Release Notes for Cisco IOS Release 15.2S

First Published: November 8, 2011
Last Updated: February 17, 2012
Release: Cisco IOS Release 15.2(1)S1
Part Number: OL- 26035-01 Rev. B0

Introduction

These release notes support Cisco IOS Release 15.2S up to and including Cisco IOS Release 15.2(1)S1. These release notes are updated as needed to describe new features, caveats, and related documents.

The latest release of Cisco IOS software for the Cisco 7600 series routers introduces new features and provides continued operational benefits for service providers. The Cisco 7600 series routers offer advanced wireless and wireline services and transport capabilities enabling Fix Mobile Convergence.

Over 30 additional features have been added to Cisco IOS Release 15.2S including the following:

Synchronization features including:

- Synchronous Ethernet: ESMC & SSM
- NTPv4 Orphan Mode Support, Range for Trusted Key Configuration

Management enhancements including support for:

- Extensible Messaging Client Protocol 2.0
- CISCO-ENTITY-DISPLAY-MIB
- Voltage Table Support for CISCO-ENVMON-MIB
- Video Monitoring MIB Support for Medianet Video Monitoring
- Point to Multi-Point MPLS-TE MIB

New hardware including support for:

- GLC-EX-SMD, GLC-ZX-SMD
- SPA-1xCHOC48-DS3 Support on Cisco 7600-SIP-400

Routing, MPLS Transport and IPv6 Enhancements including support for:

- IPv6 Policy-Based Routing

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

- DHCPv6-Relay Chaining (for Prefix Delegation) and Route Insertion in FIB
- Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: Packed Cell Relay
- ATM Port Mode Packed Cell Relay over MPLS
- BGP-Origin AS Validation
- EIGRP Dual DMVPN Domain Enhancement
- MPLS Diff-Serv-Aware Traffic Engineering
- MPLS TE-Autoroute Destinations
- MPLS TE-Autotunnel/Automesh SSO Coexistence
- MPLS TE-DS-TE (RFC-3270)
- MPLS TE-Enhanced Path Protection
- MPLS TE-Interarea Tunnels
- MPLS TE-Inter-AS TE
- MPLS TE-Shared Risk Link Groups
- MPLS VPN-L3VPN over GRE

ATM/Frame Relay enhancements including support for:

- Frame Relay Fragmentation
- N:1 PVC Mapping to PWE with Non-Unique VPI (ATMCOMMON)
- 32k PVC Scale with Multipoint Bridging on SIP-400

Fast Convergence or High Availability including support for:

- PoDWDM Proactive Protection Support for Cisco 7600
- L2VPN Resilient Pseudowire
- Multichassis LACP IGMP Snooping State Sync
- VPLS MAC Address Withdrawal
- DHCP Snooping over Pseudo-MLACP

System Requirements

This document describes the system requirements for Cisco IOS 15.2S releases and includes the following sections:

Memory Recommendations

Note Memory recommendations tables are not included in the Cisco IOS Release 15.2S release notes to improve the usability of the release notes documentation. The memory recommendations are available through 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 and when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

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

Determining Memory Recommendations for Software Images (Feature Sets)

To determine memory recommendations for software images (feature sets) in Cisco IOS Release 15.2S, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Search by feature**.

Step 2 To find the memory recommendations, use either "Search by full or partial feature name" or "Browse features in alphabetical order." Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the Features available text box on the left side of the web page.

Step 3 Choose a feature from the Features available text box, and click the **Add** button to add a feature to the Features selected text box on the right side of the web page.

Note To learn more about a feature in the list, click the Show Description(s) button below the Features available text box.

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

Step 4 Click **Continue** when you are finished selecting features.

Step 5 From the Major Release drop-down menu, select **15.2S**.

Step 6 From the Release drop-down menu, choose the appropriate maintenance release.

Step 7 From the Platform drop-down menu, choose the appropriate hardware platform. The "Search Results" table will list all the software images (feature sets) that support the feature(s) that you chose, plus the DRAM and flash memory recommendations for each image.

Supported Hardware

Cisco IOS Release 15.2S 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)
- RSP720-10GE
- Supervisor Engine 32, Supervisor Engine 720, Route Switch Processor 720

Guide to Supported Hardware for Cisco 7600 Series Routers

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

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

Determining the Software Version

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

```
Router# show version

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

Upgrading to a New Software Release

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

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

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

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

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

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

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

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

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

Limitations and Restrictions

This chapter describes limitations and restrictions in Cisco IOS 15.2S releases.

Limitations and Restrictions in Cisco IOS Release 15.2(1)S

There are no new limitations and restrictions in Cisco IOS Release 15.2(1)S.

Features and Important Notes

These release notes describe the following topics:

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.2S and contains the following subsections:

New Hardware Features in Cisco IOS Release 15.2(1)S

This section describes new and changed features in Cisco IOS Release 15.2(1)S. Some features may be new to Cisco IOS Release 15.2(1)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(1)S. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

32k PVC Scale with Multipoint Bridging on SIP-400

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

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

New Software Features in Cisco IOS Release 15.2(1)S

This section describes new and changed features in Cisco IOS Release 15.2(1)S. Some features may be new to Cisco IOS Release 15.1S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(1)S. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

32k PVC Scale with Multipoint Bridging on SIP-400

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

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

Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: Packed Cell Relay

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

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

ATM Port Mode Packed Cell Relay over MPLS

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

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

BGP—Origin AS Validation

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-origin-as.html

CISCO-ENTITY-DISPLAY-MIB

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

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

DHCP Snooping over Pseudo-MLACP

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

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

DHCPv6—Relay Chaining (for Prefix Delegation) and Route Insertion in FIB

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-dhcp.html

EIGRP Dual DMVPN Domain Enhancement

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2s/config-eigrp.html

Extensible Messaging Client Protocol 2.0

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

http://www.cisco.com/en/US/docs/ios-xml/ios/saf/configuration/15-2s/saf-saf.html

Frame Relay Fragmentation

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

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

GLC-EX-SMD, GLC-ZX-SMD

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

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

IPoDWDM Proactive Protection Support for Cisco 7600

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

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

IPv6 Policy-Based Routing

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-pol-bsd-rtng.html

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/IPv6_PBR.html

L2VPN Resilient Pseudowire

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-2s/wan-l2vpn-pw-red.html

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

MPLS Diff-Serv-Aware Traffic Engineering

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

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

MPLS TE—Autoroute Destinations

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_setup/configuration/15-2s/mp-te-interarea-tun.html

MPLS TE—Autotunnel/Automesh SSO Coexistence

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

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

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

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

MPLS TE—DS-TE (RFC-3270)

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

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

MPLS TE—Enhanced Path Protection

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

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

MPLS TE—Interarea Tunnels

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

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

MPLS TE—Inter-AS TE

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

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

MPLS TE—Shared Risk Link Groups

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

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

MPLS VPN—L3VPN over GRE

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l3_vpns/configuration/15-2s/mp-vpn-gre.html

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

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

Multichassis LACP IGMP Snooping State Sync

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

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

N:1 PVC Mapping to PWE with Non-Unique VPI (ATMCOMMON)

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

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

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_nto1_PVC_map_to_PWE.html

NTPv4 Orphan Mode Support, Range for Trusted Key Configuration

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

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/15-2s/bsm-time-calendar-set.html

Point to Multi-Point MPLS-TE MIB

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_em_and_mibs/configuration/15-2s/mp-p2mp-mpls-te-mib.html

SPA-1xCHOC48-DS3 Support on Cisco 7600-SIP-400

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

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

Synchronous Ethernet: ESMC & SSM

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

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

Video Monitoring MIB Support for Medianet Video Monitoring

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* at the following URL:

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

Voltage Table Support for CISCO-ENVMON-MIB

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

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

VPLS MAC Address Withdrawal

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

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

MIBs

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

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

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

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

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

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

Important Notes

The following sections contain important notes about Cisco IOS Release 15.2S.

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a standalone document. When behavior changes are introduced, existing documentation is updated with the changes described in these sections:

Cisco IOS Release 15.1(2)S2

The following behavior changes were introduced in Cisco IOS Release 15.2(1)S1:

- BGP-Origin AS Validation feature is changed in two ways.

  Old Behavior 1: The router may send serial query or reset query messages to an RPKI server at any time.

  New Behavior 1: The router will not send a serial query message or reset query message during the interval between when it sends a serial query or reset query message and when it receives an End of Data (EOD) message. Serial queries in this interval are stripped, and reset queries in this interval are sent upon receipt of the EOD message.

  Old Behavior 2: The Invalid state indicates the prefix is found, but either the corresponding AS received from the eBGP peer is not the AS that appears in the SOVC table or the prefix length in the BGP Update message is longer than the maximum length permitted in the SOVC table. The Not Found state indicates that the prefix is not among the prefixes or prefix ranges in the SOVC table.

  New Behavior 2: The Invalid state indicates that the prefix meets either of the following two conditions:

  1. It matches one or more Route Origin Authorizations (ROAs), but there is no matching ROA where the origin AS matches the origin AS on the AS-PATH.
  2. It matches the one or more ROAs at the minimum-length specified in the ROA, but for all ROAs where it matches the minimum length, it is longer than the specified maximum length. Origin AS does not matter for condition #2.

  The Not Found state indicates that the prefix is not among the Valid or Invalid prefixes.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-origin-as.html

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

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

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

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

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

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

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

- The IKEv2 profile name must be specified to disassociate it from a crypto map or IPsec profile.

  Old Behavior: The IKEv2 profile name does not need to be specified to disassociate it from a crypto map or IPsec profile.

  New Behavior: The IKEv2 profile name must be specified to disassociate it from a crypto map or IPsec profile.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-cfg-ikev2-flex.html#GUID-DC2773B6-7E71-43F4-B4E7-25063C7D4851

- A command is added to truncate the downstream ANCP rate.

  Old Behavior: In situations where large number of unique Access Node Control Protocol (ANCP) rates generated result in a correspondingly high number of policy maps, the number of policy maps can exceed the maximum number of policy maps supported on a router.

  New Behavior: Use the **ancp truncate** command to reduce the ANCP rate.

  Caution: This command is to be used only in exceptional scenarios, such as when the number of unique rates generated result in exceeding the maximum number of policy maps supported on a router.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/ancp/command/ancp-a1.html#GUID-4AB51EAF-C9B7-48EB-A3E4-E18D2A576816

- 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:
  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-l1.html

- Optimization of ACL TCAM entry consumption on the Cisco 7600 platforms for Policy Based Routing under certain circumstances.

  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 sub-optimal in terms of number of TCAM entries and masks used.

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

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

- Cisco ASR 1000 BDI interface supports MTU size change.

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

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

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

- Fast Network Time Protocol (NTP) synchronization is achieved.

  Old Behavior: The burst and initial burst (iburst) modes are enabled manually.

  New Behavior: The burst and iburst modes are enabled by default.

Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-CC69EFC5-68A3-4C5D-90CD-67DE45D4A370

- The **telecom-solutions** keyword is not supported.

  Old Behavior: The **telecom-solutions** keyword in the **ntp refclock** command allows users to configure the reference clock driver.

  New Behavior: The **telecom-solutions** keyword, along with its options, is visible but cannot be configured.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-875B8F64-2179-4F71-8BC0-6BF103EBB22F

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/cisco/software/advisory.html

Field Notices and Bulletins

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

Caveats for Cisco IOS Release 15.2S

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

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

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

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

This section consists of the following subsections:

- Resolved Caveats—Cisco IOS Release 15.2(1)S1, page 19
- Open Caveats—Cisco IOS Release 15.2(1)S, page 36

Resolved Caveats—Cisco IOS Release 15.2(1)S1

Cisco IOS Release 15.2(1)S1 is a rebuild release for Cisco IOS Release 15.2(1)S. The caveats in this section are resolved in Cisco IOS Release 15.2(1)S1 but may be open in previous Cisco IOS releases.

- CSCee38838

  Symptoms: A crashdump may occur during a two-call-per-second load test on a gateway, and the gateway may reload.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(7)T and that functions as a gateway when you run a two-call-per-second load test that uses H.323, VXML, and HTTP. The crash occurs after approximately 200,000 calls.

  Workaround: There is no workaround.

- CSCsb53810

  Symptoms: A Cisco Catalyst 6500 series switch may not block traffic, which is supposed to be denied by an outbound ACL on a VLAN interface.

  Conditions: This issue is under investigation.

  Workaround: Reload the switch.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

Workaround: Disable AAA. If this not an option, there is no workaround.

- 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.

- CSCtg58029

  Symptoms: After switchover, aaa_acct_session_id iss not issued to new sessions.

  Conditions: This symptom occurs only after switchover.

  Workaround: There is no workaround.

- CSCtj64807

  Symptoms: Router crashes while issuing the **show vlans dot1q internal** command.

  Conditions: The symptom is observed with the following conditions:

  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.

  Workaround 1: For any Cisco 10000 series router which has had its first crash on any subinterface if the outer VLAN has second-dot1q VLAN as only “any”, immediately delete the sub-interface and recreate it. Then add a dummy VLAN/sub-interface to this outer VLAN.

  Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.

  Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only “any” and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtk00181

  Symptoms: Password aging with crypto configuration fails.

  Conditions: The symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.

  Workaround: There is no workaround.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- CSCtn02208

  Symptoms: Old PerUser ACL is not removed on applying new ACL.

  Conditions: This symptom occurs when applying a new PerUser ACL to an existing session. The old PerUser ACL that exists on the session is not removed.

  Workaround: There is no workaround.

- CSCtn40771

  Symptoms: The process ACL Header in the **show memory allocating- process totals** command output leaks memory with per-user ACLs and PPP session churn. This will also cause the SSS feature manager process in the **show process memory** command output to appear to have a leak.

  Conditions: This symptom occurs with IPv6 per-user ACLs and session churn.

  Workaround: There is no workaround.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- 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”.

- CSCtr08680

  Symptoms: The following error messages are displayed on active and standby respectively:

  ```
  %ERROR: Standby doesn't support this command BERT is running on this channel group, please abort bert first.
  ```

  Conditions: This symptom is observed when trying to create a channel after BERT has been started irrespective of whether BERT is running or completed.

  Workaround: There is no workaround.

- CSCtr45551

  Symptoms: T1/E1 controller does not get selected as network clock input source.

  Conditions: This symptom occurs when network-clock input source t1/e1 command is configured immediately after reload of the router or within 5 minutes from router bootup.

  Workaround: After the router reloads, wait for 5 to 6 minutes (until SETS gets initialized) and then configure T1/E1 as network clock input source.

- CSCtr47642

  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the **bgp additional-paths select best- external** command, a specific prefix may not have bestpath calculated for a long time.

  Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

  1. Configure: **bgp additional-paths install** under vpnv4 AF
  2. Configure: **bgp additional-paths select best-external**

Immediately disable backup path calculation/installation using the **no bgp additional-paths install** command.

The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

Workaround: Configure the **bgp additional-paths install** command and the **bgp additional-paths select best-external** command with a delay of 10 seconds.

- 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, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

  For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

  For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

  Workaround for symptom 1: Remove import-route target and reconfigure route-target.

  Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- CSCts00341

  Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server** *server.domain.com*, the command fails with the following message on the console:

```
ASR1k(config)#ntp server server.domain.com         <<<    DNS is not resolved
with dual RPs on ASR1k
Translating "server.domain.com "...domain server (10.1.1.1) [OK]

%ERROR: Standby doesn't support this command              ^
% Invalid input detected at '^' marker.

ASR1k(config)#do sh run | i ntp
ASR1k(config)#
```

  Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

  Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts13255

  Symptoms: Standby SUP720 crash is observed on the Cisco 7600 router in c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

```
%CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive
heartbeats
```

Conditions: This symptom is observed on the Cisco 7600 router with mistral based supervisors like SUP720. This issue is fairly uncommon, but affects all the versions after Cisco IOS Release 12.2(33)SRE, including Cisco IOS Releases 15.0S, 15.1S and 15.2S. This does not affect RSP 720.

Workaround: There is no workaround.

- CSCts23882

  Symptoms: ISG calculates the radius response authenticator in CoA account- profile-status-query replies wrongly, resulting in an invalid response.

  Conditions: This symptom is observed when the CoA/WWW based session authentication is triggered via a CoA account logon using the “old” SSG command attributes.

  Workaround: Configure a fix “NAS-IP-Address” value with the **radius- server attribute 4** *x.x.x.x* command.

- CSCts67465

  Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.

  Conditions: The symptom is observed always, if the standby is configured as an SSO.

  Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCts70790

  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

  Workaround: Remove and re-add the **neighbor default- originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCts85694

  Symptoms: The following error message is displayed:

  ```
  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi (0x104C2E4)
  ```

  Conditions: This symptom is seen when clearing the sessions after a long time, and the memory leak increases incrementally. Leak is very slow.

  Workaround 1: Do not bring down all sessions together.

  Workaround 2: Do not tear down the sessions (scale numbers: 4k and above) together from different sources (say clearing PPP sessions and ISG sessions in lab; in field, clearing might happen via other triggers) simultaneously with no time gap between them.

  Workaround 3: Do not have accounting accuracy configured.

  Workaround 4: In this case, ISG Features are applied on TC and Session both. If we do not apply the features on the TCs, chances of this happening are less.

- CSCts97124

  Symptoms: Active crashes upon configuring a large number of TP tunnels with scale configurations either using copy paste or loading from a configuration file.

  Conditions: This symptom is not very consistent, not reproducible all the time, and happens only on adding tunnel TP configurations. The crash occurs when the protect-lsp is being configured.

Workaround: Manually add the MPLS-TP tunnels through CLI instead of copying from a configuration or copy pasting a large configuration.

- CSCts97856

  Symptoms: PIM Assert is sent out from a router with metric [0/0], though the router has a less preferred path to reach the Source or RP.

  Conditions: This symptom occurs when an mroute is first created and its RPF lookup to the Source or RP is via BGP or Static, which involves recursive lookup, or there is no valid path to reach Source or RP. This issue only occurs in a small window in milliseconds. After the window, the metric [0/0] is corrected.

  Workaround: There is no workaround.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCtt01056

  Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1="", "<>", or "", then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:

  - In case of service activation from Access-Accept, the session should be terminated.
  - In case of service activation from COA, the COA should be NAKed, and the services rolled back.

  Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param="", "<>", or "". This issue is seen with service activation with a missing mandatory parameter.

  Workaround: There is no workaround.

- 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.

- CSCtt02645

  Symptoms: CPUHOG is seen due to flapping of all NHRP.

  Conditions: This symptom is observed with scaling to 3k spokes on RP1.

  Workaround: There is no workaround.

- CSCtt04448

  Symptoms: There is a loss of IGMP snooping entries with a traffic drop at the pmLACP PoA boxes occurring.

  Conditions: This symptom is observed when removing/re-adding member links.

Workaround: There is no workaround.

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt17785

  Symptoms: In the output of **show ip eigrp nei** *det*, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.

  Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).

  Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- CSCtt17879

  Symptoms: The **bgp network backdoor** command does not have any effect.

  Conditions: This symptom occurs:

  – On 64-bit platform systems.

  – When the network is learned after the backdoor has been configured.

  Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt26643

  Symptoms: A Cisco ASR 1006 router that is running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.

  Conditions: This symptom is observed on a Cisco ASR 1006 router that is running the asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin image. The **show version** command causes the “Last reload reason: Critical software exception” error.

  Workaround: There is no workaround.

- CSCtt28703

  Symptoms: VPN client with RSA-SIG can access a profile where the CA trustpoint is not anchored.

  Conditions: This symptom is seen with the use of RSA-SIG.

  Workaround: Restrict access by using a certificate-map matching the right issuer.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.5/3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:N/A:N/E:POC/RL:W/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtt29615

  Symptoms: Any CLI command issued under af-interface mode in EIGRP router may lead to router crash.

Conditions: This problem is observed in a Cisco router that is running Cisco IOS Release 15.2(1)S.

Workaround: There is no workaround.

- CSCtt31634

  Symptoms: Traffic drops.

  Conditions: This symptom occurs when the hw-module reloads the IM on active and posts which switchover is performed.

  Workaround: After switchover, use the **hw-module subslot reload** command to recover from the problematic state, and traffic will resume.

- CSCtt32165

  Symptoms: The Cisco Unified Border Element Enterprise on the Cisco ASR 1000 series router can fail a call with cause 47 immediately after the call connects.

  Conditions: This symptom is observed with a sufficient call volume and a call flow that redirects many calls. The Cisco ASR router can fail to provision the forwarding plane for the new call due a race condition where a prior call is not completely cleaned up on the forwarding plane before trying to use the same structure again.

  The **show voice fpi stats** command output indicates that a failure has occurred if the last column is greater than zero. For example:

  show voip fpi stats | include provisn rsp

  provisn rsp 0 32790 15

  Workaround: There is no workaround. However, Cisco IOS Release 3.4.1 is less impacted by these call failures due to a resolution of defect CSCts20058. Upgrade to Cisco IOS Release 3.4.1 until such time as this defect is resolved. In a fully redundant Cisco ASR 1006 router, you can failover the ESP slots to clear the hung entries in the forwarding plane. Other platforms will require a reload.

- CSCtt43843

  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.

  Conditions: This symptom is occurring with a Cisco 7200 platform that is loaded with the Cisco IOS Interim Release 15.2(1.14)T0.1 image.

  Workaround: There is no workaround.

- CSCtt45536

  Symptoms: “FlowVar- Chunk malloc failed” messages are seen and this may be accompanied by slow console response.

  Conditions: The symptom is observed when a mix of IPv4 and IPv6 traffic is going through the router configured with QoS, VM, etc.

  Workaround: There is no workaround.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt70585

  Symptoms: IPv6 traffic is not flowing.

  Conditions: This symptom is seen with IPSec v6 tunnels.

  Workaround: There is no workaround.

- CSCtt95846

  Symptoms: Changing the encapsulation of an Ethernet service instance which is set up for local switching to default encapsulation may cause an error in setting up switching, resulting in an inability to switch packets.

```
PE1#show running-config | include local
connect local Ethernet0/0 1 Ethernet1/0 1
PE1#configure terminal
```

  Enter configuration commands, one per line. End with CNTL/Z.

```
PE1(config)#interface Ethernet0/0
PE1(config-if)#service instance 1 ethernet
PE1(config-if-srv)#encapsulation default
PE1(config-if-srv)#end
PE1#show ssm id
SSM Status: No switches
```

  Conditions: This symptom is observed if **no aaa new-model** is configured.

  Workaround: Unconfigure the local switching connection before changing the encapsulation of the service instance, then reconfigure the connection.

- CSCtu01172

  Symptoms: The Cisco ASR 1000 series router without an actual redundant router may crash when configured for CUBE HA based on the document “Cisco Unified Border Element High Availability(HA) on ASR platform Configuration Example.”

  Conditions: This symptom is observed with the Cisco ASR 1000 series router.

  Workaround: Remove the application configuration, that is, “no application redundancy”.

- CSCtu02286

  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.

- CSCtu12574

  Symptoms: The **show buffers** command output displays:

  1. Increased missed counters on EOBC buffers.
  2. Medium buffer leak.

```
Router#sh buffers
Buffer elements:
     779 in free list (500 max allowed)
     1582067902 hits, 0 misses, 619 created


Interface buffer pools:
```

```
....
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
     273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

This DDTS tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```
0A9C4ED8: 00200000 02150000 0202080B 01000000  . ............... --> IPC Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A  .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000    .R.............  --> ICC Header
            --  --
```

And, if we look at the ICC header at the underscored items 00520002:

```
0052   (represents the class name)             ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)          ----> L3_MGR_MLS_REQ
```

Workaround: Reload the system.

- CSCtu18201

  Symptoms: A Cisco router crashes due to low stack with the following display:

  ```
  %SYS-6-STACKLOW: Stack for process BGP Event running low, 0/6000
  ```

  Conditions: This symptom occurs with a low stack.

  Workaround: There is no workaround.

- CSCtu19450

  Symptoms: A system that is running Cisco IOS may reload when a large number of routes are simultaneously deleted at the same time that the inetCidrRouteTable is being walked.

  Conditions: This symptom is only likely to happen when there are large numbers of interfaces and routes within the system, and when large numbers of routes are being rapidly removed, and the system is loaded, at the same time that the inetCidrRouteTable is being walked.

  Routes may be deleted from the system both directly, and also indirectly for example, when a significant number of PPPoE sessions are removed.

  Workaround: Avoid walking the inetCidrRouteTable while significant numbers of routes are being removed from the routing system.

- CSCtu29729

  Symptoms: An attempt to create a frame-relay sub-interface on a serial interface may result in error. The serial interface can then not be configured as a frame-relay interface.

Conditions: This symptom is observed when a serial interface is configured as a multi-link frame-relay bundle link with a subsequent attempt to change the configuration to a frame-relay interface.

Workaround: There is no workaround.

- CSCtu31340

  Symptoms: The **show sip call called-number** crashes the router.

  Conditions: This symptom is observed when the call SIP state is DISCONNECT.

  Workaround: There is no workaround.

- CSCtu33956

  Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.

  Conditions: This symptom is observed under the following conditions:

  – The PPPoE dialer client needs to be configured on the physical SHDSL interface.
  – The GRE tunnel destination interface should point to the dialer interface.
  – The MPLS pseudowire should go over the tunnel interface.
  – After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.

  Workaround: There is no workaround.

- CSCtu35713

  Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.

  Conditions: This symptom is observed under the following conditions:

  1. Enable IPv4 address saving on BRAS.
  2. Configure AAA periodic accounting using the **aaa accounting update periodic** *time in mins* command.
  3. Initiate IPCP negotiation from the client.
  4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

  Workaround: Configure AAA accounting with the **aaa accounting update newinfo periodic** *time in mins*.

- CSCtu36674

  Symptoms: Packets stop being transmitted in the output direction on L2transport local connect PVC on the ATM interface.

  Conditions: This symptom is observed when local connect is configured and a new ATM subinterface is configured on the same ATM main interface as the one with local connect PVC.

  Workaround 1: Perform shut/no shut on local connect.

  Workaround 2: Unconfigure/reconfigure local connect.

- CSCtu39819

  Symptoms: The Cisco ASR 1002 router configured as an RSVPAgent for Cisco Unified Communication Manager crashes under extended traffic.

Conditions: This symptom is observed on a Cisco ASR 1002 router configured as an RSVPAgent for CUCM End-to-End RSVP feature. The router crashes after 45 minutes of traffic run with 150 simultaneous up MTP-RSVP sessions.

The asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin image is used.

Workaround: There is no workaround.

- CSCtu41137

  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.

  Conditions: The core is observed while doing unconfiguration.

  Workaround: There is no workaround.

- CSCtu43731

  Symptoms: On an RP1, RP switchover causes an RP reset.

  Conditions: This symptom is observed with RP switchover under the following conditions:

  – The router must be an RP1
  – The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.

  An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

  Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

  Workaround 2: Do not enable FNF monitoring.

- CSCtu87383

  Symptoms: CFM global configuration does not get applied to LC slots that are greater than 20 on LC OIR. This problem is specific to CPT platform where satellite box slot numbers go from 36 to 55.

  Conditions: This symptom occurs with satellite box OIR.

  Workaround: Disable and reenable CFM global configuration.

- CSCtu89771

  Symptoms: The Cisco ASR 1000 series router RP crashes while unconfiguring or removing the **no area 0 authentication ipsec spi <>** command.

  This behavior is not observed at the first few instances of unconfiguring the above CLI.

  Conditions: This symptom is observed only in automated tests where unconfiguring the authentication with the above CLI is executed multiple (approximately 3) times on the Cisco ASR 1000 series router. This leads to the RP crashes.

  Workaround: There is no workaround.

- CSCtu92213

  Symptoms: Console is stuck and irresponsive.

  Conditions: This symptom is seen when EVC with QoS is scaled, and traffic is being sent through many policy-maps with a large queue limit.

  Workaround: Configure a smaller queue-limit under each class on all egress policy-maps in use.

- CSCtu92289

  Symptoms: VCCV BFD on PW HE (routed pseudowire) is not working.

Conditions: VCCV BFD is not working on routed pseudowire but works fine on scalable EoMPLS.

Workaround: There is no workaround.

- CSCtu92673

  Symptoms: L2TP tunnels are not getting established with PPPoE relay.

  Conditions: This issue is seen on a Cisco 7200 router that is running Cisco IOS Interim Release 15.2(01.12)S.

  Workaround: There is no workaround.

- CSCtv19529

  Symptoms: Router crashes on unconfiguring the last available DHCP pool. Crash will also be seen on running the **no service dhcp**.

  Conditions: This crash can happen only if “DHCP Client” process is running on the router along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).

  The client process can be started:

  1. from an DHCP autoinstall attempt during router startup (with no nvram config).
  2. if the **ip address dhcp** is run on one of the interfaces. 3) if the router was used for DHCP proxy client operations.

  The relay processes are started when a DHCP pool is created by the **ip dhcp pool** *pool* command.

  Workaround: Have a dummy DHCP pool created using the **ip dhcp pool** *dummy_pool* command, and never delete this pool. Other pools can be created and removed at will, the *dummy_pool* should not be removed. In addition, do not execute the **no service dhcp** command.

- CSCtw43640

  Symptoms: An IP ping/CFM session through Handoff FPGA fails.

  Conditions: This symptom is observed after switchover with IM in slot 5.

  Workaround: There is no workaround.

- CSCtw45055

  Symptom: 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.

- CSCtw45168

  Symptoms: DTMF interworking fails when MTP is used to convert OOB---RFC2833 and vice versa.

  Conditions: This symptom is observed when MTP is used to convert OOB---RFC2833 and vice versa. This issue is seen starting from Cisco IOS XE Release 3.2S. Cisco IOS XE Release 3.1S should work fine.

  Workaround: There is no workaround.

- CSCtw46625

  Symptoms: The QL value is DNU although the four least significant bits of SSM S1 byte are pointing to PRC (bits: 0010).

  Conditions: This symptom is observed when SSM S1 byte is received on CEoPs SPAs or channelized SPA-1XCHSTM1/OC3.

  Workaround: Force the QL PRC value by executing the following command:

  network-clock quality-level rx QL-PRC *controller SONET 1/2/0*

- CSCtw48209

  Symptoms: High-end Cisco devices running Cisco IOS are likely affected. Active features at the time of this problem manifestation include any condition that leads to RSVP SNMP notification generation in Cisco IOS. BGP/MPLS TE instability, leading to changes to RSVP session status change, is observed in a test scenario while running Cisco IOS Release SXI4 and Cisco IOS Release SXI7. The issue is not reproducible consistently.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SXI4, Cisco IOS Release 12.2(33)SXI7, Cisco IOS Release 12.2SR, Cisco IOS Release 12.2SX, and Cisco IOS Release 15S.

  Workaround: Disable RSVP notification using the **no snmp-server enable traps rsvp** command.

- CSCtw50277

  Symptoms: Policy manager is getting apply config failed on standby while policy is activated through CoA. The router later crashes in policy code.

  Conditions: This symptom is seen when CoA activated policy install is failing on standby RP.

  Workaround: There is no workaround.

- CSCtw51134

  Symptoms: IMA interface configuration is lost post stateful switchover (SSO).

  Conditions: This symptom occurs after SSO.

  Workaround: There is no workaround.

- CSCtw52504

  Symptoms: WAN mode is not enabled on 10G IMs.

  Conditions: This symptom is observed when a 10G IM operates in LAN mode by default. The WAN mode supports SONET alarms to interface with SONET-like equipments.

  Workaround: There is no workaround.

- CSCtw52610

  Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.

  Conditions: The issue is seen when primary link is considered OOP based on utilization despite using the **no resolve utilization** command.

  Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure “max-xmit-utilization percentage 100”.

- CSCtw58395

  Symptoms: When executing the **clear crypto session** command in 4k FlexVPN cases, the memory of crypto IKEv2 is increasing.

  Conditions: This symptom is observed when the session is flapping.

  Workaround: There is no workaround.

- CSCtw58586

  Symptoms: IKEv2 CLI configuration currently requires to manually link the crypto IKEv2 profile default to the crypto IPSec profile default. This enhancement request will change the behavior and create an automatic anchorage.

  Conditions: This symptom is seen in IKEv2 usage.

  Workaround: There is no workaround.

- CSCtw64040

  Symptoms: Crash due to MPLS, which appears to be associated with load- balancing.

  Conditions: This symptom occurs when MPLS is configured.

  Workaround: There is no workaround.

- CSCtw68745

  Symptoms: A Cisco ASR 1000 router acting as DHPCv6 Relay standby crashes when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

  Conditions: This symptom occurs when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

  Workaround: There is no workaround.

- CSCtw73551

  Symptoms: Standby RP can crash due to a memory leak processing calls. The crashinfo file identifies the process as follows:

  ```
  UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps
  ```

  Conditions: This symptom is seen on CUBE enterprise on the Cisco ASR 1000 series router with redundant RPs and approximately 2.4 million calls processed from last start of the standby RP.

  Workaround: There is no workaround.

- CSCtw76044

  Symptoms: Need IGMP/MLD information to make IGMP/MLP snooping work.

  Conditions: The symptom is observed under all conditions.

  Workaround: There is no workaround.

- CSCtw79579

  Symptoms: Standby fails to be in standby HOT state after reload.

Conditions: This symptom is seen after removal of an IM and doing RSP stateful switchover (SSO) and then trying to bring up the standby RSP.

Workaround: There is no workaround.

- CSCtw85883

  Symptoms: The error “ace_add_one_map failed” occurs while adding an ACE to a crypto ACL that is being used by a crypto map.

  Conditions: This symptom is observed when the crypto map is applied to an interface and the crypto ACL being modified is also in use.

  Workaround: Remove the crypto map and apply the ACL changes to avoid the error.

- CSCtw94319

  Symptoms: Crash is seen at dhcpd_forward_request.

  Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.

  Workaround: Remove the **ip dhcp relay information option vpn** command, if possible. Otherwise, there is no workaround.

- 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.

- CSCtw99877

  Symptoms: IOMD process on 10G IM crashes upon booting standby.

  Conditions: This symptom is observed when the interface state is down on active.

  Workaround: There is no workaround.

- CSCtx01604

  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.

  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.

  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- CSCtx05942

  Symptoms: The session to the service module from the Supervisor Fails. This can happen with SAMI, NAM, NAM-2 etc. modules.

  For example, if the SAMI card is in Slot 2, the **session slot** *2* **processor 0** command fails to create a telnet session and fails to give out the following messages:

```
SUP#session slot 2 proc 3
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.33 ...
```

```
% Connection timed out; remote host not responding
```

Conditions: This symptom occurs with Cisco IOS Release 15.2(1)S release. It is not observed with Cisco IOS Release 15.1(3)S1 or lower version.

Workaround: Downgrading the Supervisor to Cisco IOS Release 15.1(3)S1 or lower version resolves this issue.

- CSCtx09614

  Symptoms: With the preconfigured ATM configuration, the standby RSP does not boot up.

  Conditions: This symptom is observed when one of the RSPs is up and the running configuration has the ATM configuration under the controller.

  Workaround: There is no workaround. Without an ATM configuration, the standby RSP goes to standby mode.

- CSCtx21206

  Symptoms: BFDv6 hardware offloaded sessions do not come up with all IPv6 source addresses.

  Conditions: This symptom is observed with interface source IPv6 addresses that have some specific bits in the 6th byte set like 6001:1:C::1..

  Workaround: Reconfigure the source IPv6 addresses to some address that will not match the criteria mentioned in the above Conditions.

- 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.

- CSCtx63034

  Symptoms: After a Cisco 7600 router is powered by PWR-2500-DC, PWR-4000-DC or PWR-6000-DC to Cisco IOS Release 15.2(1)S, the router logs the following error messages:

  ```
  %C7600_PWR-SP-3-PSUNKNOWN: Unknown power supply in slot 1 (idprom read
  failed).
  %OIR-SP-6-INSPS: Power supply inserted in slot 1
  %C7600_PWR-SP-4-PSOK: power supply 1 turned on.
  ```

  The **show power** command shows that the power supply only provides 919W. Most of the line cards cannot be powered up.

  Conditions: This symptom is observed in Cisco IOS Release 15.2(1)S only. The problem does not occur in Cisco IOS Release 15.1(3)S1. PWR-4000-DC and PWR-6000-DC are confirmed to be affected by this problem.

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(1)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.2(1)S. All the caveats listed in this section are open in Cisco IOS Release 15.2(1)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- 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.

- CSCtj58706

  Symptoms: On executing ISSU runversion, the standby RP reloads multiple times before reaching hot-standby.

  Conditions: This symptom is observed during ISSU upgrade/downgrade with the iso1-iso2 image. This issue is seen with scaled configuration of 7000 L2VPN, 300 BGP, 300 EIGRP, and 8000 EVC sessions.

  Workaround: There is no workaround.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- CSCtn83900

  Symptoms: After performing legacy mode or native mode subpackage ISSU with flexible NetFlow configured, the interface to monitor bindings may not be present on the newly active RP.

  Conditions: This symptom is observed when a legacy mode or native mode subpackage ISSU is performed with FNF configured.

  Workaround: Remove the FNF monitors prior to the subpackage ISSU. Add the monitors back to the interface configuration after the upgrade. Alternatively, use super-package ISSU, which does not have this limitation.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- CSCtq80891

  Symptoms: The Processor Pool for the Cisco IOS memory is used up with most of the buffers in the "IPv6 PIM input queue".

  Conditions: This symptom is observed with the following topology:

  IXIA [IPv6 Mcast Source] ------ TR1 (ASR1k) ------|500 IPv6 over IPv4 GRE

  Tunnels | ------ UUT (ASR1k) [IPv6 RP] ------ |500 IPv6 over IPv4 GRE

  Tunnels | ------ TR2 (7200) ------ IXIA [IPv6 Mcast MLD Hosts]

  - 500 IPv6 Sources sending Mcast traffic to 500 IPv6 Mcast groups
  - 500 PIM-RP on UUT
  - 500 PIM-RP Acl to make sure 1 Mcast-group/Tunnel
  - The GRE tunnels could be configured with tunnel protection or not.

  The reproduce procedure is as follows:

  1. Copy configurations (IPv6 over IPv4 GRE Tunnel Protections and IPv6 Mcast included) to TR1, TR2, and UUT.
  2. Launch Mcast traffic (500M) on IXIA.
  3. Hit the Cisco IOS memory depletion issue on UUT.

  Workaround: Configure the punt policer for PIM register packets as follows:

  platform punt-policer 55 limit-number
  platform punt-policer 55 limit-number high

  The limit-number above is a number between 1000-2000.

- CSCtr80274

  Symptoms: CISCO-LICENSE-MGMT-MIB does not populate.

  Conditions: This symptom occurs when the required license is installed on the Cisco ASR 903 router, but the SNMP query does not return any value.

```
NMS-RACK1-RUDY-1#show license
Index 1 Feature: metroaggrservices
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: metroipservices
        Period left: 8  weeks 4  days
        License Type: Evaluation
        License State: Active, Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 3 Feature: metroservices
        Period left: 8  weeks 4  days
        License Type: Evaluation
        License State: Active, Not in Use, EULA not accepted
        License Count: Non-Counted
```

```
        License Priority: None
sw-mrrbu-nms-2:2> getmany 3.3.2.11 ciscoLicenseMgmtMIB
sw-mrrbu-nms-2:3>
```

Workaround: There is no workaround.

- CSCts05124

  Symptoms: A zero-byte crash file is generated upon a crash with TREX SPA.

  Conditions: This symptom is observed with a test crash on a SIP-400 line card with TREX SPA inserted.

  Workaround: There is no workaround.

- CSCts11715

  Symptoms: After shutting the tunnel, ISAKMP does not turn OFF.

  Conditions: This symptom is observed in a scaled DMVPN setup with more than 1k spokes.

  Workaround: There is no workaround.

- CSCts12499

  Symptoms: SPA firmware crash at one bay leads to SPA crash in another bay.

  Conditions: This symptom is observed when “test crash cema” is executed from the SPA console. leading to the SPA in the other bay to reload. Also, the crashinfo is not present in the RP disk.

  Workaround: There is no workaround.

- 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.

- CSCts20632

  Symptoms: If subclassification and classification for the protocol is configured in a different class map, configuring the port map and assigning a different port (other than 80) for HTTP causes unexpected error messages to be displayed.

  Conditions: This symptom is observed when subclassification and protocol classification is configured for HTTP and a port map is configured for HTTP.

  Workaround: There is no workaround.

- CSCts47550

  Symptoms: When applying protocol attributes policy rules, traceback may be seen.

  Conditions: This symptom is not consistent and may or may not appear when applying the protocol attributes policy rules. The symptom is also not consistent with a specific protocol, but may appear with respect to different protocols.

  Workaround: There is no workaround.

- CSCts63426

  Symptoms: With 1K EoMPLS PWs, 6 percent performance drop is observed in Cisco IOS XE Release 3.5 compared to Cisco IOS XE Release 3.4 performance.

  Conditions: This symptom is observed with 1K EoMPLS PWs in Cisco IOS XE Release 3.5.

  Workaround: There is no workaround.

- CSCts63658

  Symptoms: Multicast traffic do not flow over EVCs on the port-channel.

  Conditions: This symptom is observed during router reload.

  Workaround: Reconfigure after the router reload. Configure regular EFPs before EFPs on the PC in the same BD.

- CSCts82598

  Symptoms: Incorrect IP from the NAT pool is chosen for translation, when one protocol exhausts all ports of all IPs and another protocol traffic is received.

  Conditions: This symptom occurs when one protocol (for example, TCP) exhausts all ports of all IPs in a pool, and only one IP from the pool is selected for translation, thus limiting the capacity of creating translations. This happens only when one protocol completely exhausts all ports and then another protocol traffic starts. This usually is not the case in customer environments that mostly see both TCP and UDP traffic hitting the box time.

  Workaround: There is no workaround.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCtt01056

  Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1=””, “<>”, or ““, then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:

  - In case of service activation from Access-Accept, the session should be terminated. - In case of service activation from COA, the COA should be NAKed, and the services rolled back.

  Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param=””, “<>”, or ““. This issue is seen with service activation with a missing mandatory parameter.

  Workaround: There is no workaround.

- CSCtt02645

  Symptoms: CPUHOG is seen due to flapping of all NHRP.

  Conditions: This symptom is observed with scaling to 3k spokes on RP1.

  Workaround: There is no workaround.

- CSCtt04724

  Symptoms: On PPPoEoX, when activating multiple services from Access-Accept with long Cisco-SSG-Account-Info strings, if the aggregated string length exceeds the current limit of 256 characters, then the service activation fails, a traceback is seen, and the session is allowed to establish, no services will be applied in the ingress and/or egress directions.

  Conditions: This symptom is observed when the aggregated services string length exceeds the limit (256 characters).

  Workaround: The session should be terminated instead. In case of service activation from CoA, if the cumulative services string length exceeds the limit, then the last CoA should be NAKed, and the services rolled back to the previous state.

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt11558

  Symptoms: The Cisco ASR 1000 router displays the “INVALID_GPM_ACCESS” error message due to invalid GPM load. This may cause unexpected Embedded Services Processors (ESP) reload.

  Conditions: This symptom is observed when a small packet is sent from a BDI interface to an Ethernet service instance with either the **rewrite egress tag** command or the **rewrite ingress tag** command with the **symmetric** option present.

  Workaround: There is no workaround.

- CSCtt21257

  Symptoms: After a reload or switchover, all interfaces on one or more IMs may be down down. The state of the IMs is “ok, active”, which is shown in the **show platform** command output.

  Conditions: This symptom is occasionally observed after a reload or a switchover.

  Workaround: Power cycle the box.

- CSCtt26532

  Symptoms: With QoS policy-map configured on a BFD interface, modifying the QoS policy-map flaps the BFD session.

  Conditions: This symptom is observed when BFD and QoS policy-maps are configured on the same interface.

  Workaround: There is no workaround.

  Further Problem Description: QoS and BFD use a common flag that gets reset and set during QoS policy-map update, causing the BFD session to flap. BFD session flap leads to the OSPF session also going down.

- CSCtt33937

  Symptoms: Configure port 7 on the Gigabit IM as a port to forward traffic using IP routing.

  ```
  config t
  interface g0/0/7
  ```

```
ip address 10.0.0.1 255.255.255.0
```

Conditions: This symptom is observed when traffic is flowing well. When you perform a switchover, and once the standby becomes the new active, the traffic does not hit the ingress counter of the interface itself. On checking the links status using the registers, the SGMI link appears out of sync.

Workaround: There is no workaround. Reload the box when this symptom is observed.

- CSCtt34361

  Symptoms: During a soak test with 1800 PPPoE sessions flapping with the IPv4 Saving feature enabled + per-user ACLv4 and ACLv6, there is no ISG service. After 56 iterations, one memory snapshot is taken every four iterations, that is, roughly 270 seconds per iteration. The test duration is 4 hours, with total 100800 sessions established with an average of 7cps.

  Conditions: This symptom occurs under the following conditions:

  1. No active session is there in the router.
  2. Establish 1800 PTA dual-stack sessions with per-user ACL from Radius + IPV4 Saving feature.
  3. Wait till all sessions come UP.
  4. Take a memory leak snapshot “high”.
  5. Wait for all sessions to time out on the Idle timer (no traffic).
  6. Wait for all sessions to go DOWN.
  7. Take a memory snapshot.
  8. Loop back to 1.

  Workaround: There is no workaround.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt45801

  Symptoms: The DMVPN HUB RP crashes with the default EIGRP timer when scaling to 4k spokes.

  Conditions: This symptom occurs when scaling to 4k spokes.

  Workaround: Changing the EIGRP timer to longer may reduce the chances of a crash.

- CSCtt70133

  Symptoms: The RP resets with FlexVPN configuration.

  Conditions: This symptom is observed when using the **clear crypto session** command on the console.

  Workaround: There is no workaround.

- CSCtt70346

  Symptoms: IOMD crash is seen when running the PTP session.

  Conditions: This symptom is observed when running the PTP session for a long time. Sometimes, this issue is seen when changing PTP packet rates. This issue is seen rarely.

  Workaround: There is no workaround.

- CSCtt70498

  Symptoms: After a reload or switchover, the state of F0 or F1 may become “disconnecting” instead of “ok, active/standby”, which is shown in the **show platform** command output. As a result, the corresponding RSP does not forward traffic.

  Conditions: This symptom is occasionally observed after a reload or a switchover.

  Workaround: Power cycle the box.

- CSCtt94147

  Symptoms: Nile manager crash is observed.

  Conditions: This symptom is observed with the following conditions:

  - VPLS in the core.
  - REP in the access.
  - The access-side REP segment flaps a few times.

  Workaround: There is no workaround.

- CSCtt94566

  Symptoms: The router crashes before all sessions come up.

  Conditions: This symptom occurs before all sessions come up.

  Workaround: There is no workaround.

- CSCtt95577

  Symptoms: After creating the 994th VC on a T1/E1 IM on Rudy, the traffic flow stops. Packets get dropped on the egress on Rudy.

  Conditions: This symptom is observed when ping starts to fail on all the pre-existing VCs upon adding the 994th VC. The working is unaffected till 993 VCs.

  Workaround: Delete the 994th VC to make the pre-existing VCs forward traffic.

- CSCtt97164

  Symptoms: If the router interface is flapped, the HSRP message may be dropped by the punt/inject path.

  Conditions: This symptom is seen if the router interface is flapped.

  Workaround: Disable the inject bypass.

- CSCtt97473

  Symptoms: After a reload or switchover, the RSP may reset during bootup.

  Conditions: This symptom is observed occasionally after a reload or switchover.

  Workaround: There is no workaround.

- CSCtt98574

  Symptoms: After a reload or switchover, the state of one or more IMs may become “out of service” instead of “ok, active/standby”, which is shown in the **show platform** command output. As a result, the corresponding interfaces do not come up.

  Conditions: This symptom is occasionally observed after a reload or a switchover.

  Workaround: Power cycle the box.

- CSCtt99235

  Symptoms: After a switchover, an IOMD process crashes because it has failed to establish LIPC connection.

  Conditions: This symptom is seen occasionally after a switchover.

  Workaround: Reload the box.

- CSCtu02280

  Symptoms: When running the PTP session for more than 12 hours, PTPD may crash.

  Conditions: This symptom occurs when running the PTP session for a long time.

  Workaround: There is no workaround.

- CSCtu02476

  Symptoms: An SSO followed by a change in the xconnect MTU results in the pseudowire in the redundant RP to go down. The pseudowire in the Active RP remains up and running. A subsequent SSO results in the pseudowire to go down.

  Conditions: This symptom is observed with “encapsulation default” at that end of the pseudowire where SSO is performed. An SSO followed by a change in the MTU value, and then a subsequent SSO, causes the pseudowire to go down. This issue is also seen in a setup with redundant pseudowires, where the primary and backup pseudowires configured under the service instance do not come up after changing the MTU with SSO.

  Workaround: Execute “no xconnect” under the service instance, and then reconfigure the pseudowire with the new MTU value under the service instance.

- CSCtu03699

  Symptoms: The Nile Manager crashes.

  Conditions: This symptom is observed when reloading the TP tunnel endpoint multiple times.

  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.

The DDTS CSCtr34960 tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```
0A9C4ED8: 00200000 02150000 0202080B 01000000  . ..............    -----> IPC
Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A  .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000    .R.............       ------>
ICC Header
            --  --
```

And, if we look at the ICC header at the underscored items 00520002:

```
0052   (represents the class name)             ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)          ----> L3_MGR_MLS_REQ
```

Workaround: Reload the system.

- CSCtu13806

  Symptoms: Upon switchover, the “red_switchover_process” process causes a crash on the old active RSP.

  Conditions: This symptom is observed upon switchover.

  Workaround: This crash is harmless as another RSP becomes active and works properly. Reboot the RSP to make it come up as standby.

- CSCtu13951

  Symptoms: Pending objects appear on the active and standby ESP.

  Conditions: This symptom occurs when the edge device to the core link is flapped multiple times for close to two days.

  Workaround: There is no workaround.

- CSCtu17006

  Symptoms: Mediatrace is not working because RSVP fails to select the output interface.

  Conditions: This symptom is observed only with PFR configuration.

  Workaround: Remove the PFR configuration.

- CSCtu17296

  Symptoms: Traffic failure occurs on 3 to 4 VLANs out of 1000.

  Conditions: This symptom is observed after reloading the UUT.

  Workaround: Remove and readd the service instance configuration for the affected VLANs.

- CSCtu17540

  Symptoms: IOMD core is generated on switchover for T1/E1 IM. After switchover, the IOMD process is aborted.

  Conditions: This symptom is observed with every switchover.

  Workaround: There is no workaround.

- CSCtu18150

  Symptoms: FP crash occurs due to a wrong FCID handling issue.

  Conditions: This symptom occurs due to a wrong FCID handling issue.

  Workaround: There is no workaround.

- CSCtu24765

  Symptoms: Under scale (28.8K PPPoX sessions), when executing “show policy-map session” from the CLI, both ESPs crash.

  Conditions: This symptom is observed with a large scale, that is, 28K PPPoE sessions established + ISG QoS services.

  Workaround: There is no workaround.

- CSCtu27601

  Symptoms: On ATM BRAS under scale (16K PPPPoEOA sessions + ISG services), the ESP crashes occasionally during sessions establishment.

  Conditions: This symptom is observed with a large scale (16K PPPPoEOA sessions + services).

  Workaround: There is no workaround.

- CSCtu28990

  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.

  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.

  Workaround: There is no workaround.

- CSCtu29047

  Symptoms: After a reload or switchover, the RSP may exhibit a kernel hang.

  Conditions: This symptom is observed occasionally after a reload or switchover.

  Workaround: Power cycle the box.

- CSCtu32913

  Symptoms: The system may crash when NBAR is continuously enabled/disabled.

  Conditions: This symptom is observed when NBAR is continuously enabled/disabled. This issue is seen after more than 12 hours of continuously enabling/disabling NBAR under traffic.

  Workaround: There is no workaround. The system works fine after reload.

- CSCtu32935

  Symptoms: IPv6 traffic loss of around 30 seconds is seen for routes learned from dynamic routing protocols upon RSP switchover with the Nonstop Forwarding (NSF) configuration. IPv6 CEF is not programmed on the standby RSP.

  Conditions: This symptom is observed with RSP switchover.

  Workaround: There is no workaround for the dynamic routing protocol. Problem will not be seen for static route.

- CSCtu33258

  Symptoms: LDP over MPLS-TP tunnel fails to get established upon router reload.

  Conditions: This symptom is seldom seen when the router is reloaded with scaled MPLS-TP tunnels that have LDP session established over the tunnels. Pinging traffic through the tunnel fails.

Workaround: There is no workaround.

- CSCtu34906

  Symptoms: All ptp sessions go down on the BC upon configuring more than 63 slaves to negotiate with it.

  Conditions: This symptom is observed on the BC when there are more than 63 slaves trying to negotiate with the master. This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master, but only with the BC master.

  Workaround: This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master.

- CSCtu35713

  Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.

  Conditions: This symptom is observed under the following conditions:

  1. Enable IPv4 address saving on BRAS.
  2. Configure AAA periodic accounting using the **aaa accounting update periodic** *time in mins* command.
  3. Initiate IPCP negotiation from the client.
  4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

  Workaround: Configure AAA accounting with the **aaa accounting update newinfo periodic** *time in mins* command.

- CSCtu41497

  Symptoms: The Nile Manager crashes.

  Conditions: This symptom is observed with a 256 rmep scale.

  Workaround: There is no workaround.

- CSCtu43120

  Symptoms: Service accounting start is not sent for L2TP sessions.

  Conditions: This symptom is observed with L2TP.

  Workaround: There is no workaround.

- CSCtu43731

  Symptoms: On an RP1, RP switchover causes an RP reset.

  Conditions: This symptom is observed with RP switchover under the following conditions:

  - The router must be an RP1.
  - The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.

  An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

  Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

  Workaround 2: Do not enable FNF monitoring.

- CSCtu53275

  Symptoms: Out to in traffic is not handled properly. The lookup on inside global is only done in the global routing table and not in the VRF routing table.

  Conditions: This symptom is observed with the following configuration on the Cisco ASR 1000 series router:

  ```
  ip nat inside source static 1.1.1.1 1.1.1.1 vrf test-pe1
  ```

  In to out traffic is handled properly.

  Workaround: A static route in the global routing table for each of these addresses (assuming they are unique) should provide a workaround for this issue.

- CSCtu98727

  Symptoms: ANCP shaping with Model F fails with BRR classes.

  Conditions: This symptom is observed with BRR classes, but works fine with LLQ (priority level) classes.

  Workaround: There is no workaround.

- CSCtv22685

  Symptoms: The ESP on the Cisco ASR 1000 router crashes or the GRE tunnel does not switch over when the destination interface is removed or the route changes, causing the tunnel interface to stop forwarding packets.

  Conditions: This symptom is observed when multiple GRE tunnels are configured on the same interface(s) with a high traffic rate across the tunnels.

  Workaround: Only configure one GRE tunnel per physical interface.

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 15.2S. These documents include hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, and feature modules.

Documentation is available online on Cisco.com.

Use these release notes with the resources described in the following sections:

Platform-Specific Documents

Platform-specific information and documents for the Cisco 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

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

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

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

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

Cisco IOS Software Documentation Set

The Cisco IOS Release 15.2S 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/ps11793/tsd_products_support_series_home.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

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

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

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

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Original SSLeay License:

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

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

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

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

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

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

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

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

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

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

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 49.
