retransmits the message back to the policy component.

Conditions: This symptom can occur with any Dot1x subscribers.

Workaround: There is no workaround.

- CSCth07787

Symptoms: A standby device crashes when attempting to configure login banner on the active device.

Conditions: The symptom is observed only when configuring the banner manually, but not during bulk sync or any copy operations. In addition, this symptom is observed when using the following delimiters:

- Cntrl-v + Cntrl-C
- Shift-6 + Shift-C

Workaround: Use any delimiters other than the following:

- Cntrl-v + Cntrl-C
- Shift-6 + Shift-C

- CSCth11062

Symptoms: When two or more sessions share a common layer4 service, if one session is cleared, the service may not work correctly for the other existing session.

Conditions: This symptom occurs when the layer4 service is configured by an access list, and two or more layer4 redirected traffic streams, corresponding to the different sessions, originate from the same client. For example, the sessions exist on ISG for a single client.

Workaround: Use different services or access lists.

- CSCth11747

Symptoms: When a switchover occurs with GR enabled, sometimes the NSF states are not preserved and the forwarding entries are lost, leading to packet loss for a few seconds.

Conditions: This symptom is observed only with single sessions with GR configured when the restarting neighbor does a passive open. Chances of hitting this are low since this issue occurs because we receive a new open message before the old tcp session has a chance to reset.

Workaround: Configuring multi-session capability on the neighbor sessions or restricting the restarting neighbors connection to active mode would prevent this issue.

Further Problem Description: When an established session already exists between the GR-enabled routers, and the tcp has not yet notified of reset due to neighbor SSO, if the receiving router gets a new open from the restarting router, as per the RFC it is supposed to tear down the old session and accept the new connection. The old session was being torn down properly but it would take the service reset walker to completely free the session. In case of multi-sessions there was no problem in accepting the new session since multiple sessions are allowed. But in case of a single session that already exists, the new sessions are not allowed until the old session is completely freed. Hence, the new session was getting rejected and notification was sent to the restarting neighbor. The restarting neighbor, upon reception of this notification, would clear the NSF preserve bits and further opens would clear the NSF states on the receiving neighbor and hence the problem. The solution would be to accept the new connections in single session support neighbors when the GR reopen has marked the session for reset and de-linked the topologies. The topologies would be added to the new session and the connection accepted. The old session would be freed when service reset walker is invoked. So, for a transient period of time between the session mark reset and the session free, there would be multiple sessions established on the neighbor even though the neighbor was configured as single session. Dependent DDTs CSCtd99802 and CSCth90239 need to be committed along with this fix to ensure complete working of this functionality.

- CSCth13153

Symptoms: An incorrect UDLR Reporter exists on a router that is connected to a UDLR link and PIM-SM domain with auto-rp configurable.

Conditions: This symptom is observed on a Cisco 7200 series router with Cisco IOS Release 15.1(1.16)T0.1.

Workaround: There is no workaround.

- CSCth13454

Symptoms: PIM neighborhood is not established with the remote PE and RP for the MVRFs.

Conditions: This symptom is observed with traffic, after removal and restoration of MVRFs. Traffic is not flowing properly since pim neighborhood is not established with the remote PE and RP for those MVRFs.

Workaround: There is no workaround.

- 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.

- CSCth33457

Symptoms: A Cisco IOS router configured with IPSec may reload when receiving encrypted packets.

Conditions: This symptom is observed when one or more of the following is configured on an interface configured with IPSec:

- ip accounting precedence input
- ip accounting mac-address input
- WCCP
- Flexible NetFlow
- BGP accounting
- uRPF
- mpls accounting experimental input

Workaround: Avoid using IPSec or avoid using all of the above features on the interface.

- CSCth33949

Symptoms: An LNS standby crashes when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the **clear ppp all** command.

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.

- CSCth35873

Symptoms: The Subject Alternative Name (SAN) is incorrect in persistent self- signed certificates.

Conditions: This symptom occurs in persistent self-signed certificates. The SAN is displayed as DNS:secp6-11.cisco.com, but it is supposed to be DNS:zzztmp.cisco.com.

Workaround: There is no workaround.

- CSCth37793

Symptoms: High CPU utilization caused by process switching of multicast traffic after IPv6 Address Family (AF) is configured for VRF.

Conditions: The symptom is observed on a Cisco 7600 series router that is acting as a PE router in mVPN. It is seen with multicast traffic forwarded inside a VRF for which IPv6 AF is configured. The issue can be seen when you:

1. Bootup with VRF configured only with IPv4; configure IPv6 AF after bootup
2. Bootup with VRF configured with both IPv4 and IPv6 AF; unconfigure IPv6 AF after bootup.

Workaround: Unconfigure IPv6 AF from VRF.

Alternate Workaround: Clear mroute for VRF.

Alternate Workaround 2: Reload the device.

Further Problem Description: The problem can be identified on a device by following these steps:

1. High CPU seen using **show proc cpu**
2. **sh redundancy** used to identify slot with active supervisor as *X*
3. Attach *X*
4. **sh platform software vpn mapping | i VRF-NAME\_HERE:**

```
IOS | <VRF-NAME-HERE> | 4 || <NUMBER1> | 0x0004 | 0x0000 | R[2]:4
```

5. **show platform software multicast ip cmfib vrf REN SOURCE GROUP verbose:**

```
Multicast CEF Entries for VPN#4 (<SOURCE>, <GROUP>) IOSVPN:<NUMBER2> (1) PI:1 (1)
CR:0 (1) Recirc:0 (1)
```

6. If *NUMBER1* and *NUMBER2* do not match, the defect is hit.

(Note: Values in “<>” are variables fitting your configuration.)

- CSCth38699

Symptoms: Cisco IOS platforms configured for Auto-RP in a multicast environment lose the RP-to-group mappings.

Conditions: This symptom is observed in Cisco IOS Release 12.2(18)SXF7, Release 12.2(33)SXH4, and Release 12.2(33)SRC4, but it is believed to affect other releases. This symptom occurs when the length of the RP-Discovery packet reaches its limit. If the Mapping Agent receives RP-Announce packets, increasing the number of multicast groups, and that number makes the limit of the packet size, then an empty RP-Discovery packet is triggered that clears the RP-to-group mapping tables in all the routers receiving such a packet.

Workaround: Configure static RP-to-group mappings.

- 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 than 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.

- CSCth42594

Symptoms: Remote standby router crashes when you configure and remove “ppp multilink mrru local” under a multilink interface.

Conditions: The symptom is observed under the following conditions:

1. When multilink is bundled with more than one serial interface (not seeing this issue with only one serial interface)
2. Seeing this issue from 1500 and above (not seeing this issue when configuring and removing "ppp multilink mrru local 1499").

Workaround: There is no workaround.

- CSCth47888

Symptoms: In a Hot-Standby psuedowire redundancy setup, traffic is forwarded on the Standby psuedowire instead of the Active psuedowire, which is in up/up state.

Conditions: This symptom is seen in a Cisco 7600 router that is running Cisco IOS Release 15.0(1)S with hot psuedowire redundancy configuration.

Workaround: There is no workaround.

- CSCth50096

Symptoms: Crash occurs under certain EAP to DHCP communications.

Conditions: The symptom is observed when the memory leak fix for CSCtg98501 is present.

Workaround: There is no workaround.

- CSCth50479

Symptoms: With a high rate of session churn, the **show subscriber sessions** command shows sessions are stuck in the "Attempting" state. The **show subscriber stat detail** command shows that these sessions are actually stuck in the "installing-config" state.

Conditions: The symptom is observed with a high rate of PPP session churn and with a large number of sessions (resulting in more than 70% IOS memory used).

Workaround: Router reload is required to clear stuck sessions.

- CSCth55383

Symptoms: When entering the **show tech** command on RP, the line card with DFC may display the SWITCH\_BUS\_IDLE message.

Conditions: This symptom occurs when entering the **show tech** command on RP.

Workaround: There is no workaround.

- CSCth62425

Symptoms: When trying to add a static and extendable NAT rule for port 80 or 443 (PAT), the operation fails with this error message:

```
%Port 80 is being used by system min80 or %Port 443 is being used by system min443
```

Conditions: This symptom is observed under the following conditions:

- Cisco IOS Release 12.2(33)XND to Release 12.2(33)XNF
- add NAT rule for either port 80 or 443
- delete NAT rule
- add the same NAT rule with a different Inside Local address
- delete NAT rule
- try to add the original NAT rule (at this point no other static NAT rule can be added with the same Inside Global and port 80/443).

## Workaround:

1. Make sure that the HTTP port and secure-port are assigned to other than 80 and 443, respectively, and enable them; for example:

```
ip http port 10500 ip http secure-port 11000 ip http server ip http secure-server
```

2. Now, configure the port static mappings for the above ports for 80 and 443; for example:

```
ip nat inside source static tcp 10.50.50.50 80 10.1.1.4 80 extendable ip nat
inside source static tcp 10.50.50.50 443 10.1.1.4 443 extendable
```

3. Change these HTTP ports back to 80 and 443.

```
ip http port 80 ip http secure-port 443
```

4. Afterwards, the above port static mappings can be deleted and re-added normally.

- CSCth62854

Symptoms: A Cisco router crashes with traceback `ospfv3_intfc_ipsec_cmd`.

Conditions: This symptom is observed when the interface is configured with `ospfv3`, null authentication/encryption, and non-null encryption/authentication.

Workaround: Remove the `ospfv3 area` command, then remove the null authentication/encryption.

- CSCth64439

Symptoms: With different image versions and with “`issu image-version comp disable`” configured, the standby comes up in SSO mode instead of RPR.

Conditions: The symptom is observed when “`issu image-version comp disable`” is configured.

Workaround: Enable image-version compatibility check using **`issu image-version comp enable`**.

- CSCth64507

Symptoms: Bulk Sync failure is seen on redundancy force-switchover command when eem policy is configured and only when the policy file is present in the active module.

Conditions: This issue is observed only when the policy file is present in the active and not in the standby module.

Workaround: Have the policy file present in both the active and the standby.

- CSCth65072

Symptom: A memory leak occurs in the big buffer pool while using the service reflect feature.

Conditions: This symptom is observed when the service reflection feature is enabled. A packet is generated from service reflection and is blocked by an ACL on the outgoing interface. This will cause the buffer leak.

Workaround: Remove the ACL on the outgoing interface or permit the packets generated from service reflect on the ACL.

- CSCth66347

Symptoms: Traffic is impacted with replication mode as ingress and bidirectional at the core in an MVPN network.

Conditions: This issue is observed in `mcp_dev` and `xe31` releases.

Workaround: Use sparse mode in the core.

Further Problem Description: The issue is mainly because of HW not getting programmed properly in the PE.

- CSCth67608

Symptoms: Some groups are missing in the MLD Proxy cache on the Proxy router.

Conditions: This symptom is observed when “ipv6 mld host-proxy” is applied with existing multicast routes.

Workaround: Clear the multicast routes using “clear ipv6 pim topology” after applying “ipv6 mld host-proxy.”

- CSCth69469

Symptoms: ICMP filtering is not working in an SACL configuration.

Conditions: This symptom is observed when ACE is configured with icmp options.

Workaround: There is no workaround.

- CSCth69504

Symptoms: A Cisco 7600 series router may experience a small buffer leak in the small buffer pool on SP.

Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD configured with IGMP snooping.

Workaround: Disable IGMP snooping either globally or per VLAN.

- CSCth69525

Symptoms: Multicast traffic is not forwarded towards the CE router on the ATM interfaces.

Conditions: The symptom is observed with AAL5MUX, which shows that there is an active stream towards the CE, but the CE is not receiving this stream. With AAL5SNAP encapsulation, we cannot see any active stream.

Workaround: There is no workaround.

- CSCth69588

Symptoms: Disposition traffic does not flow across ES+ cards. Imposition traffic for sceompls works fine.

Conditions: This symptom is observed with ES+ card mainly on switchover, reprovisioning of circuits, etc.

Workaround: Enter the **clear xconnect all** command on the device and wait for reprovision. Once all circuits are up, traffic will flow across fine.

- CSCth69827

Symptoms: Crash seen while issuing “no origin file bootdisk:dhcp\_bind.txt.”

Conditions: This symptom is observed when using DHCP.

Workaround: There is no workaround

- CSCth69883

Symptom: EVCs under the same service group belonging to a port-channel are not getting mapped to the same member link. The PC has weighted load- balancing configured.

Conditions: This symptom is observed upon completion of the following steps:

1. Create a PC with multiple EVCs
2. Assign the EVC under different SGs
3. Configure weighted load balancing for the PC
4. Add 2 member-links to the PC
5. Do a **no-shut** on the PC.



- Workaround: There is no workaround.
- CSCth72565
 

Symptoms: The reachability of the PE2 router's loopback is lost from PE1 after an interface flap in the core. The LSP toward PE2 "breaks" due to a data plane programming error (wrong labels).

Conditions: The symptom is observed with MPLS with the presence of ECMP. The PE1 has two uplinks to core routers. In a steady state there is no ECMP between PE1 and PE2. When a link is lost in the P-core (link flap or shut/no shut) there is ECMP between PE1 and PE2. After the link flap between the two P routers in the core, PE1 is losing connectivity to PE2.

Workaround: Use the **clear ip route** on the affected IP address.

Alternate Workaround: Avoid ECMP by altering link cost.
  - CSCth72765
 

Symptoms: Configuring "mls qos protocol hsrp police <rate>" does not enable policing of HSRPv2 packets.

Conditions: The symptom is observed on a Cisco 7600 series router when "mls qos protocol hsrp police *rate*" is configured.

Workaround: There is no workaround.
  - CSCth74869
 

Symptoms: Paralled Express forwarding (PXF) fails when one of the load balancing links goes down. This issue is seen on the interface used by Cisco Express Forwarding (CEF).

Conditions: This issue is seen on the interface used by Cisco Express Forwarding (CEF).

Workaround: Clear the vrf routing table for the particular VRF that is affected so that the router selects another interface to use for traffic.
  - CSCth75354
 

Symptoms: There is an intermittent problem when a SPAN source is set to be a VLAN. The destination in the SPAN session does not receive the data.

Conditions: The symptom is observed on a Cisco 7600 series router with an ES+20 card that is running Cisco IOS Release 12.2(33)SRE0.

Workaround: Reload the module.
  - CSCth77503
 

Symptoms: The link-state advertisement (LSA) is not generated or updated on a Cisco router.

Conditions: This symptom is observed with a network configuration that covers a large number of interfaces.

Workaround: Increase the buffer size or configure redistribution to advertise the links.
  - CSCth78148
 

Symptom: Cannot attach to 8XCHT1/E1 SPA console.

Conditions: This issue is observed after configuring SSO.

Workaround: Reload the SPA.
  - CSCth78630
 

Symptoms: Call manager or other SAF clients are not able to learn SAF patterns.

On the forwarder, “show eigrp service-family external-client” displays multiple expired client registrations. The keepalive timer on the stale registrations is “0” and the “Client API Handle” is “0”; however, the File Descriptor is still listed in the table. See the following example:

```
abi-4506#sh eigrp service-family external-client SAF External Clients Client Label
Client API Handle File Descriptor ABI_SAF_CLIENT1 0 1 ABI_SAF_CLIENT1 0 2
ABI_SAF_CLIENT1 0 3 ABI_SAF_CLIENT1 0 4 ABI_SAF_CLIENT1 0 5 ABI_SAF_CLIENT1 0 6
ABI_SAF_CLIENT1 0 7 ABI_SAF_CLIENT1 0 8 ABI_SAF_CLIENT1 0 9 ABI_SAF_CLIENT1 0 10
ABI_SAF_CLIENT1 0 11 ABI_SAF_CLIENT1 0 12 ABI_SAF_CLIENT1 0 13 ABI_SAF_CLIENT1 0 14
ABI_SAF_CLIENT1 15 15 ABI_SAF_CLIENT1 16 16 abi-4506#
```

Using the **debug voice saf** command or the **debug eigrp service-family [external-client {client|messages|protocol}]** command shows the following traceback:

```
%SCHED-3-STUCKMTMR: Sleep with expired managed timer 229C03BC, time 0xF2968 (4d20h
ago). -Process= "SAF-EC FORWARDER", ipl= 4, pid= 235 -Traceback= 11A14818 11A14E3C
11130E54 109A0594 10997584
```

Conditions: This symptom occurs when an SAF client unregisters/re-registers to a SAF forwarder.

Workaround: Reload the router acting as forwarder and ensure there is no unregister/re-register activity on the client (for example, do not restart publishing/subscribing services, etc.).

- CSCth79336

Symptoms: Ingress QoS policy, when applied on an EVC configured on port-channel, is getting configured for only one of the NPs, instead of all of the NPs that have member-links belonging to the port-channel. If traffic enters the port-channel via multiple member-links, provided the member-links belong to different NPs, ingress QoS will be applied on only one of the member-links.

Conditions: This symptom is observed when EVC is configured on port-channel.

Workaround: There is no workaround.

- CSCth80166

Symptoms: EVCs belonging to the same group are mapped to different member links, and the packets are forwarded over different member links.

Conditions: This symptom is observed when dynamic changes such as adding an EVC to a group or removing it are made; all the group members are not mapped to the same member link.

Workaround: Perform a **shut/no shut** on the device.

- CSCth80343

Symptoms: Interface of “SPA-1XCHOC12/DS0” is removed after doing OIR for the SPA.

Conditions: This symptom is observed when we have “SPA-1XOC12-ATM-V2” and “SPA-1XCHOC12/DS0” together on the same CC in 13RU (Grande).

Workaround: There is no workaround.

- CSCth81950

Symptoms: A memory leak occurs in ES+ cards.

Conditions: This symptom is observed on a Cisco 7600 with the cac enabled.

Workaround: There is no workaround.

- 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.

- CSCth85294
 

Symptoms: A PIM neighborship is not established with the remote PE and RP for the MVRFs.

Conditions: This symptom is observed with traffic, after removal and restoration of MVRFs. Traffic does not flow properly since the PIM neighborship is not established with the remote PE and RP for those MVRFs.

Workaround: There is no workaround.
- CSCth86402
 

Symptoms: When flapping a WAN interface, the PIM tunnel disappears.

Conditions: This symptom is observed when flapping a WAN interface after a few hours of working.

Workaround: Disable multicast routing, then enable it again.
- CSCth86517
 

Symptoms: A crash occurs while stacking data mdt and default mdt mvpn extranet tests.

Conditions: This symptom is observed when stacking mvpn extranet data mdt and default mdt test cases.

Workaround: There is no workaround.
- CSCth87132
 

Symptoms: Diagnostic tests may fail on an ES+ linecard with the following message:

```
Mandatory.go_fabrich0.tcl: GOLD EEM TCL policy for TestFabricCh0Health
```

Conditions: This symptom is observed when 802.1 TAP MIB is used to tap based on an if\_index belonging to an “access” interface.

Workaround: IP-TAP MIB may be used instead of 802.1 TAP MIB.
- 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.
- CSCth87357
 

Symptoms: A Cisco 10000 router fails to forward priority queueing traffic (dscp = ef) when interleaving is enabled on the CE connected to the router.

Conditions: This symptom is observed only when “ppp multilink interleave” is enabled on the CE connected to the router.

Workaround: There is no workaround, other than removing the command on the CE.

Further Problem Description: No PQ traffic passes from the local CE to the remote CE, but the same PQ traffic between the local PE and the local CE is forwarded. This symptom applies only to PQ traffic and does not affect normal pings.
- CSCth90001
 

Symptoms: Packets egressing interfaces of ES+ line cards are not received on the other side of the L2 link when SVI plus switchport configuration is used. It is random and does not occur on every ES+ line card.

Conditions: This symptom is observed when the ES+ line card is the egress line card and SVI plus L2 switchport configuration is used. When this issue is seen, the CFI bit in vlan tag header for such packets is set by X40g egress-intf causing the peer router to drop such packets.

Workaround: Use L3 802.1q subinterface configuration.

- CSCth90497

Symptoms: When a Cisco IOS In-Service Software Upgrade (ISSU) from Cisco IOS Release XE3.1.0 to Release XE3.2.0 with NAT configured is performed, a traceback of the following form is seen from the FPs during the runversion stage:

```
*Jul 14 17:14:02.653: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: SERVICE:
appl type unknown, proto unknown, acl NONE, port 0, is_reg_port 0, default_on 1
download to CPP failed
```

There is no functional impact. The message occurs just before the FPs are reloaded with the Cisco IOS Release XE3.2.0 image as part of the normal ISSU process. Upon booting with the Cisco IOS Release XE3.2.0 image, the FPs handle all objects from the RP as expected.

Conditions: This symptom is observed when NAT has been configured on the box and the Cisco ISSU is being done to upgrade Cisco IOS Release XE3.1.0 to Cisco IOS Release XE3.2.0 or higher.

Workaround: There is no workaround.

- CSCth91093

Symptoms: Exact symptom due to memory corruption is unknown at this time.

Conditions: This symptom is observed after an L2TP HA switchover when L2TP retransmission takes a long time.

Workaround: There is no workaround.

- CSCth91984

Symptoms: Standby resets continuously.

Conditions: This symptom is observed when 32 extended communities are configured with the **set extcommunity** command on the active RP.

Workaround: Unconfigure the **set extcommunity** command.

- CSCth92820

Symptoms: Some serial interfaces are not coming up after performing shut/no shut in fr\_scaling.

Conditions: This symptom is observed with frame relay scaling in a channelized card.

Workaround: Performing a shut/no shut on the hardware module will bring up the interfaces.

- 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.

- CSCth97341

Symptom: L4R is not working properly.

Conditions: This symptom is observed after a microcode reload.

Workaround: There is no workaround.

- CSCth98344

Symptoms: When using DMVPN with vrf configuration, if fvrf is not the same as ivrf, HUB router does not send delete notify during invalid SPI event.

Conditions: This symptom is observed under the following conditions:

- Use vrf
- DMVPN topology (only HUB is affected)
- HUB router has only isakmp SA and Spoke router has both ipsec and isakmp SA

Workaround: Rekeying or manual SA clear on spoke can solve the problem.

Alternate Workaround: Configure fvrf == ivrf.

- CSCth99560

Symptoms: VRF mapping service fails to apply correctly for via radius-proxy authenticated sessions if IP address is not assigned during authentication.

Conditions: This symptom is observed when VRF mapping service for via radius-proxy authenticated sessions No IP address is assigned as part of the authentication.

Workaround: There is no workaround.

Further Problem Description: VRF mapping service would apply successfully if the IP address is present in the authentication response. However, this was just verified in lab tests and is not a realistic scenario.

Radius-proxy authentication functionality is used on ISG for EAP-SIM based authentications in PWLAN environments. During the initial EAP-SIM authentication PWLAN subscribers do not have L2/L3 connectivity to the network yet. IP addresses are assigned to the subscribers once the initial EAP-SIM authentication completes and the DHCP server sends a DHCP-related RADIUS accounting start to ISG. Once this DHCP accounting message arrives, the VRF mapping service should be activated / updated.

- CSCti00020

Symptoms: Standby takes more time to come up on SSO.

Conditions: This symptom depends on the SIP-based cards that are on the chassis. Every single SIP-based card increases the time by one more minute.

Workaround: There is no workaround.

- CSCti04678

Symptom: A Cisco router crashes with redzone corruption.

Conditions: This symptom is observed when a router is configured for any subscribers and someone tries to execute some of the “show” CLI while clearing the sessions.

Workaround: There is no workaround.

- CSCti12726

Symptom: The compatibility matrix (CM) is not present in RLS7 branch/image. This would block Cisco IOS In-Service Software Upgrade (ISSU) from 7.0 to 7.x.

Conditions: This symptom is observed with a Cisco IOS ISSU.

Workaround: Cisco IOS ISSU can be done by disabling cm check via CLI.

- CSCti14290

Symptoms: A Cisco 7600 series router acting as the PE router in an MPLS network may stop forwarding traffic for certain IP prefixes within a VRF. This symptom may occur after a router reload, upgrade or crash due to corrupted hardware-forwarding information on the ingress module for the VPN label of the affected IP prefix.

The problem can be identified by comparing the output of the following commands:

1. Determine the BGP VPN Label for the prefix:

**show ip bgp vpnv4 all vrf vrf name prefix**

```
router# sh ip cef vrf test 10.1.1.1 detail 10.1.1.0/24, epoch 13 local label info:
other/4828 <== label is 4828 recursive via 10.100.1.2 attached to
GigabitEthernet1/1
```

- Determine the hardware forwarding for the prefix on the Supervisor:

**show mls cef mpls label label detail**

```
RCORL02#sh mls cef mpls label 4828 detail
Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority D -
FIB Don't short-cut, m - mod-num, E - ELSP? Format: MPLS - (b | xtag vpn pi cr
mcast label1 exp1 eos1 valid2 label2 exp2 eos2) V(2570 ): B | 1 0 0 0 0 4828 0 1 0
0 0 0 (A:213683 ,P:0,D:0,m:0 :E:1) M(2570 ): F | 1 FFF 0 0 1 FFFF 0 1 0 0 0
```

**show mls cef adjacency entry entry id**

```
DRCORL02#sh mls cef adjacency entry 213683 detail
Index: 213683 smac: 0000.0000.0000, dmac: 00d0.2b12.5500 mtu: 65535, vlan: 1024,
dindex: 0x7FFA, l3rw_vld: 1 format: MPLS, flags: 0x1000008600 label0: 0, exp: 0,
ovr: 0 label1: 0, exp: 0, ovr: 0 label2: 0, exp: 0, ovr: 0 op: POP packets: 0,
bytes: 0
```

- attach to the ingress module and use the same commands as step 2 and compare the values; if the destination mac address is not the same there is hardware forwarding corruption. Note: The adjacency index will be a different number on the module dfc.

**remote login module module number**

```
Router# remote login module 1 Trying Switch ... Entering CONSOLE for Switch Type
"^C^C^C" to end this session
```

```
Router-dfc1#sh mls cef mpls label 4828 detail Codes: M - mask entry, V - value
entry, A - adjacency index, P - FIB Priority D - FIB Don't short-cut, m - mod-num,
E - ELSP? Format: MPLS - (b | xtag vpn pi cr mcast label1 exp1 eos1 valid2 label2
exp2 eos2) V(1301 ): B | 1 0 0 0 0 4828 0 1 0 0 0 0 (A:147570 ,P:0,D:0,m:0 :E:1)
M(1301 ): F | 1 FFF 0 0 1 FFFF 0 1 0 0
```

```
0 0 Router-dfc1#sh mls cef adjacency entry 147570 detail Index: 147570 smac:
0000.0000.0000, dmac: 0000.138b.0000 mtu: 65535, vlan: 1024, dindex: 0x7FFA,
l3rw_vld: 1 format: MPLS, flags: 0x1000008600 label0: 0, exp: 0, ovr: 0 label1: 0,
exp: 0, ovr: 0 label2: 0, exp: 0, ovr: 0 op: POP packets: 59, bytes: 24025
```

Conditions: The Cisco 7600 must have a distributed forwarding card installed on the ingress module and be configured as an MPLS PE router. The problem is only observed after a router reload, upgrade or crash.

Workaround: Reloading the ingress module will resolve the hardware forwarding corruption on the module:

**hw-module module module number reset**

- CSCti26540

Symptoms: A memory leak in both SSS Manager and AAA Attribute list can be created when multiple services are downloaded and one of the services fails.

Conditions: This symptom is observed when a failure in the finishing application of all services leads to a memory leak in the cleanup code.

Workaround: Proper service profiles should avoid the memory leak.

- CCSCti35170

Symptoms: With REP over EVC configured and a high volume of traffic, REP could flap due to REP Hellos getting dropped.

Conditions: This condition is observed only when a high volume of traffic (mostly priority traffic) is sent on the interface.

Workaround: There is no workaround.

- CSCti37533
 

Symptoms: A Cisco router may crash.

Conditions: This symptom is observed with a half-inserted standby card that generates an internal stall; if this stall continues for more than 30 seconds, a crash occurs.

Workaround: Remove or fully insert the standby card.
- CSCti39893
 

Symptoms: On the PE with no receivers, traffic gets punted to the CPU. Expected behavior is to drop this traffic in the HW.

Conditions: This symptom is observed when running SSM in the core and SM in VPN. We have VRF with no data MDT, hence all traffic is transferred over default MDT.

Workaround: There is no workaround.
- CSCti41910
 

Symptoms: Changes to the spanning-tree mst instance configuration are not synced to a standby SP. Hence, after a switchover, the new Active will have old MST instance configuration on SP.

Conditions: The symptom is observed after completing the following steps:

  1. Configure MST instance configuration
 

```
(config)#spanning-tree mst configuration (config-mst)#instance 1 vlan 102
```
  2. Do HA switchover
  3. “Show spanning-tree mst configuration” on active SP will not show “instance 1” in configuration.

Workaround: Reload the standby.

Further Problems Description: Bulk sync for MST configuration works fine. Only the incremental configuration sync is broken.
- 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.

- CSCti61394
 

Symptoms: While sending a multicast stream in default MDT with “spt-threshold infinity” configured on the CE, all the traffic is punted into the CPU, and the stream is cut to a 1000 pps speed. The CPU levels are not as high; occasionally, there are some higher peaks in the interrupt levels and in the CPU, but nothing critical.

Conditions: This symptom is observed only in default MDT when “spt-threshold infinity” is configured on the CE. When the “spt-threshold infinity” is unconfigured from the CE, or SB6aa is loaded on the PE router, this issue is not seen.

Workaround: Switch to Data MDT.
- 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.
- CSCti67559
 

Symptoms: A Cisco router may crash.

Conditions: This symptom is observed when configuring ip multicast routing after ip pim sparse-mode has been configured under an interface.

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.”
- 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.
- CSCti81137
 

Symptom: Port-channel interfaces are flapping.

Conditions: This symptom is observed with a single member link.

Workaround: There is no workaround.
- CSCti83737
 

Symptom: SIP-600 will crash with a software-forced crash:

```
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 SIP-600.

Workaround: There is no workaround.



## Open Caveats—Cisco IOS Release 15.0(1)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.0(1)S. All the caveats listed in this section are open in Cisco IOS Release 15.0(1)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCeh32251

**Symptoms:** A mismatched bandwidth may generate corrupt packets that are not detected in the hardware when CRC-16 is configured on the interfaces. The corrupt packets may cause the CPU usage of the RP to increase to 100 percent, and the corrupt packets may be dropped.

**Conditions:** This symptom is observed on a Cisco platform that is configured with a 2-port or 4-port clear channel T3/E3 SPA (SPA-2XT3/E3 or SPA-4XT3/E3) or 4-port channelized T3 (DS0) SPA (SPA-4XCT3/DS0) that is configured for T3 DSU Kentrox mode with a subrate bandwidth above 35,000 when the far-end is also configured for DSU Kentrox mode but with a mismatched bandwidth that is less than 35,000

**Workaround:** When you use DSU Kentrox mode, configure CRC-32 on the interfaces and configure the correct bandwidth before you enable the interfaces.

- CSCsj70622

**Symptoms:** Cisco router running Cisco IOS Release 12.2(33)SRD or 12.2(33)SRE may experience a memory leak due to crypto processes using MallocLite.

**Conditions:** The symptom is observed when crypto is configured.

**Workaround:** There is no workaround.

- CSCsv23450

**Symptoms:** If you type any interface name at a configuration prompt and hit “?”, an IDB is created. If the command is cancelled, the recently-created IDB remains in the system which causes problems after a switchover.

**Conditions:** The symptom is observed if you type any interface name at a configuration prompt and hit “?”, thus creating an IDB.

**Workaround:** Do not cancel the command. Instead complete the command by using “enter”.

- CSCsv70157

**Symptoms:** On a Cisco 7609 router that is running Cisco IOS Release 12.2(33)SRD, after configuring any interface with any carrier-delay value other than 0 (the default), upon entering **wr mem** you get an unexpected warning message:

```
"Warning: Overriding existing carrier delay value to 0"
```

**Conditions:** There appears to be no special conditions to reproduce this defect. Simply configure any interface with a carrier delay and execute **wr mem**:

```
Router#conf t
      Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f2/12
Router(config-if)#carr
Router(config-if)#carrier-delay 2
Router(config-if)#end
Router#wr
Building configuration...
Warning: Overriding existing carrier delay value to 0
```

```
%SYS-5-CONFIG_I: Configured from console by console[OK]
Router#
```

Workaround: There is no workaround.

Further Problem Description: This warning should come when Asymmetric Carrier Delay (ACD) is configured on an interface and you then attempt to configure Standard Carrier Delay via the **carrier-delay** *delay* interface command. However, the message is coming when ACD is not configured.

- 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.

- CSCta37670

Symptoms: Router crashes due to the interrupt being held for too long under stress loading.

Conditions: The symptom is observed when using the BGP PIC feature and MPLS with 300,000 prefixes.

Workaround: There is no workaround.

- CSCtb54422

Symptoms: An MFR bundle moves from SW to HW mode and flaps after reload.

Conditions: This symptom is observed on a Cisco 7200 router when an MFR is configured on CJ-PA, then one member is added from MCTE1 and the following commands are entered: **wr mem** and **reload**.

Workaround: Create a new MFR after reload and add members to it.

- CSCtb66273

Symptoms: EzVPN traffic is getting dropped at the DVTI interface on the server.

Conditions: The symptom is observed with an EzVPN DVTI server configured with split tunneling.

Workaround: Removing the split tunnel configuration.

- CSCtd08709

Symptoms: When one LTS is restricted CAC calls are not terminating through another LTS.

Conditions: The symptom is observed when configuring call admission control on LTS2 to one and making 20 calls through LAC (all are going to LTS2 as per the priority). As call admission is configured on LTS2, the call should be diverted back to LAC and should terminate on LTS1. This is not happening.

Workaround: Do not restrict call admission control on LTS.

- CSCtd87072

Symptoms: IOSD restart seen.

Conditions: The symptom is observed when changing tunnel mode on scaled IPsec sessions.

Workaround: There is no workaround.

- CSCtd87788  
Symptoms: Traceback is seen when serial from second CJ-PA controller is added and removed from multilink. This interface remains up/down until a reload.  
Conditions: This symptom is seen when serial from second controller in unchannelized mode is added to multilink.  
Workaround: Reload the box to bring up the interface.
- CSCte30136  
Symptoms: An adjacency might be incorrectly programmed as drop (dindex: 0x7FFF) on one or multiple DFC cards, while the SUP and other DFC cards have the correct hardware programming.  
Conditions: The symptom is observed after a link flap.  
Workaround: There is no workaround.
- CSCte48131  
Symptoms: A Cisco 7200 G2 may crash.  
Conditions: The symptom is observed when a multilink has members from CJ-PA and MCTE1. Then you configure the minimum mandatory members on multilink as four. Since the multilink has three members, it is down. Now try to flap the multilink using the **clear int range multilink1 1** to see the crash.  
Workaround: There is no workaround.
- CSCte86038  
Symptoms: High CPU utilization for ATM OAM timer process.  
Conditions: The symptom is observed with a scaled L2 VC configuration.  
Workaround: Increase the AIS RDI timeout with higher number of up and down retries.
- CSCtf01109  
Symptoms: The NAS-IP-Address value in the “accounting start” changes after an RP SSO. Before the RP SSO, the NAS-IP-Address contains the IP address of the interface connected to the AAA server. After an RP SSO, the new active RP sends out a new accounting start. This time, the NAS-IP-Address contains the loopback0 IP address. When the session disconnects, the accounting stop record contains the correct IP address.  
Conditions: The symptom is observed in a redundant RP system with PPP subscribers.  
Workaround: There is no workaround.
- CSCtf05408  
Symptoms: IP address on a loopback interface is lost.  
Conditions: The conditions are currently under investigation.  
Workaround: Reconfigure the loopback interface.
- CSCtf32348  
Symptoms: Router crashes.  
Conditions: The symptom is observed when you apply “ip security dedicated topsecret sci nsa” on any of the interfaces.  
Workaround: Remove “ip security dedicated topsecret sci nsa” configuration.

- CSCtf54919
 

Symptoms: When you bring down the virtual-access interface the router crashes giving CPU hog messages.

Conditions: The symptom is observed when using the fix for CSCtc42941.

Workaround 1: When an access list is removed, remove corresponding “distribute-list” configuration as well.

Workaround 2: Do not use the same access list name for IPv4 and IPv6.
- CSCtf90970
 

Symptoms: TX CPU might crash on a Cisco 7600 SIP-200 due to a particle chain corruption.

Conditions: The symptom is observed when “ppp multilink interleave” is configured on a multilink PPP bundle.

Workaround: Disable the “ppp multilink interleave” feature on the multilink PPP bundle.
- CSCtf92354
 

Symptoms: Traceback seen when doing a shut/no shut under heavy traffic (100Mbps).

Conditions: The following steps cause this issue:

  1. 256 dLFioATM interfaces on a single PA.
  2. Traffic is flowing through all the bundles which is above NDR (100 Mbps) but less than interface bandwidth (155Mbps). This 100 Mbps traffic includes 20 Mbps of 64 byte + 40 Mbps of TCP + 40 Mbps of UDP.
  3. Do a shut/no shut.
  4. Tracebacks will be seen.

Workaround: There is no workaround.
- CSCtg01296
 

Symptoms: Enhanced FlexWAN with scaled DLFi setup resets on doing a shut/no shut on the ATM interface.

Conditions: The symptom is observed with the following steps:

  1. 256 dLFioATM interface on a single PA.
  2. Traffic of around 44 Mbps Imix types is flowing through the all bundles. This is equally divided between all the bundles.
  3. Do a continuous shut/no shut.
  4. Enhanced FlexWAN might reset. It does not generate a crashinfo.

Workaround: There is no workaround.
- CSCtg08523
 

Symptoms: The following message is seen at random intervals on the console and/or in the syslogs:

```
%CONST_DIAG-SP-3-HM_TEST_FAIL:TestIPSecEncrypDecrypPkt
```

Conditions: This issue is seen on a Catalyst 6500 with an SPA-IPSEC-2G module running Cisco IOS version 12.2SXI.

Workaround: There is no workaround.

Further Problem Description: The root cause appears to be the SPA not replying to the diagnostic packets from the supervisor from time to time. User traffic is not affected.

- CSCtg11344  
Symptoms: A few PPPoA sessions fail to sync up with the standby.  
Conditions: The symptom is observed after an SSO switchover in a scaled scenario.  
Workaround: There is no workaround.
- CSCtg32407  
Symptoms: RP crashes.  
Conditions: The symptom is observed on a Cisco router that has ATM multipoint interfaces configured with different BBA groups of different session limits. If you deconfigure the BBA-group first and then remove the PPPoE configurations from the ATM interface, the crash is seen.  
Workaround: First disable the PPPoE configuration under interface level and remove any references to the BBA-group from the interfaces. After that unconfigure the BBA group.
- CSCtg35257  
Symptoms: The message “previous instance of CNS Event Agent still executing” is seen even if a CNS event is not configured.  
Conditions: The symptom is observed if the **cns event <IP> encrypt** command is enabled and disabled.  
Workaround: There is no workaround.
- CSCtg35298  
Symptoms: Traffic drops are seen between two PEs after re-optimization.  
Conditions: The symptom is observed with 16k VPLS VC, 4k scalable EoMPLS, 1K software EoMPLS, 600 primary tunnels to nPE1 and one tunnel to nPE2 from nPE3.  
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**.
- CSCtg48368  
Symptoms: BFD sessions flap.  
Conditions: The symptom is observed when an outbound QoS shaper policy is applied to the port with BFD configured.  
Workaround: Put in the class-map match protocol ARP and add that to the MQC policy in a separate class.
- 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.

- CSCtg49474

Symptoms: Assertion failure in c10k\_jacket4spa\_isr.c is seen after SSO due to multiple PXF crashes.

Conditions: This symptom occurs after SSO due to multiple PXF crashes.

Workaround: There is no workaround.

- CSCtg57599

Symptoms: Lots of SNMP CPUHOG messages are seen and there is a crash due to a watchdog timeout:

```
%SYS-3-CPUHOG: Task is running for (126004)msecs, more than (2000)msecs
(252/37),process =SNMP ENGINE
```

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SNMP ENGINE
```

Conditions: The symptom is observed when polling Dot3Stats.

Workaround 1: Use the following command: **no snmp-server sparse-tables**.

Workaround 2: Block the objects in dot3 mib that contains this table from being polled:

```
snmp-server view cutdown iso included
snmp-server view cutdown 1.3.6.1.2.1.10.7 excluded
```

Then to apply the view, use:

```
no snmp-server community your_string_here RO
no snmp-server community your_string_here RW
```

and then put it back so it looks like:

```
snmp-server community your_string_here view cutdown RO
snmp-server community your_string_here view cutdown RW
```

- CSCtg65989

Symptoms: Only the first user is able to get authenticated successfully and browse the internet. All subsequent users are constantly redirected to the web portal after successful authentication. The **show sss sess uid xxx** command shows that the internet service is not applied to the account even though the session is authenticated.

Conditions: The symptom is observed with customers using web logon with a session applying an auto service.

Workaround: Remove “autoservice” and apply static service at account logon.

- CSCtg84969

Symptoms: The output of **show ip mfib vrf vrf name verbose** may show the following line “Platform Flags: NP\_RETRY RECOVERY HW\_ERR” and multicast traffic may not be hardware switched.

Conditions: The symptom is observed on a dual RP Cisco 7600 series router with line cards after multiple reloads or SSO switchovers. When the issue occurs the output of **show ip mfib vrf vrfname verbose** on the standby SP will show some lines preceded with “###” where an interface name is expected.

Workaround: There is no workaround.

- CSCtg94250

Symptoms: Removing **address-family ipv4 vrf vrf** (in router BGP) followed by **no ip vrf vrf** (where “vrf” is the same) could result in a crash.

Conditions: The symptom is observed in a large VPNv4 scale setup, when applying the following commands to the same VRF back-to-back:

1. **no address-family ipv4 vrf vrf**
2. **no ip vrf vrf**
3. **ip vrf vrf**

The trigger of the BGP crash is a result of a racing condition between event 1 and event 2.

Workaround: Since this is a racing condition, the workarounds are:

1. Not applying (1) before (2).
2. Give sufficient time for (1) to complete before applying (2).

- CSCth07333

Symptoms: Intermittently an IP session cannot be established. The following error message is seen prior to the issue:

```
%SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error: Class SSS: - update segment failed.
```

Conditions: The symptom is observed on a Cisco 7204VXR that is running Cisco IOS Release 12.2(33)SRC4.

Workaround: There is no workaround.

- CSCth13105

Symptoms: Traceback is seen at `polycymgr_handle_get_context`.

Conditions: The symptom is observed while creating a session with many policies attached.

Workaround: There is no workaround.

- 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.

- CSCth21050

Symptoms: ASBR2 is not able to ping RR2 loopback address.

Conditions: The symptom is observed when verifying inter-AS IG connectivity in both ASs. The switching path on 6PE1 is CEF.

Workaround: There is no workaround.

- CSCth24102
 

Symptoms: There is some differences between CEF and MLS routing entries. Some of the routes in VRF1 in CEF are not preset in MLS VRF1, but are seen in some other VRFs.

Conditions: The symptom is observed with a line card reset.

Workaround: There is no workaround.
- CSCth24135
 

Symptoms: A Cisco 7600 series router that is running Cisco IOS Release 12.3(33)SRD4 experiences two known issues:

  1. Device crashes at a crypto process.
  2. Memory leaks on each accounting request which eventually consumes the processor memory and causes a reload.

Conditions: The symptoms are observed when “aaa accounting” is configured for crypto.

Workaround: Remove “aaa accounting” broadcast.
- CSCth37793
 

Symptoms: High CPU utilization caused by process switching of multicast traffic after IPv6 Address Family (AF) is configured for VRF.

Conditions: The symptom is observed on a Cisco 7600 series router that is acting as a PE router in mVPN. It is seen with multicast traffic forwarded inside a VRF for which IPv6 AF is configured. The issue can be seen when you:

  1. Bootup with VRF configured only with IPv4; configure IPv6 AF after bootup.
  2. Bootup with VRF configured with both IPv4 and IPv6 AF; unconfigure IPv6 AF after bootup.

Workaround 1: Unconfigure IPv6 AF from VRF.

Workaround 2: Clear mroute for VRF.

Workaround 3: Reload device.

Further Problem Description: Problem can be identified on a device following those steps:

  1. High CPU seen using **show proc cpu**.
  2. **sh redundancy** used to identify slot with active supervisor as *X*.
  3. Attach *X*.
  4. **sh platform software vpn mapping | i VRF-NAME\_HERE:**  
 IOS | *VRF-NAME-HERE* | 4 || *NUMBER1* | 0x0004 | 0x0000 | R[2]:4
  5. **show platform software multicast ip cmfib vrf REN SOURCE GROUP verbose:**  
 Multicast CEF Entries for VPN#4 (*SOURCE*, *GROUP*) IOSVPN:*NUMBER2* (1) PI:1 (1) CR:0 (1)  
 Recirc:0 (1)
  6. If *NUMBER1* and *NUMBER2* do not match, the defect is hit.  
 (Note: Values in “<>” are variables fitting your configuration.)
- CSCth39857
 

Symptoms: OBFL semaphore waits indefinitely in “IPC Seat Manager” process context causing all the messages in IPC inbound to starve, thereby accumulating the leak. 8090 messages considered as IPC message leak:

```
ESM-20G-7#sh proc even 23
```



```

Process 23: IPC Seat Manager, state: Waiting for Event
  Watching semaphore 'OBFL UPTIME SEM' (0x468DBE60), id 0x0, value 1.
  ---
  Watching queue 'IPC inboundQ' (0x468D67CC), id 0x0, count 8090.

```

Conditions: The symptom is observed with the “IPC Seat Manager” process.

Workaround: There is no workaround.

- CSCth39988

Symptoms: Memory leak with MIB.

Conditions: The symptom is observed when MIB has opened 4040 sessions with DFC. In each session it has leaked one message and caused 4040 IPC message leaks. The reason for such a huge number of Rx sessions could be related to [1] as the IPC\_CLOSE\_PORT request goes via “IPC inbound” and it is never processed.

Workaround: There is no workaround.

- CSCth42594

Symptoms: Remote standby router crashes when you configure and remove “ppp multilink mrru local” under a multilink interface.

Conditions: The symptom is observed with the following conditions:

1. When multilink is bundled with more than one serial interfaces (not seeing this issue with only one serial interface).
2. Seeing this issue from 1500 and above (not seeing this issue when configure and remove “ppp multilink mrru local 1499”).

Workaround: There is no workaround.

- CSCth45336

Symptoms: Under extremely rare conditions, a multicast replication engine table might be corrupted with circular dependency. This might lead to a multicast packet replicated at very high rate potentially affecting the control plane stability.

Conditions: Conditions are unknown at present.

Workaround: Corruption can be cleared by:

1. Reloading a line card with corrupted replication table; or
2. By switching to ingress replication mode (from egress mode). This workaround should be tried first (as it is less impacting) and if that does not work the line card may be reloaded.

Further Problem Description: In the instance where this issue has been seen the packet was sent to the RP CPU which drove high CPU utilization. It was possible to limit the impact on CPU by configuring rate-limiter for multicast partial shortcut packets to 3000 packets. However, it must be noted that potentially the packet might be sent out of only some interfaces, sent only to the RP, or in another combination depending on how the table will be corrupted.

- CSCth47473

Symptoms: After microcode reload, the traffic does not recover and SPA configuration errors are seen.

Conditions: The symptom is observed with a serial interface set with less than 4-5 seconds keepalive.

Workaround: Reload the SIP.

Further Problem Description: The issue is seen with serial interfaces set with `keepalive` of 4-5 seconds and less, as the microcode reload takes around 7 seconds and until then it stops the `keepalive` from reaching from the SPA to the host. The interface goes down and the host tries to bring it up by resending the serial configuration to the SPA.

- CSCth47875

Symptoms: Incorrect bandwidth remaining ratios may be observed.

Conditions: This symptom is seen when `fair-queue` is configured with a user defined `queue-limit`. If the `queue-limit` is defined in the configuration after the `fair-queue` statement, the per-flow queue limit may be incorrect.

Workaround: Define a per-flow queue limit on each class configured with `fair-queue`, or make sure that the user defined `queue-limit` is defined in the configuration prior to the `fair-queue` statement.

- CSCth47888

Symptoms: In a Hot-Standby psuedowire redundancy setup, traffic is forwarded on the Standby psuedowire instead of the Active psuedowire which is in up/up state.

Conditions: This symptom is seen in a Cisco 7600 router that is running Cisco IOS Release 15.0(1)S with hot psuedowire redundancy configuration.

Workaround: There is no workaround.

- CSCth49604

Symptoms: CPU hog traceback is seen when the **no ip routing** command is issued.

Conditions: The symptom is observed under the following conditions:

1. 8000+ PPPoE sessions are established.
2. You clear all the sessions.
3. The **no ip routing** command is issued.

Workaround: Do not use the **no ip routing** command with a scaled setup.

- CSCth50479

Symptoms: With high rate of session churn, the **show subscriber sessions** command shows sessions are stuck in the “Attempting” state. The **show subscriber stat detail** command shows that these sessions are actually stuck in the “installing-config” state.

Conditions: The symptom is observed with a high rate of PPP session churn and with a large number of sessions (resulting in more than 70% IOS memory used).

Workaround: Router reload is required to clear stuck sessions.

- CSCth55315

Symptoms: Spurious interrupts show 375.

Conditions: This symptom occurs when the router is booted with configuration as in `run_config`. Malformed packets that are pumped to it could reload.

Workaround: There is no workaround.

- CSCth58047

Symptoms: SSH server may fail after the RSA key is generated.

Conditions: This issue occurs intermittently under normal conditions.

Workaround: Zeroize and re-generate the RSA key.

- CSCth59593  
Symptoms: Spurious memory access is seen.  
Conditions: The symptom is observed when issuing the command **show pxf cpu isg ip-session mtrie no**.  
Workaround: There is no workaround.
- CSCth64700  
Symptoms: On a Cisco 7600 series router or on a Cisco Catalyst 6500 series switch, a high CPU may be experienced if an IPv6 packet with a link local source address is received on an interface configured for EoMPLS.  
Conditions: The symptom is observed when an inband trace (“rp-inband tx”) is enabled.  
Workaround: Remove the monitor session configured for the inband trace.
- CSCth66700  
Symptoms: (S,G) expiry timer is updated again about two minutes after stopping the (S,G) stream.  
Conditions: The symptom is observed with the (S,G) expiry timer.  
Workaround: There is no workaround.  
Further Problem Description: The behavior of the expiry timer is not changed even if you change the value of **mls ip multicast flow-stat-timer**.
- CSCth69504  
Symptoms: A Cisco 7600 series router may experience a small buffer leak in the small buffer pool on SP.  
Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD configured with IGMP snooping.  
Workaround: Disable IGMP snooping either globally or per VLAN.
- CSCth69525  
Symptoms: Multicast traffic is not forwarded towards the CE router on the ATM interfaces.  
Conditions: The symptom is observed with AAL5MUX which shows that there is an active stream towards the CE, but the CE is not receiving this stream. With AAL5SNAP encapsulation, we cannot see any active stream.  
Workaround: There is no workaround.
- CSCth71095  
Symptoms: DHCP binding table is not completely synced to standby RP.  
Conditions: This symptom occurs when box is acting as DHCP Relay and ISG is configured.  
Workaround: Use unnumbered multiservice interface instead of numbered one.
- 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.

- CSCth71899  
Symptoms: An SSO causes a met3 VLAN to become 0.  
Conditions: The symptom is observed with 600 S,G distributed with OIFs over SVIs and L3 interfaces and after an SSO. It happens only on triggering joins and leaves for the groups, on the CFC card.  
Workaround: There is no workaround.
- CSCth72565  
Symptoms: The reachability of the PE2 router's loopback is lost from PE1 after an interface flap in the core. The LSP toward PE2 "breaks" due to data plane programming error (wrong labels).  
Conditions: The symptom is observed with MPLS with the presence of ECMP. The PE1 has two uplinks to core routers. In a steady state there is no ECMP between PE1 and PE2. When a link is lost in the P-core (link flap or shut/no shut) there is ECMP between PE1 and PE2. After the link flap between the two P routers in the core, PE1 is losing connectivity to PE2.  
Workaround 1: Use the **clear ip route** on the affected IP address.  
Workaround 2: Avoid ECMP by altering link cost.
- CSCth72765  
Symptoms: Configuring "mls qos protocol hsrp police *rate*" does not enable policing of HSRPv2 packets.  
Conditions: The symptom is observed on a Cisco 7600 series router when "mls qos protocol hsrp police *rate*" is configured.  
Workaround: There is no workaround.
- CSCth74112  
Symptoms: A ping from a directly connected PC to a Cisco 7600/SUP720 has large latency varied from 1ms to 2s.  
Conditions: The symptom is observed with a ping from a directly connected PC to a Cisco 7600/SUP720.  
Workaround: There is no workaround.
- CSCth75354  
Symptoms: There is an intermittent problem when a SPAN source is set to be a VLAN. The destination in the SPAN session does not receive the data.  
Conditions: The symptom is observed on a Cisco 7600 series router with an ES+20 card that is running Cisco IOS Release is 12.2(33)SRE0.  
Workaround: Reload the module.
- CSCth79882  
Symptoms: Traffic counters give double the value of matching.  
Conditions: This symptom occurs when there is a TC service and sending traffic and checking the session statistics.  
Workaround: There is no workaround.
- CSCth83055  
Symptoms: VPNv4 route-reflector with 240K from multiple neighbors crashes in certain conditions.  
Conditions: The symptom is observed with Cisco IOS Release 12.2(31)SB16.

Workaround: There is no workaround.

Further Problem Description: The issue is due to heavy BGP churn in the network. The PEs become desynchronized with the RRs.

- CSCth83421

Symptoms: A standby PRE crashes.

Conditions: The symptom is observed when PPP is configured on a router that is running Cisco IOS Release 12.2(33)SB8a.

Workaround: There is no workaround.

- CSCth85040

Symptoms: A Cisco Catalyst 6000 series switch crashes due to a bus error.

Conditions: The symptom is observed on a Cisco Catalyst 6000 series switch with Sup2 that is running Cisco IOS Release 12.1(26)E8 and while configuring a new network line under OSPF.

Workaround: There is no workaround.

- CSCti03199

Symptoms: During switch-over, standby crashes after every recovery due to config-sync.

Conditions: This symptom happens while it tries to sync with Active when crypto pki trustpoint is configured with an unavailable port-channel as source-interface.

Workaround: There is no workaround.

- CSCti03603

Symptoms: Router may reload after the following error messages are observed in succession:

```
%LLIST-3-ONLIST: add(de) %LLIST-3-OFFLIST: rem(de)
```

Conditions: This symptom is seen when router is running mpls.

Workaround: There is no workaround.

- CSCti10188

Problem Statement: GE port does not come up 3% of times after doing spa reload. It does not affect 1588-2008 or Sync-e services offered by 2x2GE\_SYNCE SPA. If you are not using GE ports of this SPA for data or 1588 packets transport, it does not affect you.

Symptoms: Link does not come up even after doing “shut/no-shut” on GE port. The following syslog message appears in router logs:

```
SLOT 2: *Jul  8 04:34:04.167: %SIPSPA-4-SPABUS: Bay 1 RD failed. sz=3
rd_par=0 noresp=0 err_1=0 addr=0x1040204 data=0x0 parity=0xF1 deadman=4
```

Conditions: This symptom occurs when there are multiple SPA reloads and power cycles.

Workaround: Reload SPA if link does not come up.

## Resolved Caveats—Cisco IOS Release 15.0(1)S

All the caveats listed in this section are resolved in Cisco IOS Release 15.0(1)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCdy26008

Symptoms: The negotiated IP address is not cleared from an asynchronous interface when a call ends, even though the IP address is returned properly to the IP peer pool.

Conditions: This symptom is observed when the peer is configured to dial in to the network access server (NAS) and to obtain an IP address through IP Control Protocol (IPCP) negotiations with the NAS. The NAS is configured with pools of IP addresses to be allocated to the peer when the peers generate a PPP call to the NAS. The NAS is also configured to authenticate the peer through RADIUS.

Workaround: There is no workaround.

- CSCek75694

Symptoms: A router running Cisco IOS 12.4T may reload unexpectedly

Conditions: Occurs when BFD is configured and active.

Workaround: Disable the BFD feature.

- CSCsc13670

Symptoms: The backup configurations that are generated by the Archive feature may be truncated.

Conditions: This symptom is observed when you reload the router with the Archive feature enabled.

Workaround: Enter the privileged mode.

Another workaround is using Kron,

Since archiving works fine if we use the **archive** configuration command, we can schedule the command. For example, see the followin:

```
kron policy-list CONFIG-ARCHIVE
  cli archive config
kron occurrence CONFIG-ARCHIVE in 1:0 recurring
  policy-list CONFIG-ARCHIV
```

- CSCsi25430

Symptoms: A router crashes when the **show processes event** command is issued.

Conditions: The symptom is observed when the **show processes event** or **show tech** commands are issued.

Workaround: There is no workaround.

- CSCsk84780

Symptoms: High CPU usage may occur when IPCP is being renegotiated. Eventually, the high CPU usage may cause buffers to be backed up, may cause error message to be generated, and may cause L2TP tunnels to be dropped.

Conditions: This symptom is observed on a Cisco router when clients renegotiate IPCP unnecessarily. You can verify this situation by enabling the **debug ppp negotiation** command or by configuring RADIUS authorization and then checking the virtual-access interface for the phrase “cloned from: AAA, AAA, ...” (that is, multiple instances of AAA) as identification.

Workaround: There is no workaround.

Further Problem Description: You can alleviate the situation somewhat by configuring the NCP Timeout to 15 seconds to disconnect clients that take a long time to renegotiate IPCP. You can also do the following:

- Increase the hello timers for L2TP and for the receive windows.
- Configure the timers under the virtual template.
- Do not configure the **redistribution connected** command under a routing protocol such as (but not limited to) EIGRP, RIP, or OSPF.

- Ensure that the IP local pools are concise. For example, create one statement for multiple /24s instead of splitting all /24s on single lines, because with single lines, the look-up becomes long and contributes to the high CPU usage.
- CSCsk86642
 

Symptoms: SPA-2xOC3-POS is not seeing the correct K1/K2 bytes on working group 1 APS, when switching from Protect to Working port.

Conditions: This was observed in a lab environment with a Cisco 7604 router back to back with a Cisco 7206 router. Code tested Cisco IOS Release SRA1 and Cisco IOS Release SRA2.

Workaround:

  1. Hw-slot reset on the Sip400-SPA corrects the problem.
  2. A shut/no shut on the protect interface corrects the problem.
- CSCs114450
 

Symptoms: Under a high load of multicast traffic, a Cisco router may unexpectedly reload due to a CPU vector 300 or bus error.

Conditions: This symptom has been observed only in environments where more than 10 tunnels have been configured on the same device using multicast over these tunnels.

Workaround: There is no workaround.
- CSCs192316
 

Symptoms: Router may experience mwheel CPUHOG condition.

Conditions: This condition is observed on Cisco router while clearing all L2TP sessions when there are more than 2500 sessions with multicast traffic flowing on the sessions.

Workaround: There is no workaround.
- CSCsm14833
 

Symptoms: All incoming ISDN calls are rejected.

Conditions: This symptom occurs when a Cisco IOS router is:

  - equipped with NPE-G2.
  - configured for ISDN dial-in with multiple Dialer Profiles.

This is seen in devices (Cisco 7206VXR) that are configured for ISDN PRI dial- in with Dialer Profiles for backup purposes.

The problem could be reproduced in the lab where ISDN BRI i.o. PRI line is in use:

  - When only 1 Dialer Profile is configured, all incoming ISDN calls are bound to it by default.
  - When 2 Dialer Profiles are configured in the same pool, all incoming ISDN calls were rejected due to “Incoming call rejected, unbindable”.

The Caller ID or DNIS binding cannot be used as all incoming ISDN calls have no Caller ID and the same DNIS.

Workaround: Upgrade to Cisco IOS Release 12.4(11)T or later releases, which also support NPE-G2.
- CSCsm62179
 

Symptoms: MPLS pseudowire ping for SVI Mode Ethernet over MPLS over GRE (EoMPLSoGRE) may fail.

Conditions: The symptom is observed if EoMPLSoGRE is configured with SVI mode.

Workaround: There is no workaround.

- CSCsm73592

Symptoms: A reload may occur when an anything over MPLS (AToM) VC is torn down. Bug triggered initial crash of SIP-400 in slot 4 & ES20 in slot 3. Both cards had to be powered down and reset from the console to recover.

Conditions: Occurs when AToM VC is setup and torn down later.

Workaround: There is no workaround.

Further Problem Description: The crash may occur when an event triggers access to a previously set up AToM VC. For example, the crash may occur when fast reroute (FRR) is configured on the tunnel interface and the primary interface is removed, such as in the following scenario:

```
pseudowire-class ER1_to_HR1_EoMPLS
    no preferred-path interface Tunnel501331 disable-fallback
!
interface tunnel501331
    shutdown
!
no interface tunnel501331
```

1

- CSCsm73602

Symptoms: High CPU load due to VTEMPLATE Backgr process.

Conditions: Occurs when **ip multicast boundary** command is used on many interfaces (8000 or more).

Workaround: There is no workaround.

- CSCso06409

Symptoms: A Cisco 7600 (RSP720-3C/CXL) may experience high CPU utilization from the moment (S,G) expires due to all outgoing interfaces are down.

Conditions: This symptom occurs when indirect-connected multicast source traffic arrives at PIM-RP router without any receiver on that group, a (\*,G) state with NULL RPF interface and NULL OIL is created and used to forward the traffic. Because of NULL RPF, this (\*,G) state cannot be installed in Cisco 7600 hardware. The multicast data packet is punting to CPU and causes high CPU utilization.

Workaround: Partial workaround is to apply RP rate-limiter with fib-miss option.

- CSCso18626

Symptoms: Destinations via MLPPP sessions may become unreachable following a switchover.

Conditions: The symptom is observed when MLPPP sessions are active and BGP nexthops are reachable via the MLPPP session prior to a switchover. An RP switchover then occurs.

Workaround 1: The affected multilink interfaces can be shut/no shut:

```
shut/no shut interface multilink <>
```

Workaround 2: Repopulating the routes in the affected VRF(s) will also restore reachability:

```
clear ip route vrf FOO
```



- CSCso57886
 

Symptoms: A Cisco IOS device may crash with a data bus error exception and stack trace PC = 0xA0000100

Conditions: Device is running normal production traffic. Presence of malformed punted RP packets in this network caused the issue.

Workaround: There is no workaround.
- CSCsq09962
 

Symptoms: Cisco 7600 router crashes at “pim\_proxy\_empty\_rd.”

Conditions: Customer seeing crash with decode during initial deployment of new Cisco 7600 router.

Workaround: There is no workaround.
- CSCsq75944
 

Symptoms: A Cisco Catalyst 6500 or a Cisco 7600 may reload unexpectedly. On the console or in the RP crashinfo file, the following message can sometimes be seen:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.
```

Conditions: This symptom occurs when NetFlow is configured on one of the following:

  - Cisco 7600 running Cisco IOS Release 12.2(33)SRC.
  - Cisco Catalyst 6500 running Cisco IOS Release 12.2SXH.

Workaround: Disable Netflow by using one of the following commands on every subinterface for which Netflow is configured:

**no ip flow ingress**

**no ip flow egress**

**no ip route-cache flow**

Other Notes:

Only the Cisco IOS Releases 12.2SRC and 12.2SXH code trains are affected. The specific versions affected are Cisco IOS Releases 12.2(33)SXH, 12.2(33)SXH1, 12.2(33)SXH2, 12.2(33)SXH2a, 12.2(33)SRC, and 12.2(33)SRC1.

The issue is fixed in the two affected code trains from the Cisco IOS Releases 12.2SXH3 and 12.2SRC2 onwards. However, for the Cisco IOS SXH train, Cisco would recommend the use of Cisco IOS SXH4 due to ddts CSCso71955.

The following release trains do not have this issue: Cisco IOS Releases 12.2(18)SXF, 12.2(33)SRA, 12.2(33)SRB, 12.2(33)SXI and all other release trains after those affected.
- CSCsq81116
 

Symptoms: Router may reload when Optimized Edge Routing (OER) master configuration is **shutdown** followed by **no shutdown**.

Conditions: This symptom only occurs when OER master controller goes down and then rarely.

Workaround: There is no workaround.
- CSCsq81235
 

Symptoms: A VRF cannot be configured again when it is deleted by using the **no ip vrf** command.

Conditions: This symptom is seen only on VRFs with an MDT tunnel.

Workaround: There is no workaround.

- CSCsr01709

Symptoms: Bus error crash at `ppp_sip_fsm_event` at switchover.

Conditions: The symptom is observed after a switchover and if PPP is configured.

Workaround: There is no workaround.
- CSCsr54959

Symptoms: Router crashed when removing a policy attached to a VLAN interface with a route map and access lists attached.

Conditions: This symptom occurs on a Cisco Catalyst 4500 that is running Cisco IOS Release 12.2(46)SG. The device may reload unexpectedly due to a software-forced crash. Defect also affects other platforms and releases of Cisco IOS.

Workaround: There is no workaround.
- CSCsr59284

Symptoms: Memory allocation fails. Sometimes neighbor relationship also drops.

Conditions: This symptom happens after entering **show mem** command. After the system booted up, while the Cisco 7600 system was receiving the BGP routes, the command is entered. Upon hitting the space key to scroll the windows for two to three times. The following errors are displayed:

```
%COMMON_FIB-3-NOMEM: Memory allocation failure for CEF: terminal fibs list in IPv4
CEF [0x08812F1C] (fatal) "
```

Workaround: Enter the **show mem sum** command.
- CSCsr74295

Symptoms: Upon reload, static routes pointing to MLPPP interfaces do not get inserted in the RIB.

Example: **ip route 172.16.2.2 255.255.255.255 multilink22**

Conditions: This symptom occurs in a router that is running Cisco IOS Release 12.2(33)SRC1.

Workaround: Reconfigure the static routes being affected, or simply configure **copy run start** to initialize the routes.
- CSCsu39864

Symptoms: If the startup configuration includes a boot host TFTP command that calls for a file that contains something other than interfaces, the PRE (the primary or the standby) crashes, and the remote configuration file does not make it to the active configuration.

Conditions: The symptom is observed when the startup configuration includes a boot host TFTP command that calls for a file that contains something other than interfaces. If the remote configuration file consists of only interfaces (no matter how many), everything works as expected. This problem is seen in both Cisco IOS Release 12.2(31)SB13 and Release 12.2(33)SB2.

Workaround: Do not have this option configured.

Further Problem Description: Stack degradation or a CPU hog message might also appear on the screen.
- CSCsu49066

Symptoms: In SSM when no receivers have joined yet and the source becomes active, a CPU spike on the RP will be seen.

Conditions: This symptom happens only when there are no receivers joined to receive the multicast traffic.

Workaround: Configuring “`mls rate-limit multicast ip fib-miss <>`” will help alleviate the problem and keep the CPU utilization on the RP down.

- CSCsu65189

Symptoms: If router is configured as follows:

```
router ospf 1
...
  passive-interface Loopback0
```

And later is enabled LDP/IGP synchronization using command:

```
Router(config)#router ospf 1
Router(config-router)# mpls ldp sync
Router(config-router)#^Z
```

MPLS LDP/IGP synchronization will be allowed on interface loopback too.

```
Router#sh ip ospf mpls ldp in
Loopback0
  Process ID 1, Area 0
  LDP is not configured through LDP autoconfig
  LDP-IGP Synchronization : Required < ---- NOK
  Holddown timer is not configured
  Interface is up
```

If the **clear ip ospf proc** command is entered, LDP will keep the interface down. Down interface is not included in the router LSA, therefore IP address configured on loopback is not propagated. If some application like BGP or LDP use the loopback IP address for the communication, application will go down too.

Conditions: Occurs when interface configured as passive. Note: all interface types configured as passive are affected, not only loopbacks.

Workaround: Do not configure passive loopback under OSPF. Problem only occurs during reconfiguration.

The problem will not occur if LDP/IGP sync is already in place and:

- router is reloaded with image with fix for CSCsk48227
- passive-interface command is removed/added

- CSCsv02117

Symptoms: The following system error message with “Out of IDs!” warning is seen with traceback:

```
%IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0)
```

Conditions: This symptom is observed when flapping 24K sessions over 12K tunnel once, recreating this issue.

Workaround: There is no workaround.

- CSCsv08352

Symptoms: Some static routes are not in the IP routing table state after a stateful switchover (SSO).

Conditions: This only occurs following a SSO event.

Workaround: Perform a **shutdown** followed by a **no shutdown** of interface if the route does not come up automatically.

- CSCsv90106

Symptoms: A router may write a crashinfo that lacks the normal command logs, crash traceback, crash context, or memory dumps.

Conditions: This might be seen in a memory corruption crash depending on precisely how the memory was corrupted.

Workaround: There is no workaround.

- CSCsw48209
 

Symptoms: A router may reload unexpectedly if the commands **no ipv6 unicast-routing** then **ipv6 unicast-routing** are issued several times within a short space of each other.

Conditions: The router must be running Cisco Express Forwarding for IPv6, and have multiple IPv6 VRFs configured.

Workaround: If issuing the command **no ipv6 unicast-routing**, wait several seconds before issuing **ipv6 unicast-routing**.
- CSCsx56362
 

Symptoms: BGP selects paths which are not the oldest paths for multipath. This causes BGP to unnecessarily flap from multipath to non-multipath as a result of route flaps.

Conditions: The symptom is observed when:

  1. BGP is configured.
  2. More than one equally-good route is available.
  3. BGP is configured to use less than the maximum available number of multipaths.

Workaround: There is no workaround.

Further Problem Description: The selection of non-oldest paths as multipaths is only problematic in releases which include CSCsk55120, because in such releases it causes changes with respect to whether paths are considered multipaths.
- CSCsx87562
 

Symptoms: The following error is seen following interface range configuration change:

```
%SYS-3-TIMERNEG: Cannot start timer (0XXXXXXXX) with negative offset (- YYYYYYYYYY).
-Process= "<interrupt level>", ipl= 2
```

Conditions: This symptom is seen with dual supervisors installed and affects these Cisco Catalyst 4000 releases: Cisco IOS Releases 12.2(52)SG/XO, 12.2(50)SG4/5/6/7, 12.2(53)SG/SG1/SG2. This bug applies to all hardware, not specific to Cisco Catalyst 4500 switches.

Workaround:

  1. Configure the interfaces one by one.
  2. Force a switchover "redundancy force-switchover". 3- Use Cisco IOS Release 12.2(50)SG3 until the fix code is released.

Resolution: Fix is available in Cisco IOS Release 12.2(54)SG, which is available to download on Cisco.com.
- CSCsy08264
 

Symptoms: MQC policy applied on ES+ interface may not work as expected. Occurs if too many unique bandwidth rates are configured and applied on same line card and on the interfaces belonging to same Network Processor.

Conditions: If more than 32 unique bandwidth rates are (defined in policy maps applied on same NP) configured, the policy map is accepted without error but may not work as intended.

Workaround: If multiple unique bandwidth rates are required, space the policy maps across interfaces based on different network processors.
- CSCsy42615
 

Symptoms: Entries for ABRs and ASBRs are missing from the OSPF route table. This results in inter-area and external routes being omitted from the Routing Information Base (RIB).

Conditions: The bug will only be seen when MPLS-TE tunnels are being used. Also, specifying non-default SPF timer values with **timers throttle spf** will increase the risk of hitting this bug.

Workaround: There is no workaround.

- CSCsy81519

Symptoms: ISG subnet session feature if used in an environment where subscribers are connected to ISG interface on Layer 2 cloud, that is, ISG is the default gateway for the subscribers yet ISG subscribers interface is in routed mode, then adjacency to these connected subscribers is removed as soon as a subnet session is created and next hop is installed for these subscribers as the logical network id computed using the framed subnet mask received from AAA server as access accept radius attribute.

Conditions: This condition will occur for subnet session feature in scenario where ISG interface is defined under routed mode; however subscribers are connected over layer-2 cloud to this ISG interface, that is, ISG is the default gateway for these subscribers.

Workaround: There is no workaround if the subnet session feature has to be deliberately used in scenario as defined under conditions above. However this problem will not occur if the subscribers are one hop or more away from ISG.

Further Problem Description: ISG subnet session feature is used to group a number of sessions together using IP framed netmask attribute. The ISG subnet session feature can be used if ISG interface is defined under routed mode.

For example IP addresses belonging to a client say 192.168.0.68/24, 192.168.0.69/24, 192.168.0.70/24 and 192.168.0.70/24 can be grouped together under one ISG session if at the time of session creation a IP framed netmask 255.255.255.252 is returned in the access accept message from AAA server. The subscribers are one or more hop away from ISG interface (10.10.10.1/24)

The IP Framed Netmask attribute is used to compute the range of IP addresses to be grouped together under one ISG session. In example above, if a session is initiated firstly by IP address 192.168.0.69/24; then using IP Framed Netmask the computed range of IP addresses to be grouped together will be 192.168.0.68 to 192.168.0.71.

Now in a scenario where ISG interface is defined under routed mode though the subscribers are connected directly over Layer 2 cloud to ISG interface and Subnet Session is required to be used as a feature; then the stated problem under section Symptom above will occur.

Using example above and applying to this problematic scenario - the IP addresses of client 192.168.0.68/24, 192.168.0.69/24, 192.168.0.70/24 and 192.168.0.70/24 have to be grouped together under one ISG session using Subnet Session feature by returning a IP Framed Netmask 255.255.255.252 under Access Accept from AAA server, however the ISG interface (192.168.0.1/24) in this scenario is the default gateway to these Client IP end points.

Now as soon as the session is created and authenticated and Subnet Session feature is installed the next hop for these IP range 192.168.0.68 to 192.168.0.71 computed using IP Framed Netmask value 255.255.255.252 would be 192.168.0.68/30 resulting in traffic destined to all the range of IP addresses grouped under Subnet Session forwarded to 192.168.0.68/30 instead of using ARP to reach the IP end points directly.

- CSCsy86078

Symptoms: Router crashes with memory corruption.

Conditions: This symptom is observed when BFD is configured

Workaround: There is no workaround.

- CSCsz05181

Symptoms: A router may reload unexpectedly.



Workaround: Reload the Standby card frequently.

- CSCsz61184

Symptoms: Including a new class that does packet marking on an output service-policy (which also does policing in class-default class) drops packets on the policer in class-default class.

Conditions: The symptom is observed on a Cisco 10008 router (PRE4-RP) that is running Cisco IOS Release 12.2(33)SB3.

Workaround: Remove and add again the policer in the class-default.

- CSCsz83570

Symptoms: SSH sessions disconnect during large data exchanges, such as large logs with pagers.

Conditions: The symptom is observed when large amounts of data are exchanged between both ends: client and server (that is, the client provides a large input to the server and the server has a large output to send to the client). The session gets hung momentarily and disconnects after the timeout period of 120 seconds.

Workaround: Use 3DES for encryption.

- CSCta03194

Symptoms: An IP packet gets corrupted in the disposition path of EoMPLS over ES+ cards when the VC is type 4.

Conditions: The symptom is observed with an ScEoMPLS pseudowire terminated on an ES+ card.

Workaround: There is no workaround.

- CSCta18596

Symptoms: The following tracebacks and messages appear on the console logs:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x61AB0C78 reading 0x22
%ALIGN-3-TRACE: -Traceback= 61AB0C78 623849E8 62384A58
607CCD8C 61372428 613769FC 61376E68 613773C4
```

In addition, you may see instability of the serial interfaces (that is, when an interface is configured, it stays up for a while and then goes down).

Conditions: The symptoms are observed when upgrading to Cisco IOS Release 12.2(31)SB14 on a Cisco 7200 series router only on the interfaces configured with frame-relay fragmentation configured on the main interface.

Workaround 1: Use fragmentation in the map-class with FRTS (that is, configure “frame-relay traffic-shaping” under the main interface and configure fragmentation under the map-class and apply the map-class to PVC). For example:

```
interface Serial11/0.1/1/4/2:0
  no ip address
  encapsulation frame-relay IETF
  ...
  frame-relay traffic-shaping
  frame-relay lmi-type ansi
  frame-relay intf-type dce
  no clns route-cache
  max-reserved-bandwidth 100
!
```

```

interface Serial1/0.1/1/4/2:0.101 point-to-point
    ...
    frame-relay interface-dlci 101
        class BANKOFIRE-S1/0.1/1/4/2:0.101-SR611638725

map-class frame-relay BANKOFIRE-S1/0.1/1/4/2:0.101-SR611638725
    frame-relay cir 768000
    frame-relay mincir 768000
    no frame-relay adaptive-shaping
    service-policy input BANKOFIRE-IN-S1/0.1/1/4/2:0
    service-policy output BANKOFIRE-OUT-S1/0.1/1/4/2:0
    frame-relay fragment 600
!
```

Workaround 2: Make sure that the fragmentation size is different in different interfaces (with interface fragmentation).

- CSCta38476
 

Symptoms: When removing the tunnel interface with CDP enabled, tracebacks are generated. CDP does not come up in all interfaces.

Conditions: The symptom is observed with large numbers of CDP neighbors in an MCP router.

Workaround: Disable CDP before deleting the tunnel interface.

Further Problem Description: CDP tries to send a packet over a deleted tunnel interface causing the issue.
- CSCta55561
 

Symptoms: Per-VRF dampening is not supported.

Conditions: The symptom is observed during normal code flow.

Workaround: There is no workaround.
- CSCta65610
 

Symptoms: When configuring an OSPF sham-link between two PEs also used for multicast VPN, RPF check for the source of a multicast stream points to the physical interface used by the sham-link instead of the tunnel.

Conditions: Configure two PEs to run MVPN and create a sham-link between them. Remote routes that are learned through the sham link will not have an MDT tunnel.

Workaround: There is no workaround. Prefixes must be learned through i-BGP.
- CSCtb41458
 

Symptoms: IPv6 multicast traffic is process-switched on IPv6 RBE.

Conditions: IPv6 Cisco Express Forwarding (CEF) is enabled, however IPv6 multicast traffic is process-switched on IPv6 RBE interface.

Workaround: There is no workaround.
- CSCtb57460
 

Symptoms: BGP scanner process is taking a lot of CPU.



Conditions: The symptom is observed with a five second BGP scanner timer and with a large number of routes. It is seen on a PRE2.

Workaround: Change to a pre-BGP LMM supported image.

- CSCtb75413

Symptoms: IGMP membership is lost for multiple groups on multiple interfaces. After a few minutes, membership is reestablished. Hosts are observing loss of multicast streams during the loss of membership.

Conditions: This issue will be seen only when the SSM mapping is enabled and when the DNS lookup for the SSM source mapping fails due to the unavailability of the DNS server.

Workaround: Disable the DNS lookup for the SSM mapping by the **no ip igmp ssm-map query dns** command.

If DNS is used, ensure that DNS servers are always reachable and also have low DNS query timeout value.

Further Problem Description: If SSM Static Mapping command is used and router processes SSM groups outside the configured Static SSM Mapping range, then routers falls to DNS based lookup to find SSM mapping. If DNS servers are not reachable or DNS servers not configured to provide mapping, input interface Q builds up leading to control plane instabilities affecting other protocols also.

- CSCtb85661

Symptoms: On doing multiple switchovers or after ISSU completion followed by a failover, the hardware programming of bidir entries does not show the correct dest\_index (0xFFFF) leading to a drop in traffic.

Conditions: This symptom only affects Cisco IOS Release 12.2(33)SRE. This issue may hit only in case of multiple failovers.

Workaround: The dest\_index can be set to the correct value using a test CLI, and traffic will resume.

- CSCtb86439

Symptoms: Slow memory leak occurs on Cisco Intelligent Services Gateway (ISG) during normal operations.

Conditions: Leak is observed if there is some error condition such as a mis-configuration in the user or service profile.

Workaround: There is no workaround.

- CSCtc05649

Symptoms: No SNMP trap is raised and there are missing paths in the output of the **show ip sla mpls-lsp-monitor lpd operational-state** command.

Conditions: The symptom is observed in an ECMP scenario, when “mpls ip” is removed from one interface out of all the interfaces supporting available paths between A and B. No LPD-group trap is raised when the path is discovered as broken.

Workaround: There is no workaround.

- CSCtc13344

Symptoms: Cisco Optimized Edge Routing (OER) experiences a fatal error and is disabled:

```
%OER_MC-0-EMERG: Fatal OER error <> Traceback %OER_MC-5-NOTICE: System Disabled
```

Conditions: This symptom is observed when configuring OER to learn the inside prefixes within a network by using the **inside bgp** command.

Workaround: Disable prefix learning by using the **no inside bgp** command.

- CSCtc15394

Symptoms: The parity errors are seen on a 4XOC3-ATM 1XOC3-ATM 1XOC12-ATM SPA while it is operational and plugged into SIP200 or SIP400 chassis with or without traffic running.

Conditions: No known conditions. Soft errors can happen any time due to environmental effects.

Workaround: There is no workaround.

- CSCtc24959

Symptoms: Occasionally you may experience a multicast traffic loss in dual path linecards.

Conditions: The symptom is observed in dual path line cards. Occasionally, met2 programming will go out of sync between two data paths.

Workaround: Any change that triggers reprogramming that entry will help. Changing replication mode to ingress is a workaround.

- CSCtc36072

Symptoms: The following error message accompanied with a traceback might be seen on a BRAS that is configured for PPPoEoA:

```
%C10K_QOS_GENERAL-3-EREVENT: Error @ Policy count exceeds max supported policymaps: ()
line:805306368
```

Conditions: The symptom is observed when the PPPoE sessions were cleared either locally or remotely.

Workaround: There is no workaround.

Further Problem Description: The issue was seen with Cisco IOS Release 12.2(34)SB4a but it might affect other software as well.

- CSCtc39809

Symptoms: Memory leak is seen at EIGRP component.

Conditions: The symptom is observed when EIGRP encounters an SIA condition.

Workaround: There is no workaround.

- CSCtc50985

Symptoms: Output of the **show ip subscriber dangling 500** at a steady state shows lots of sessions of the form:

```
dhcp          0000.6401.2a64          [37649]          control  waiting
```

Conditions: The symptom is observed in large scale scenarios or when CPS is much higher than recommended.

Workaround: Clear the session on the router and reboot, if required.

Further Problem Description: In scale scenarios, the DHCP handshakes between the client, so the DHCP relay and server might take a long time. Also, the wire or DHCP server is loaded so that it drops some offers or ACKs. In this case, some sessions might be seen dangling without corresponding binding and there is no connectivity to the user.

- CSCtc51539

Symptoms: A Cisco router crashes with a “Watch Dog Timeout NMI” error message.

Conditions: This symptom is observed only on devices configured with Bidirectional Forwarding Detection (BFD). For further information on BFD, consult the following link:

[http://www.cisco.com/en/US/docs/ios/12\\_0s/feature/guide/fs\\_bfd.html](http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html)

- Workaround: Disable BFD.
- CSCtc57044
 

Symptoms: The **mpls propagate-cos** command may not function correctly on a Cisco 7600 router.

Conditions: This was observed on several Cisco 7600s running Cisco IOS Release 12.2(33)SRC.

Workaround: Remove and reapply the **mpls propagate-cos** command.
  - CSCtc60463
 

Symptoms: The **traceroute mac src\_mac dst\_mac** command can cause a software crash on a Cisco 7600 router when configured with a large number of VLANs.

Conditions: This occurs on a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRC4.

Workaround: Do not use the **traceroute mac src\_mac dst\_mac** command. Use a specific VLAN ID when using this command.
  - CSCtc74804
 

Symptoms: Two ARP entries for the same MAC are seen on the intelligent service gateway (ISG) acting as a relay.

Conditions: This symptom occurs when there are multiple DHCP servers there in the deployment, and a delayed offer comes from one of the DHCP servers to DHCP relay (ISG).

Workaround: Use only a single DHCP server.
  - CSCtc75687
 

Symptoms: Some commands with large outputs allow the use of ctrl-^ to stop the output before completion. This can cause a crash.

Conditions: Unknown at this time.

Workaround: Enter the **no parser command serializer** command.
  - CSCtc90579
 

Symptoms: Router crashes due to memory corruption during MPLS TE auto backup tunnel deletion.

Conditions: Caused by topology changes triggering backup tunnel deletion and RSVP hello mechanism.

Workaround: Globally, disable RSVP hello and enable BFD hello:

```
Router(config)#no ip rsvp signalling hello
Router(config)#ip rsvp signalling hello bfd
```

Per MPLS TE enabled interface:

```
Router(config-if)#no ip rsvp signalling hello
Router(config-if)#ip rsvp signalling hello bfd
```
  - CSCtc90779
 

Symptoms: A router may crash after displaying align fatal errors pointing to PPPoE functions.

Conditions: The symptom is observed on a Cisco 7206VXR router (NPE-G1) that is running Cisco IOS Release 12.2(31)SB15.

Workaround: There is no workaround.

- CSCtd00070

Symptoms: If “arp ignore local” is configured under “ip subscriber l2-connected” submode on an interface, ISG will no longer reply to ARPs coming to that interface if the ARPs’ destination IPs are in the same subnet as the ARP source’s IP, or if the ARPs’ destination IP is not in the subnet of ISG but is routable from the interface where the ARP is received.

Conditions: The symptom is observed if “arp ignore local” is configured under “ip subscriber l2-connected” submode.

Workaround: There is no workaround.

Further Problem Description: If this session is in VRF mapping or transfer mode, and the CPE’s ARP is for an IP on the access interface that happens to be reachable in the VRF by ISG (e.g.: due to VRF IP spaces overlapping or VRF’s default route is set to matching all traffics), the ARP request will receive a reply, even with the above configuration, unless the destination IP is in the same VRF subnet as the VRF’s MSI. Note that when the CPE receives ISG’s ARP reply in this case and routes the corresponding IP packets to ISG, ISG will route the packet in the VRF space.

- CSCtd06275

Symptoms: When issuing the **show policy-map interface brief** command, the system might crash with a bus-error.

Conditions: The symptom is observed when the system is configured for ISG-services in a scaled ATM-environment.

Workaround: There is no workaround.

- CSCtd08797

Symptoms: MPLS packets are software switched when port-channel interfaces are the MPLS interfaces. Affects tag-to-tag traffic.

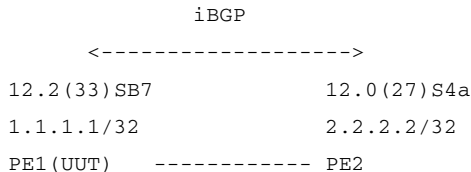
Conditions: Issue is seen after the router is upgraded to Cisco IOS Release 12.2(33)SRD3. The MTU for the MLS CEF adjacency for the MPLS label is misprogrammed and shows up as 0. Should see “MTU failures” incrementing in **show mls stat**.

Workaround: Flap the interface.

- CSCtd15853

Symptoms: When removing VRF configuration on remote PE, local PE receives withdraw message from remote PE to purge its MDT entry. However, local PE does not delete the MDT entry.

/// Topology ///



PE1 receives MDT entry from PE1 and PE2.

Please focus a entry of “2.2.2.2/32” from PE2.

PE-1  
---

```

PE1-PRE2#
PE1-PRE2#sh ip bgp ipv4 mdt all
BGP table version is 13, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf V1)
*> 1.1.1.1/32          0.0.0.0                                0 ?
*>i2.2.2.2/32          2.2.2.2              0   100      0 ? <<<---- HERE
*>i3.3.3.3/32          3.3.3.3              0   100      0 ?
---
```

To trigger the issue, vrf configuration is remove on PE2. You can see that PE2 sends withdraw message to PE1(1.1.1.1).

```

PE-2
---
PE2-PRE1#
PE2-PRE1#
PE2-PRE1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
PE2-PRE1(config)#
PE2-PRE1(config)#no ip vrf V1
Tunnel interface was deleted. Partial configuration may reappear on reuse.
% IP addresses from all interfaces in VRF V1 have been removed
PE2-PRE1(config)#
PE2-PRE1(config)#
*Nov  9 12:29:35.447: %LINK-5-CHANGED: Interface Tunnel3, changed state to
administratively down
*Nov  9 12:29:36.467: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel3,
changed state to down
PE2-PRE1(config)#
PE2-PRE1(config)#end
PE2-PRE1#
PE2-PRE1#
*Nov  9 12:30:05.435: BGP(2): nettable_walker 2:1:1:2.2.2.2/32 no best path
*Nov  9 12:30:05.435: BGP(2): 1.1.1.1 send unreachable 2:1:1:2.2.2.2/32
*Nov  9 12:30:05.435: BGP(2): 1.1.1.1 send UPDATE 2:1:1:2.2.2.2/32 --
unreachable <<--- HERE
*Nov  9 12:30:05.435: BGP(2): updgrp 1 - 1.1.1.1 enqueued 1 updates,
average/maximum size (bytes) 45/45
PE2-PRE1#
PE2-PRE1#
PE2-PRE1#sh ip vrf
```

PE2-PRE1#

---

The MDT entry(2.2.2.2/32) is not deleted even if PE1 indeed receives withdraw message from PE2. "clear ip bgp \*" would be needed to purge the MDT entry.

PE-1

---

PE1-PRE2#

\*Nov 9 12:29:34.323: BGP:from:3 to:4 update format 1:1:3.3.3.3/0 MDT grp  
239.0.0.1 pfxptr->masklen 96

\*Nov 9 12:29:34.323: BGP:from:3 to:4 update format 1:1:1.1.1.1/0 MDT grp  
239.0.0.1 pfxptr->masklen 96

\*Nov 9 12:29:34.323: BGP(4): 2.2.2.2 send UPDATE (format) 2:1:1:1.1.1.1/32,  
next 1.1.1.1, label 0, metric 0, path Local

\*Nov 9 12:29:34.323: BGP:from:3 to:4 update format 1:1:2.2.2.2/0 MDT grp  
239.0.0.1 pfxptr->masklen 96

\*Nov 9 12:29:34.323: BGP(4): updgrp 1 - 2.2.2.2 updates replicated for neighbors:

\*Nov 9 12:30:05.799: BGP(4): 2.2.2.2 rcv UPDATE about 1:1:2.2.2.2/64 --  
withdrawn, label 3 <---- HERE

\*Nov 9 12:30:05.799: BGP: 2.2.2.2 Modifying prefix 1:1:2.2.2.2/64 from 4 -> 3  
address

PE1-PRE2#

PE1-PRE2#sh ip bgp ipv4 mdt all

BGP table version is 13, local router ID is 1.1.1.1

Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,  
r RIB-failure, S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 1:1 (default for vrf V1)					
*> 1.1.1.1/32	0.0.0.0			0	?
*>i2.2.2.2/32	2.2.2.2	0	100	0	? <---- HERE
*>i3.3.3.3/32	3.3.3.3	0	100	0	?

PE1-PRE2#

PE1-PRE2#

PE1-PRE2#clear ip bgp \*

PE1-PRE2#

\*Nov 9 12:31:22.043: %BGP-5-ADJCHANGE: neighbor 2.2.2.2 Down User reset

\*Nov 9 12:31:22.043: %BGP\_SESSION-5-ADJCHANGE: neighbor 2.2.2.2 VPNv4 Unicast  
topology base removed from session User reset

\*Nov 9 12:31:22.043: %BGP\_SESSION-5-ADJCHANGE: neighbor 2.2.2.2 IPv4 MDT  
topology base removed from session User reset

\*Nov 9 12:31:22.043: %BGP-5-ADJCHANGE: neighbor 3.3.3.3 Down User reset

\*Nov 9 12:31:22.043: %BGP\_SESSION-5-ADJCHANGE: neighbor 3.3.3.3 VPNv4 Unicast  
topology base removed from session User reset

```

*Nov  9 12:31:22.043: %BGP_SESSION-5-ADJCHANGE: neighbor 3.3.3.3 IPv4 MDT
topology base removed from session User reset
*Nov  9 12:31:22.555: %BGP-5-ADJCHANGE: neighbor 3.3.3.3 Up
*Nov  9 12:31:22.563: BGP(3): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 3.3.3.3,
origin ?, localpref 100, metric 0
*Nov  9 12:31:22.563: BGP(3): 3.3.3.3 rcvd 1:1:3.3.3.3/32
PE1-PRE2#
PE1-PRE2#
PE1-PRE2#sh ip bgp ipv4 mdt all
BGP table version is 1, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

```

```

      Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf V1)
*  i3.3.3.3/32        3.3.3.3                0      100      0 ?
---
```

Conditions:

- mVPN is configured on PE router.
- Both Pre-MDT SAFI and MDT-SAFI IOS are running in a Multicast Domain.

For detailed information, see the following MDTSAFI document:

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod\\_white\\_paper0900aecd80581f3d.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html)

Workaround: There is no workaround.

- CSCtd25133

Symptoms: Router gets into APS channel mismatch state.

Conditions: Observed with MGX connected as APS peer, when both MGX cards (active and standby) are reloaded simultaneously.

Workaround: Force APS switchover.

- CSCtd25933

Symptoms: Active or standby RP crashes on executing the **shut** then **no shut** commands on the interface.

Conditions: The symptom is observed with the following conditions:

1. Encapsulation QnQ (or dot1q) is configured and removed on the subinterface, on a WAN interface (SIP400).
2. Same VLAN configured as Encapsulation QnQ (or dot1q) on a LAN interface (ES+).
3. Perform shut/no shut on the ES+ interface.

Workaround: There is no workaround.

- CSCtd28348

Symptoms: On an ESR PRE3 throughput may be reduced down to 80% of expected throughput for high speed VBR-NRT VCs.

Conditions: The symptom is seen under the following conditions:

- Seen on VCs with speed more than 240MB.
- The higher the rate of the PVC the higher the impact (the lower the percentage throughput/expected throughput).
- The lower the MBS the higher the impact (the lower the percentage throughput/ expected throughput).
- Default MBS seems fine for 300 MB PVCs but may not be for faster VCs.
- MBS=1 hits the issue for PVCs with speed of 240MB.

Workaround: Do not set the MBS explicitly.

- CSCtd33567

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323>.

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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

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](http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html)

- CSCtd33642

Symptoms: Flow/Service Accounting records are missing if “delay-start” is configured.

Conditions: The symptom is observed if “aaa delay-start” is configured.

Workaround: Removing the “delay-start” configuration will result in accounting records generating.

- CSCtd38225

Symptoms: When ISG is enabled and DHCP sessions re-start just around the time their leases expire, some sessions may get stuck dangling indefinitely. Sending DHCPDISCOVER message (that is, restarting the CPE) will not restore the session. The affected subscriber(s) will not be able to establish a session.

Conditions: The issue seems to be a corner-case situation. It is observed when ISG is enabled and DHCP sessions re-start just around the time their leases expire.

Workaround: The only known workaround is to manually clear the dangling session(s) using the **clear ip subscriber dangling time** command although this may not be a suitable workaround in a live production network.



- CSCtd42928

Symptoms: An IP DHCP ISG subscriber session is not being created for a particular subscriber. Other subscribers are not affected.

Conditions: The symptom is observed under the following conditions:

1. Scale scenario (less than 20k sessions).
2. Using debugs and show commands it is determined that no session or binding exists for the subscriber, but a DPM context exists.

Workaround: There is no workaround.

Further Problem Description: In such conditions the only way to start the session for the subscriber is a reload or switchover.

- CSCtd49801

Symptoms: The “ip sla reaction” configuration resets after restarting the Collector.

Conditions: The symptom is observed with the following conditions:

1. A Collector is created for specific device with an Echo operation.
2. The Collector is stopped and the device is configured follows:
 

```
ip sla reaction-configuration 167086 react timeout threshold-type xOfy 2 3
action-type trapOnly
```
3. The Collector is stopped again and the configuration is unexpectedly modified as follows:
 

```
ip sla reaction-configuration 167086 react timeout threshold-type immediate
action-type trapOnly
```

 (The threshold-type has modified from “xOfy 2 3” to “immediate”.)

4. It is seen with IPM 4.2.

Workaround: There is no workaround.

- CSCtd54338

Symptoms: The following output from the command **show ip rtp header-compression**, shows that one channelized serial interface has a large accumulated number of “seconds since line card sent last stats update” compared with another channelized serial interfaces in device with the same platform:

```
GR_SA_CORE_7613R_1#show ip rtp header-compression Serial1/2/0.1/3/1:0
RTP/UDP/IP header compression statistics:
Interface Serial1/2/0.1/3/1:0 (compression on, Cisco)
Distributed fast switched:
10364 seconds since line card sent last stats update
Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
         0 dropped, 0 buffer copies, 0 buffer failures
Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
         0 bytes saved, 0 bytes sent
Connect: 16 rx slots, 16 tx slots,
         0 misses, 0 collisions, 0 negative cache hits, 0 free contexts
```

Sometimes there is also a one-way call signaling problem.

Conditions: The symptom is observed with the following conditions:

- Cisco IOS Release 12.2(33)SRD3.

- Platform: Cisco 7613 router.
- RP: RSP720-3CXL-GE.
- SIP: Cisco 7600 SIP-200.
- SPA: SPA-1XCHSTM1/OC3.

This issue normally begins to show when the count of the channelized subinterface (number of cRTP sessions) is 200 or over.

Workaround: Disable then enable RTP header-compression on the interface.

Further Problem Description: The issue can be resolved by using **disable cRTP** and **enable cRTP** on each subinterface (see DDTs CSCso48621). However, sometimes the problem can reoccur in a few days after recovery on the same subinterface.

- CSCtd66014

Symptoms: ES+ line card crashes at powerup of a Cisco 7600 router that is running Cisco IOS Release 12.2SRE if either the Traffic Manager or Frame memories in the ES+ Network processors report a double bit ECC error. The ES+ line card crashinfo will have the following string:

```
%NP_DEV-DFC2-3-ECC_DOUBLE: Double-bit ECC error detected on NP 0, Mem 19, SubMem 0x1, SingleErr 1, DoubleErr 1 Count 1 Total 1
```

Conditions: Router reloads, OIR of ES+ cards, system environment temperatures that slowly vary around an ambient temperature of about 30 degreesC. This happens at system powerup. We have seen double bit ECC problems reported after a few hours of traffic if the ambient temperatures vary around 30 degreesC.

Workaround: No configuration workaround is available. The line card will reset itself and will be operational in the second reload.

- CSCtd67010

Symptoms: A Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD3 may crash in process "Ethernet OAM".

Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD3. It is not necessary to have Ethernet OAM configured.

Workaround: There is no workaround.

- CSCtd67076

Symptoms: Standby PRE resets due to parser sync error.

Conditions: The symptom is seen when a non-existing GigE interface is deleted.

Workaround: Configure the following:

```
(config-red)# no policy config-sync lbl prc reload
(config-red)# no policy config-sync bulk prc reload
```

- CSCtd71372

Symptoms: DHCP-initiated IP sessions sometimes get into a dangling state, either in data plane or control plane. This leads to lost connectivity for the end users who have the sessions dangling.

Conditions: The symptoms are due to some not yet identified race conditions in DPM/DHCP.

Workaround: There is no workaround.

- CSCtd72426

Symptoms: Checkpointing facility on the standby SP is leaking memory buffers. This can lead to a WATERMARK error message.

Conditions: The symptom is observed with the checkpointing facility on the standby SP.

Workaround: There is no workaround.

Further Problem Description: This issue can be checked with the command **show ipc session all verbose** from the standby SP. This output will show more messages requested than messages returned for the client “CHKPT:STANDBY SP” and this difference will grow every day. The **show check client** command from the standby SP will show the buffers held for “REP CHKPT CLIENT” and that this value is increasing over time.

- CSCtd72462

Symptoms: A Cisco 7600 series router with an RSP720-3C processor may unexpectedly reboot after the **show policy-map interface** command is executed.

Conditions: The issue is seen when there is a policy map on an interface with the following:

- No set action.
- No shared aggregate policer action.
- No aggregate policer action.
- uflow policer with “conform action” configured.

Workaround: There is no workaround.

- CSCtd74135

Symptoms: Microsoft Point-to-Point Encryption (MPPE) enforcement may not work on a Cisco router. The router may allow Point-to-Point Tunneling Protocol (PPTP) users to connect without negotiating the MPPE.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 15.0(1)M even if it is configured with the **ppp encrypt mppe 128 required** command.

Workaround: Using the authentication type of MS-CHAP in place of MS-CHAP-V2 can prevent this issue. The MPPE works fine with the “required” option as well, when used with the authentication type “MS-CHAP”.

- CSCtd75033

Symptoms: Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability.



**Note** The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section “Further Description” of this release note enclosure.

Conditions: Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

This is the same as the vulnerability which is described in <http://www.kb.cert.org/vuls/id/568372>.

Cisco has released a public facing vulnerability alert at the following link:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=19540>

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client
```

The following example identifies a Cisco device that is configured with NTP:

```
router#show running-config | include ntp
      ntp peer 192.168.0.12
```

The following example identifies a Cisco device that is not configured with NTP:

```
router#show running-config | include ntp
router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to “Cisco Internetwork Operating System Software” or “Cisco IOS Software.” The image name displays in parentheses, followed by “Version” and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

The following example shows a product that is running Cisco IOS Software Release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

<output truncated>

Additional information about Cisco IOS Software release naming conventions is available in “White Paper: Cisco IOS and NX-OS Software Reference Guide” at the following link:

<http://www.cisco.com/web/about/security/intelligence/ios-ref.html>

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.




---

**Note** NTP peer authentication is not a workaround and is still a vulnerable configuration.

---

#### \* NTP Access Group

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
!--- Configure trusted peers for allowed access

access-list 1 permit 171.70.173.55

!--- Apply ACE to the NTP configuration

ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled “Performing Basic System Management” at the following link:

[http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm\\_basic\\_sys\\_manage.html#wp1034942](http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942)

#### \* Infrastructure Access Control Lists

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
```

```
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Note: If the router is acting as a NTP broadcast client
!--- via the interface command "ntp broadcast client"
!--- then broadcast and directed broadcasts must be
!--- filtered as well. The following example covers
!--- an infrastructure address space of 192.168.0.X

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 255.255.255.255 eq ntp

!--- Note: If the router is acting as a NTP multicast client
!--- via the interface command "ntp multicast client"
!--- then multicast IP packets to the multicast group must
!--- be filtered as well. The following example covers
!--- a NTP multicast group of 239.0.0.1 (Default is
!--- 224.0.1.1)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 239.0.0.1 eq ntp

!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.

access-list 150 deny udp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.

access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example
!--- shown)

interface fastEthernet 2/0
    ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link:

[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_white\\_paper09186a00801a1a55.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml)

#### \* Control Plane Policing

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, while the second looks at rate limiting NTP traffic to the box.

- Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS Software Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```

!--- Feature: Network Time Protocol (NTP)

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 123

!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.

access-list 150 permit udp any any eq 123

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-udp-class
    match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic

```

```

class drop-udp-class
  drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
  service-policy input drop-udp-traffic

```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function.

- Rate Limiting the traffic to the device.

The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning: If the rate-limits are exceeded, valid NTP traffic may also be dropped.

```

!--- Feature: Network Time Protocol (NTP)

access-list 150 permit udp any any eq 123

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all rate-udp-class
  match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp\_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates

policy-map rate-udp-traffic
  class rate-udp-class
    police 10000 1500 1500 conform-action transmit
      exceed-action drop violate-action drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
  service-policy input drop-udp-traffic

```



Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S—Control Plane Policing” at the following links:

[http://www.cisco.com/web/about/security/intelligence/coppwp\\_gs.html](http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html) and  
[http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t4/feature/guide/gtrtlimt.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html)

Further Description: Cisco IOS Software releases that have the fix for this Cisco bug ID, have a behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message: Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command **ntp allow mode private** should be configured. This is disabled by default.

- CSCtd75248

Symptoms: With QoS is disabled globally and when the ES20 interface is configured as a trunk, if traffic is sent with a valid COS value, the ES20 re-marks all COS values to “0”.

Conditions: The symptom is observed when QoS is globally disabled.

Workaround: Enable QoS globally using **mls qos** and trust the ES20 trunk interface to retain CoS values using **mls qos trust cos**.

Further Problem Description: This issue is not seen in Cisco IOS Release 12.2(33)SRB. It is present in Cisco IOS Release 12.2(33)SRC onwards

- CSCtd77905

Symptoms: Traffic will not flow properly for the first VRF, if there is a switchover from active to standby. This issue occurs because of a race condition.

Conditions: The symptom is observed only in the HA setup.

Workaround: Delete and reconfigure the problematic VRF.

Further Problem Description: The problem is a timing issue. In the standby Supervisor, the aggregate labels are not getting programmed properly for the first VRF configured in the system.

- CSCtd87264

Symptoms: DHCP unicast BootP offers can not be propagated back in the incoming interface as the ARP entry is missing. This happens only when the relay function is combined in a VRF and the incoming interface is unnumbered.

Conditions: The symptom is observed when SRD/SRE Cisco 7600 series router is a DHCP relay/snooping agent. The request must come in a VRF.

Workaround: Move the relay agent function to the global routing table.

- CSCtd99802

Symptoms: There is packet loss due to the BGP session reopening from the peer that has been rejected.

Conditions: The symptom is observed when a Cisco peer has a BGP session and a non-Cisco peer does not (because of reloading the non-Cisco peer line card or a similar reason). The non-Cisco peer does not send TCP RST properly to close the BGP session on the Cisco peer.

Workaround: There is no workaround.

- CSCtd99916

Symptoms: After a quick activation/deactivation of a BGP neighbor in the VPNv4 address family, the router can have a unexpected reload. Traceback shows:

```
1#9ef25813351d0da79497b4305144eadc :10000000+5A9860 :10000000+5A9BE4
:10000000+10B9CA0 :10000000+10BEF34 :10000000+421761C :10000000+2AD6FC
:10000000+2ADA28 :10000000+2FA91C :10000000+2FAF84 :10000000+2E748C
```

```
Exception to IOS Thread:
Frame pointer 35233FD8, PC = 1027203C
```

```
ASR1000-EXT-SIGNAL: U_SIGSEGV(11), Process = BGP Router
-Traceback= 1#9ef25813351d0da79497b4305144eadc :10000000+27203C
:10000000+271DAC :10000000+273218 :10000000+2741B8 :10000000+33AE64
:10000000+33B5C4 :10000000+291D2C :10000000+2921C8 :10000000+2928AC
```

Conditions: The symptom is observed whenever an old style multicast update is received and it uses the same AF value as that for VPNv4. Cisco IOS Release 12.2(33)XNE has code that detects this behavior, hence the traceback.

Workaround: Use new-style MDT peering.

- CSCte02089

Symptoms: IP DSCP is rewritten to 0 after disposition on PE.

Conditions: This symptom occurs when unconfiguring and adding a VRF back for packets exiting out of an interface having ip vrf receive configured.

Workaround: There is no workaround.

- CSCte02973

Symptoms: Routing protocols like EIGRP may be dropped in the global table.

Conditions: The symptom is observed when multicast is configured for a VRF and no multicast is configured for the global table.

Workaround: Enable “ip multicast routing” and create a loopback interface with “ip pim sparse-mode” enabled.

Further Problem Description: The problem should not occur for MVPN since this is not a valid configuration, as multicast in the core is a requirement.

However, it can occur for a feature called MVPN-lite, where multicast traffic is routed between VRF tables without the tunneling and therefore without the requirement for multicast in the global table.

- CSCte04701

Symptoms: PRE2 crashes.

Conditions: The symptom is observed on a PRE2 with Netflow configured.

Workaround: There is no workaround.

- CSCte05357

Symptoms: Router crashes.

Conditions: The symptom is observed when you configure per-VRF AAA based on templates configuration and ISG policy for PPPoE clients.

Workaround: Do not use template. Use “if-config” or another mechanism.

- CSCte06443

Symptoms: The IPv6 configuration shows incorrectly in running configuration. Additionally, the configuration may disappear after a reload:

```

7200-7(config)#int lo 0
7200-7(config-if)#ipv6 address 2001:0dB8:FFFF::2/128 ----> configured address
7200-7(config)#^Z
7200-7#sh run int lo 0
interface Loopback0
 ip address 10.195.95.2 255.255.255.255
 ipv6 address /1698840608 -----> displayed address
end

```

After a reload, it becomes like this:

```

7200-7#sh run int lo 0
 interface Loopback0
 ip address 10.195.95.2 255.255.255.255

```

Conditions: The symptom is observed only with an “spservice” image of a Cisco IOS SRE Release.

Workaround: There is no workaround.

- CSCte10706

Symptoms: When you configure FRF.12 “frame-relay fragment 512 end-to-end” on the serial interface, the router crashes.

Conditions: The symptom is observed when you configure FRF.12 “frame-relay fragment 512 end-to-end” on a CJ-PA.

Workaround: There is no workaround.

- CSCte38855

Symptoms: Chunk leak is seen after exec-timeout expires.

Conditions: The symptom is observed after the **interface range** command is configured and when the console timeout expires.

Workaround: There is no workaround.

- CSCte48656

Symptoms: The router crashes at “Illegal access to a low address”.

Conditions: The symptom is observed while stopping the SSS handling timer. This condition is triggered by an ISG PBHK configuration and when existing translations are inactive.

Workaround: There is no workaround.

- CSCte49283

Symptoms: Sometimes the LNS router sends an incorrect NAS-Port value.

Conditions: The symptom is observed when the LNS router sends a stop accounting-request to the RADIUS server.

Workaround: There is no workaround.

- CSCte56594

Symptoms: Seeing two dips of traffic drop after SSO, the first dip is about 80 milliseconds, the second traffic dip up to about 30 seconds.

Conditions: This symptom is observed on the PE (Cisco 7609-S) that is configured with OSPF NSF and both MPLS and RSVP GR. Also 4K vlans, 20K virtual circuit is configured peering with another 5 PEs on the VPLS domain. Generate 60M unidirectional traffic across this VPLS domain, then execute redundancy switchover via CLI.

Workaround: There is no workaround.

- CSCte58686

Symptoms: Link flaps after an upgrade to Cisco IOS Release 12.2(33)SRD3.

Conditions: The symptom is observed following an upgrade from Cisco IOS Release 12.2(33)SRB5 to SRD3.

Workaround: There is no workaround.

- CSCte58749

Symptoms: Some interfaces start flapping upon upgrading to Cisco IOS Release 12.2(33)SRD3.

Conditions: This is a corner case condition. The interface flaps occur under following conditions:

1. The peer connected on the other side of the interface sends a CODEREJ for a valid ECHOREP sent by a Cisco router.
2. On receiving CODEREJ for ECHOREP, the router terminates the PPP session. The PPP sessions restart, and the interface flaps.

Workaround: Disable keep-alive on the misbehaving peer router.

- CSCte60000

Symptoms: Destination prefix is not collected for IP to MPLS packet flow in netflow aggregation cache.

Conditions: The symptom is observed in a VRF + MPLS setup.

Workaround: Collect prefix in non-VRF + MPLS setup.

- CSCte66219

Symptoms: The following symptoms are observed:

1. When copying files from the active to standby (or vice versa), you may see an error:  

```
%Error writing stby-disk0: (TF I/O failed in data-in phase)
```
2. A failed MD5 checksum when reading a file off the disk. This may or may not indicate a previous failure that went unnoticed. (Note: not all disk errors and not all MD5 checksum errors are due to this problem.)
3. The disappearance of Smart Modular 128MB PCMCIA cards, typically on the standby PRE.

Conditions: The issue may be seen with Cisco IOS Release 12.2(33)SB. In particular, this card is susceptible: STI 7.4.0 Compact Flash and PCMCIA Flash cards. Other cards may or may not have the same issue, but empirical data indicates that other cards are at least somewhat less susceptible.

Workaround 1: Once a file is successfully copied to the disk and the MD5 checksum matches the file, that file is fine and not subject to corruption. Cards that are not being written do not spontaneously become damaged. That is, once the file is on the flash disk, it will not become defective. Only cards with actual errors should be RMAed. There is no need to preemptively or proactively replace flash cards.

Workaround 2: The disappearance of the Smart Modular 128MB PCMCIA cards can be resolved by the physical removal and re-insertion of the card or by reloading the PRE.

Further Problem Description: There was a recent change in the Cisco IOS DOS compatible file system. That change resulted in a higher performance file system. But there is a condition which has been seen on at least one variant of flash card that can lead to disk errors and file system damage. This condition arises from a gray area of the ATA specification and can be fixed in software.

- CSCte68259

Symptoms: Random end-to-end traffic failure with an ES+ line card with L2TPv3 termination on one port which is interfacing with EVC BD remotely.

Conditions: This issue occurs when the ES+ line card is configured with the L2TPv3 feature.

Workaround: There is no workaround.

- CSCte72128

Symptoms: After a reload, “cdp enable” is missing on prior configured interfaces.

Conditions: The symptom is observed with the following conditions:

- Before the reload, “cdp enable” is configured on some interfaces and after the reload the running-configuration shows missing “cdp enable” on those interfaces.
- It is seen on all kinds of interfaces.
- It is seen with Cisco IOS Release XNE1 (but not with Cisco IOS XNE Releases).

Workaround: Add it manually after a reload.

Further Problem Description: Because of the nature of the problem, upgrading to the releases where this fix is available does not restore the CDP configuration which was present before the upgrade. After the upgrade CDP needs to be reconfigured.

- CSCte74705

Symptoms: A Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRD may generate L2 Queue Error (%L2-SP-4-QUEER) messages when a link down/up event occurs across multiple interfaces in a short period of time.

Conditions: This symptom may occur when a large number of attachment circuits are configured with EVC style configuration, and a large number of MAC addresses are known to the system.

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”.

- CSCte78165

Symptoms: Device may reload when the **show ip protocol** command is issued.

Conditions: The symptom is observed when routing protocol is configured and the ISIS routes are being redistributed.

Workaround: Do not use the **show ip protocol** command.

- CSCte79112

Symptoms: When swapping to ISG, the final Access-Accept received from the AAA server triggers an authentication that fails at the Access-Point. ISG is not transparent to EAP authentication.

Conditions: This symptom is seen when migrating from SSG to ISG. ISG is proxy radius.

Workaround: There is no workaround.

- CSCte82917

Symptoms: On a Cisco 7600 series RSP720, the **show proc cpu sort** command displays a CPU utilization of 0, but the per-process CPU utilization is 100% for some processes; no packet loss occurs, however.

Conditions: This symptom is observed under the following conditions:

- The router has recently loaded
- HSRP is enabled in an HA environment
- A large number of HSRP sessions are established.

Workaround: Reduce the number of HSRP sessions to only a few. The router does not see any performance or functional impact. This is an issue only with internal CPU accounting.

- CSCte83888

Symptoms: If PoD request contains target Acct-Session-Id prepended with NAS- Port-ID, it will not be honored.

Conditions: This symptom occurs when PoD is prepended with NAS-Port-Id for target session.

Workaround: Use only the Session-Id which is located after the “\_” in the Account-Session-ID to specify the session needing disconnect.

- CSCtf00132

Symptoms: A Cisco 7200 series router crashes when there are unauthenticated sessions in a multichassis SGBP environment.

Conditions: The symptom is observed when multiple unauthenticated sessions in a multichassis multilink PPP SGBP environment are dialed from the same client on multiple home gateways as part of the same session.

Workaround: There is no workaround.

- CSCtf00234

Symptoms: With Cisco IOS Release 12.2(33)SB8, PPPoE users are rejected, with the following error message:

```
PPPOE: Max Inner Vlan session count(1) exceeded on TenGigabitEthernet5/0/0.xxx
```

Conditions: The symptom is likely to be seen when you encounter an error during PADR processing which can be triggered due to low memory on the router or a wrong PADR from peer. In this case, some sessions are not freed properly leading to ghost sessions, so the new session are rejected if BBA group is configured with some sort of session limit (for example “sessions per-vlan limit 65530 inner 1”).

Workaround: There is no workaround.

- CSCtf02916

Symptoms: IPv6 multicast traffic is not replicated properly after a shut/no shut.

Conditions: The symptom is observed when you do a **shutdown** followed by a **no shutdown** to a port downstream.

Workaround: Set replication mode ingress.

- CSCtf06442

Symptoms: The newly active supervisor on a Cisco 7600 router with SSC-400 may crash shortly after SSO failover due to a large amount of traffic causing system instabilities.

Conditions: This behavior is seen on a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRC5.

Workaround: Configure MLS rate limiters to prevent RP from being overwhelmed, which may prevent the router from crashing.

- CSCtf06486

Symptoms: SSO failover may be delayed by approximately 10 seconds when SSC- 400 is present in chassis.

SSC-400 is not SSO aware. However other line cards may be affected by this.

Conditions: The following error message can be seen:

```
oir_enable_switching_for_modules_replied: Slot: 7 (nonEMS20g) took > 10000 ms extra to reply
```

Workaround: There is no workaround.

- CSCtf12072

Symptoms: The expected behavior after a failed authorization action does not get applied onto the session when authorization is based on option 82 information. The FSOL does not contain option 82 information.

Conditions: The symptom is observed when the ISG policy is to provide authorization based on the subscriber's option 82 information, such as remote-id and/or circuit-id. However, the option 82 is missing in the DHCPDISCOVER packet. The subscriber session comes up in unauthenticate as expected, but the expected actions (that is, applying L4R service) do not get applied onto the session.

Workaround: There is no workaround.

- CSCtf12803

Symptoms: The command to configure overhead accounting on an ES+ module is not available.

Conditions: The symptom is observed with an ES+ module.

Workaround: There is no workaround.

- CSCtf15982

Symptoms: A router crashes.

Conditions: This symptom is seen when clearing dangling session in data plane, which corrupts memory and leads to router crash.

Workaround: Do not try to clear dangling session from CLI and disable auto clearing the dangling session by issuing the **ip subscriber timer clear-dangling 0** command.

- CSCtf16623

Symptoms: On a Cisco 7600 ES+, the internal VLAN tag is incorrectly inserted into VC-type 4 frames.

Conditions: The symptom is observed with basic functioning.

Workaround: There is no workaround.

- CSCtf19387

Symptoms: CPU hogs may be seen for IP Input process when NHRP is configured.

```
%SYS-3-CPUHOG: Task is running for (5000)msecs, more than (5000)msecs (11/5),process = IP Input.
```

Conditions: This symptom is seen when packets are punted due to incomplete CEF adjacency and processed switched to resolve the next-hop address.

Workaround: Configure “ip nhrp server-only” under DMVPN tunnel.

- CSCtf20154

Symptoms: Max VTemplate limit on RSP720 is 200 and cannot go beyond this number.

Conditions: This symptom is specific to RSP720.

Workaround: There is no workaround.

Further Description: This limit is seen on RSP720. The limit for SUP720 is 1000.

- CSCtf22243

Symptoms: High adjacency usage is seen in stats/non-stats region.

Conditions: This symptom is observed when VPNV4 prefixes are getting load balanced across even number of TE Tunnels that are FRR protected.

Workaround: Change the load-balancing mode to simple and use the **clear ip bgp neighbor \*** command.

- CSCtf22968

Symptoms: IP multicast cannot be L3-switched between two routed pseudowires.

Conditions: The symptom occurs when routed pseudowire is the ingress and egress interface for multicast traffic, and an ES20+ is the exit line card. IP unicast traffic is not affected.

Workaround: There is no workaround.

- CSCtf26061

Symptoms: Packets sent through PXF are not matching the prepaid service but the default service.

Conditions: The symptom is observed with packets sent through PXF.

Workaround: Reload the router.

- CSCtf27303

Symptoms: On a Cisco router, a BGP session for a 6PE (peer-enabled in AF IPv6 and end-label configured) with a third-party router, which does not advertise capability IPv6 unicast (not AFI 2 SAFI 1, only AFI 2 SAFI 4) may be torn down right after it establishes, as the Cisco router sends out an update in the non-negotiated AF IPv6 unicast (AFI/SAFI 2/1).

Conditions: The symptom is observed under the following conditions:

- Cisco side: session enabled for IPv6 + send-label. Cisco router is running Cisco IOS Release 12.2(33)XNE1 and Release 12.2(33)SRE.
- Third-party: only capability IPv6 labeled unicast advertised.

Workaround: There is no workaround.

- CSCtf28329

Symptoms: WCCP service groups do not establish because WCCP control packets (HIA msgs) from the WCCP-enabled appliances are rejected by the router. The WCCP event debugs will indicate “no such service”.

Conditions: The symptom is observed as the router does not support VRF aware WCCP and the router is configured with one or more WCCP service groups where packets from the WCCP appliance arrive at the router on an interface that is configured with a VRF.

Workaround: There is no workaround.



- CSCtf29654
 

Symptoms: Ingress plus egress traffic on ES-20 line card traffic is spanned. The total output traffic span destination interface is much less than aggregate traffic at ingress.

Conditions: This symptom is seen in Cisco 7600 router having ES-20 as ingress line card and trying to monitor huge amount of traffic of more than 5 Gbps.

Workaround: There is no workaround.
- CSCtf33203
 

Symptoms: Supervisor crashes due to RPC communication failure SP-RP.

Conditions: This symptom is observed when high temperature is seen on entire device. One module crosses alarm threshold which generates minor error RPC message.

Workaround: There is no workaround.
- CSCtf33336
 

Symptoms: Offset list configured under RIP process with specific access list number has been NVgened as "offset list 0".

Conditions: The symptom is observed when you use a numbered access list within the range specified. The configuration set to value 0 with an offset-list command under RIP.

Workaround: There is no workaround.
- CSCtf39455
 

Symptoms: Router can hang when xconnect configuration is modified on a VLAN subinterface while data packets are being switched. The following error traceback is printed:

```
%SYS-2-NOTQ: unqueue didn't find 0 in queue
```

Conditions: The symptom is observed when the VLAN subinterface is still seeing data traffic and the main interface is not shut down, and when the xconnect configuration on the VLAN subinterface is being modified.

Workaround: Shut down the main ethernet interface when doing xconnect configuration changes on the subinterface.
- CSCtf40673
 

Symptoms: All OIFs are reset when there is a **shutdown** on one of the interfaces followed by a **no shutdown**.

Conditions: This symptom occurs when there is a **shutdown** on one of the interfaces followed by a **no shutdown**.

Workaround: There is no workaround.
- CSCtf48413
 

Symptoms: MLS CEF entries for default route are not getting reprogrammed for default routes after a LC reload. This issue is there when default route is getting resolved through MPLS TE tunnels with FR objects, and one of the LC through which MPLS TE tunnel passes through crashes.

Conditions: This symptom occurs when default route is reachable through more than one MPLS TE tunnels with FR objects. When one of the LC resets (through which MPLS TE tunnel is passing through), FR object backwalk is not fixing the adjacency properly.

Workaround: This issue happens only in LC reset cases. This will usually not happen in customer networks. Fix by flapping the MPLS TE FRR back up tunnel.

- CSCtf50894

Symptoms: During the collection process an interrupt is raised by a higher priority event (topology change, that is, a tunnel shutdown). If the tunnel shutdown occurs at a very precise time before the collection is complete, data structures used by FRR collection end up being deleted/changed by the higher priority event. When the suspended FRR statistics collection process resumes, it ends up working with data that has become stale/trashed. This results in a crash.

Conditions: The symptom is observed on an MPLS TE FRR enabled router that will trigger periodic collection of accounting information for all prefixes using a given TE tunnel as its next-hop. This process is invoked in 10 second intervals and it can be suspended by other higher priority processes before its runtime completion.

Workaround: Disable FRR protection.

- CSCtf51332

Symptoms: An interface with PBR/VRF select configuration punts all traffic to the RP and causes high CPU usage. When MLS rate-limiter is configured, there might be packet losses at higher rate of traffic.

Conditions: When a PBR/VRF-select route map is removed from the first interface on which the PBR/VRF select was configured, the internal RSVP VLAN is removed. This causes the packets from all interfaces with this route map to be punted to the RP.

Workaround 1: Disable VPN-CAM lookup.

Workaround 2: Configure identical route maps with different names, for example:

```
route-map sak-vrfs-in1 permit 10
    match ip address SAK-PAM-SOURCES
    set vrf sak-pam
!
route-map sak-vrfs-in1 permit 20
    match ip address SAK-VOIP-SOURCES
    set vrf sak-voip
!

route-map sak-vrfs-in2 permit 10
    match ip address SAK-PAM-SOURCES
    set vrf sak-pam
!
route-map sak-vrfs-in2 permit 20
    match ip address SAK-VOIP-SOURCES
    set vrf sak-voip
!
```

Apply these route maps on to the interfaces which will carry identical VRF select configurations.

```
interface GigabitEthernet2/3.104
    description SAK/PAM Turku C-FI-20709-8416
    encapsulation dot1Q 104
    ip vrf receive sak-pam
    ip vrf receive sak-voip
```

```

    ip address 10.100.220.177 255.255.255.252
    no ip redirects
    no ip proxy-arp
    ip policy route-map sak-vrfs-in1
arp timeout 300
!
interface GigabitEthernet2/3.505
    description SAK/PAM Turku C-FI-20709-8416
    encapsulation dot1Q 505
    ip vrf receive sak-pam
    ip vrf receive sak-voip
    ip address 10.100.220.26 255.255.255.254
    no ip redirects
    no ip proxy-arp
    ip mtu 1500
    ip policy route-map sak-vrfs-in2
    arp timeout 300
!
```

Workaround 3: Create a dummy interface and apply this route map first on the dummy interface (but do not delete the subinterface).

- CSCtf52083

Symptoms: When an ISG system with DHCP subscribers get reloaded, some sessions may not restart when DHCP renew messages are received by the ISG router.

Conditions: The symptom is observed on a system reload/restart.

Workaround: There is no workaround.

- CSCtf53672

Symptoms: A router crashes when any CWAN module is not responding to the RP keepalives.

Conditions: The symptom is observed with a Supervisor 32.

Workaround: There is no workaround.

- CSCtf54547

Symptoms: After resetting the Standby ESR-PRE2, the card continuously stays in a boot cycle.

Conditions: The symptom is observed when there is “loopback remote” configured under a serial interface. It is seen only with an 8E3DS3 card.

Workaround: Remove the “loopback remote” configuration.

- CSCtf56678

Symptoms: Aggregate policer starts dropping traffic before reaching the configured Committed Information Rate (CIR).

Conditions: The symptom is observed when the PFC QoS aggregate policer is configured and when the CIR configured is above 1370 Mbs. For example:

```

Policy Map POLICER-IN
    Class class-default
```

```

police cir 1380000000 bc 31250000
  conform-action transmit
  exceed-action drop

```

Workaround: Configure a value below or equal to cir 1370000000.

- CSCtf72678

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip>.

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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

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](http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html)

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm>

- CSCtf75064

Symptoms: MAC withdrawal is not sent to remote VPLS peer.

Conditions: The symptom is observed with a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRE0a upon receiving a TCN BPDU on an L2GP port.

Workaround: There is no workaround.

- CSCtf75587

Symptoms: Active RP crashes when ISSU upgrade is initiated (SSO mode) from Cisco IOS Release 12.2(33)SRD3 to Release 12.2(33)SRD4.

Conditions: The symptom is observed when “mls qos” is configured on the router and then an SSO mode ISSU switchover is initiated.

Workaround 1: Disable QoS with the **no mls qos** command.

Workaround 2: Upgrade in RPR mode. First, verify that following command is not in the running-configuration:

**no service image-version efsu.**

If this command is in the running configuration, remove it using **service image-version efsu.**

- CSCtf78196
 

Symptoms: Although tunnel interface has alternative path to an OSPF neighbor, when the primary interface goes down, the tunnel interface goes down for a moment.

Conditions: The symptom occurs when a tunnel tracks an MTU from higher value to a lower value on the outgoing interface. (It is seen on many images)

Workaround: Statically configure “ipv6 mtu *mtu*” on tunnel interfaces.
- CSCtf78662
 

Symptoms: On a Cisco 7600 series router that is configured with REP, the IGMP query is not forwarded through the secondary REP port leaving part of the ring incapable of receiving multicast traffic. The other switches in the REP ring located after the secondary port are unable to receive the IGMP queries from the Cisco 7600 and thus may not elect any mrouter port.

Conditions: The symptom is observed only when the REP has a converged topology and the alternate port is not located in the Cisco 7600 but anywhere else in the REP ring.

Workaround 1: One of the two REP ports on the Cisco 7600 must be elected/configured as an alternate port.

Workaround 2: One of the two REP ports on the Cisco 7600 must be in shutdown.
- CSCtf82883
 

Symptoms: When clearing a VRF route, there is a traffic drop on other VRF routes.

Conditions: The symptom is observed with an L3 VPN configuration.

Workaround: There is no workaround.

Further Problem Description: Some LTE broker distribution is leaked to other VRFs.
- CSCtf98985
 

Symptoms: MAC withdrawal is not sent to the remote VPLS peer for MST instances other than MST0.

Conditions: The symptom is observed on a Cisco 7600 series router with Cisco IOS Release SRE0a upon receiving a TCN BPDU on an L2GP port.

Workaround: There is no workaround.
- CSCtg00497
 

Symptoms: Router runs out of memory due to NHRP leaking memory.

Conditions: The symptom is observed when NHRP is running (DMVPN). A leak is caused whenever you see “NHRP: Encapsulation failed” when “debug nhrp” is enabled.

Workaround: There is no workaround.
- CSCtg11421
 

Symptoms: The following issues are observed:

  - All egress traffic by SIP-400 is dropped.
  - Consecutive BusConnectivityTest failure for SIP-400.
  - When SIP-400 is hosting intelligent SPAs such as SPA-8XCHT1/E1, then this SPA gets into OutSrvc state.

Conditions: The symptom is observed with a SIP-400 with egress LLQ shaping and with a high volume of traffic to low speed stream.

Workaround 1: SIP-400 reload using the **hw-module module X reset** command (where X is the module/SIP-400 number).

Workaround 2: Remove LLQ configuration.

Workaround 3: SIP-400 microcode reload (where X is the module/SIP-400 number):

attach X enable microcode reload np

- CSCtg14446

Symptoms: Packets are dropped in excess of the configured rate for hierarchical policies, with shaper in the parent policy.

Conditions: The symptom is observed only with HQoS policies (flat policies are not affected).

Workaround: There is no workaround.

- CSCtg14755

Symptoms: In a 6PE environment, on a Cisco 7600 PE injecting a directly connected v6 prefix, the hardware programming for the BGP local label for that prefix might be incorrect when an IPv6 address is deleted and re-added.

Conditions: The symptom is observed when multiple BGP paths exist for this prefix (remote PEs advertise the same prefix).

Workaround: Perform a shut/no shut on the local interface.

- CSCtg16191

Symptoms: A SIP-400 line card may crash due to a memory leak in the code for bringing down PPPoE sessions. A few hours before the crash, the line card starts to generate the following logs:

```
%SYS-2-MALLOCFAIL: Memory allocation of
100352 bytes failed from 0x407F181C, alignment 0
Pool: Processor Free: 2242304 Cause: Memory fragmentation Alternate Pool:
None Free: 0 Cause: No Alternate pool
```

You can also verify this memory leak using the **show memory allocating-process totals** command on the SIP-400 line card and searching for VA\_LOCK. More memory is allocated to VA\_LOCK when you bring up PPPoE sessions, but the usage will not go down even after the PPPoE sessions are torn down.

Conditions: The symptom is observed only with PPPoE sessions.

Workaround: There is no workaround.

- CSCtg22349

Symptoms: Real reassign is not working in the ASNLB Vserver.

Conditions: The symptom is observed when the real server is configured with reassign.

Workaround: There is no workaround.

- CSCtg22774

Symptoms: The input queue on which the packets are being received for RLB is getting wedged and all the packets are being dropped.

Conditions: The symptom is observed on an RSP720 platform only and when the packet size is more than 512 bytes.

Workaround: You can use SUP720, if the hardware is available.

Further Problem Description: RSP platform supports particle-based packet buffers. When the packet is punted to the SLB process, the particles are collated and converted to contiguous buffers. If there is an error in the RLB packet processing, then the packet is being freed assuming that it is a particle. This freeing is not succeeding and the packet is getting queued to the input interface queue permanently.

- CSCtg25798

Symptoms: The issue is associated with the two labels imposition for the next-hop address. If there is no label bind for the destination prefix and in order to reach next-hop address the router imposes two labels, only one label is imposed for the final prefix.

Conditions: The symptom occurs when all of the following conditions are met:

1. The prefix does not have a label bind (BGP prefixes for example).
2. There is a static route for the next-hop address pointing to the tunnel only.
3. The router imposes two labels for the next-hop address.

Workaround: There are three potential workarounds:

1. Explicit next hop avoiding recursive research: “ip route 192.168.4.4 255.255.255.255 Tu1 192.168.4.4” (that is, breaking rule 2).
2. Use “neighbor 192.168.1.1 send-label” on both PEs (that is, breaking rule 1).
3. Use “mpls traffic-eng signaling interpret explicit-null verbatim” on P (that is, breaking rule 3).

In the following example 192.168.200.200 is the final destination. There is no label bind for this prefix and it is recursive to 192.168.100.100:

```
PE1#sh mp ld bin 192.168.200.200 32
  lib entry: 192.168.200.200/32, rev 35
    local binding: label: 31

PE1#sh ip route 192.168.200.200
Routing entry for 192.168.200.200/32
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 192.168.100.100
    Route metric is 0, traffic share count is 1
```

The next-hop 192.168.100.100 has a static route pointing to the tunnel and is double tagged:

```
PE1#sh ip route 192.168.100.100
Routing entry for 192.168.100.100/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Tunnel10
    Route metric is 0, traffic share count is 1

PE1#sh ip cef 192.168.100.100
192.168.100.100/32
  attached to Tunnel10 label 26

PE1#sh mp ld bin 192.168.100.100 32
```

```
lib entry: 192.168.100.100/32, rev 30
  local binding: label: 29
  remote binding: lsr: 192.168.2.2:0, label: 26
  remote binding: lsr: 192.168.4.4:0, label: 26 <<<<< tunnel head-end
```

So the traffic to 192.168.200.200 should also be double tagged as shown below:

```
PE1#sh ip cef 192.168.200.200
192.168.200.200/32
  nexthop 192.168.100.100 Tunnel10 label 26
```

However traffic is leaving the router only with the tunnel label:

```
PE1#trace 192.168.200.200
Type escape sequence to abort.
Tracing the route to 192.168.200.200
 0 192.168.12.2 [MPLS: Label 20 Exp 0] 4 msec 0 msec 0 msec
 1 192.168.23.3 [MPLS: Label 23 Exp 0] 4 msec 0 msec 0 msec
 2 192.168.34.4 4 msec 0 msec 0 msec
 3 192.168.48.8 4 msec * 4 msec
```

- CSCtg31434

Symptoms: A Cisco router crashes due to an unexpected exception to the CPU.

Conditions: This symptom occurs when the **privilege interface level 10 ppp authentication** command is entered. This symptom is observed in Cisco IOS Release 12.2(31)SB through Release 12.2(31)SB18, and in Cisco IOS Releases 12.2(33)SB and 12.2(34)SB.

Workaround: There is no workaround.

- CSCtg32647

Symptoms: Crypto tunnel fails to come up and the following message is seen:

```
%CRYPTO-3-IKMP_QUERY_KEY: Querying key pair failed.
```

Conditions: The symptom is observed when using Cisco IOS Release 12.2(33)XNF. Other releases may also be affected.

Workaround: Use Cisco IOS Release 12.2(33)XND1.

- CSCtg40901

Symptoms: Crash seen while authenticating with TACACS.

Conditions: The symptom is observed if the TACACS server does not respond.

Workaround: Use multiple connections.

Alternate Workaround: Configure a dummy TACACS server.

- CSCtg44661

Symptoms: A router crashes when unconfiguring a route map.

Conditions: The symptom is observed when a policy route map with the **set ip next-hop recursive** command is removed from an interface, then the route map is unconfigured.

Workaround: There is no workaround.



- CSCtg68047
 

Symptoms: The router reloads.

Conditions: The symptom is observed if several tunnels with crypto protection are being shut down on the router console and the **show crypto sessions** command is executed simultaneously on another terminal connected to the router.

Workaround: Wait until the tunnels are shut down before issuing the show command.
- CSCtg70117
 

Symptoms: A newly added EVC cannot receive multicast traffic.

Conditions: The symptom is observed with ES20/ES+ configured with EVC mode. There are two METs in ES20/ES+ line cards. When a service instance is configured under Met0 and it starts receiving a multicast flow, and then you configure another interface under Met1 with service instance in same BD, the newly added service instance will not receive the multicast traffic.

Workaround: Perform a shut/no shut on the VLAN.
- CSCtg72735
 

Symptoms: In MPLS VPN, CE-CE traffic and PE-CE traffic experience high packet loss from 10 to 50 percent.

Conditions: The symptom is observed under the following conditions:

  1. There is access configuration on the subinterface.
  2. Some subinterfaces belong to same VRF.
  3. There is a frequent interface flapping on a subinterface with this VRF.

Workaround: Cancel access configuration on subinterface.
- CSCtg79881
 

Symptoms: The subscriber cannot enable the SSS session due to DPM not finding the binding in the table although the binding exist when performing the **show ip dhcp server binding** command. If you use **debug sss policy event/err** the following message shows:

```
SG-DPM: DHCP Binding does not exist to query session
```

Conditions: The symptom is observed under the following conditions:

  - The subscriber has DHCP binding when using **show ip dhcp server binding** (Note: Also check the VRF, if any).
  - The subscriber has no entry in the DPM policy.
  - Session trigger needs to be L2-connect DHCP.

Workaround 1: If this is a low lease time and relay dhcp case:

  - Make sure the subscriber does not send a DHCP packet.
  - Wait for the binding to disappear.
  - Reenable the user DHCP forwarding.

Workaround 2: If this is a dhcp server case, then clear DHCP binding.

Workaround 3: Reload the router.
- CSCtg91201
 

Symptoms: DHCP-added static routes get removed sometimes and the traffic towards the host gets dropped.

Conditions: The symptom is observed with IP unnumbered relay and with a third-party external DHCP server. (This issue can also occur with an IOS DHCP server, but the probability is quite low.)

Workaround: There is no workaround.

- CSCtg92105

Symptoms: IPv6 CLI is missing under the subinterface after EVC is configured on the main interface on SRE.

Conditions: The symptom is observed when EVC is configured on the main interface.

Workaround: Remove the EVC configuration on the main interface then IPv6 can be configured.

- CSCth01288

Symptoms: ES+ 10G interface can flap (up and then down) during bootup and SSO.

Conditions: The symptom is observed when the interface is not administratively down and when XFP is connected with no cable.

Workaround: Administratively shut down the interface.

- CSCth02725

Symptoms: There is an interoperability issue between a third-party vendor's routers and Cisco routers with severe IPTV service failure in Prune-Overriding environment.

Conditions: The symptom is observed in the following scenario:

1. Router A is Cisco 7609 router (IP address 10.1.1.1) and connects to Router B (third-party vendor's router; IP address 10.1.1.3) and Router C (IP address 10.1.1.2).
2. If the subscriber under Router C disappears, Router A receives "Prune" message from Router C.
3. Router A does not change "source IP of PruneEcho message (10.1.1.2)" and sends it to Router B.
4. At this time, Router B should send overriding-join to Router A because Router B still has subscribers. But Router B drops the PruneEcho message because source IP (10.1.1.2) is not from PIM neighbor. Router B cannot send overriding-join to Router A.
5. As a result, multicast traffic (IPTV stream) to Router B stops.

Workaround: Connect C and B to become PIM neighbors. However, this cannot always be considered a recommended workaround because of potential high cost or other (sometimes third-party) limitations.

- CSCth08505

Symptoms: PPPoE sessions may not sync to the standby RP.

Conditions: This symptom is observed after the first attempt at establishing a PPPoE session fails.

Workaround: Reloading the standby RP may resolve this issue.

- CSCth15790

Symptoms: ES+ low-queue line card crashes with HQoS policy applied.

Conditions: The symptom is observed with an HQoS policy and with three-level HQoS and classes containing "priority" statements for either priority level1 or level2. When traffic passed through either of the PQ classes the line card may crash after some random period of time.

Workaround: There is no workaround.

- CSCth18571

Symptoms: An ES+ module may reload when a SPAN session is configured for a source VLAN.

Conditions: The symptom is observed with a Cisco 7600 ES+ and with Cisco IOS Release 12.2(33)SRD4. VFI configuration needs to be present.

Workaround: There is no workaround.

- CSCth29393

Symptoms: Downstream traffic (to the subscriber) is not forwarded. Only upstream counters are increasing.

Conditions: The symptom is observed with the **show sss session detail** command with PXF output.

Workaround: Clear the affected SSS session.

- CSCuk47773

Symptoms: IPv6 BGP does not flag RIB failure.

Conditions: The symptom is observed when a BGPv6 learned route is not the best option in RIB due to the availability of better administrative distance route or RIB reaches max-prefix.

Workaround: There is no workaround.

## Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page:*  
<http://www.cisco.com/warp/public/108/index.shtml>
- *Troubleshooting Bus Error Exceptions:*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_tech\\_note09186a00800cdd51.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml)
- *Why Does My Router Lose Its Configuration During Reboot?:*  
[http://www.cisco.com/warp/public/63/lose\\_config\\_6201.html](http://www.cisco.com/warp/public/63/lose_config_6201.html)
- *Troubleshooting Router Hangs:*  
[http://www.cisco.com/warp/public/63/why\\_hang.html](http://www.cisco.com/warp/public/63/why_hang.html)
- *Troubleshooting Memory Problems:*  
<http://www.cisco.com/warp/public/63/mallocfail.shtml>
- *Troubleshooting High CPU Utilization on Cisco Routers:*  
<http://www.cisco.com/warp/public/63/highcpu.html>
- *Troubleshooting Router Crashes:*  
[http://www.cisco.com/warp/public/122/crashes\\_router\\_troubleshooting.shtml](http://www.cisco.com/warp/public/122/crashes_router_troubleshooting.shtml)
- *Using CAR During DOS Attacks:*  
[http://www.cisco.com/warp/public/63/car\\_rate\\_limit\\_icmp.html](http://www.cisco.com/warp/public/63/car_rate_limit_icmp.html)

## Related Documentation

The following sections describe the documentation available for Cisco IOS Release 15.0S. These documents consist of hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, feature modules, and other documents.

Documentation is available online on Cisco.com.

Use these release notes with the following resources:

- [Platform-Specific Documents, page 212](#)
- [Cisco Feature Navigator, page 212](#)
- [Cisco IOS Software Documentation Set, page 212](#)

## Platform-Specific Documents

Platform-specific information and documents for the Cisco 7600 series routers are available at the following location:

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](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 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 15.0S 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/ps10890/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps10890/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](mailto: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](mailto: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 212.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

---

