Cross-Platform Release Notes for Cisco IOS Release 12.2SR

January 14, 2008

Cisco IOS Release 12.2(33)SRC

OL-10394-03

These release notes support Cisco IOS Release 12.2SR for the Cisco 7600 series routers up to and including Cisco IOS Release 12.2(33)SRC. With the release of Cisco IOS Release 12.2(33)SRC, Cisco IOS Release 12.2SR also supports the Cisco 7200 series routers (Cisco 7200, Cisco 7200-NPE-G2, and Cisco 7201 routers) and the Cisco 7301 router. These release notes are updated as needed to describe new features, caveats, potential software deferrals, and related documents.

Cisco IOS Software Release 12.2SR is designed for Enterprise WAN and service provider edge networks that require world-class IP and Multiprotocol Label Switching (MPLS) services. The routers in Cisco IOS Release 12.2SR provide scalable, secure, converged network services in the most demanding Enterprise WAN and service provider edge environments.

For more information, see the "Introduction" section on page 2.

For a list of the software caveats that apply to Cisco IOS Release 12.2SR, see the "Caveats" section on page 102 and the *Caveats for Cisco IOS Release 12.2* document. These documents are updated for every maintenance release and are located on Cisco.com.

Use these release notes with theappropriate platform documentation. See the "Related Documentation" section on page 479.

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html.

Contents

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

Introduction

Cisco IOS Release 12.2SR is based on the following releases:

- Cisco IOS Release 12.2
- Cisco IOS Release 12.2S up to and including Release 12.2(18)S
- Cisco IOS Release 12.2SX up to and including Release 12.2(18)SXF
- Cisco IOS Release 12.2SB up to and including Release 12.2(31)SB2 (beginning with Cisco IOS Release 12.2(33)SRC).

In addition, many new features are introduced in Release 12.2SR. Many features and hardware that are supported in this software have been previously released to customers on other software releases.

For information on new features and Cisco IOS commands that are supported by Release 12.2SR, see the "New and Changed Information" section on page 18 and the "Caveats" section on page 102.

Early Deployment Releases

These release notes describe the networking devices for Cisco IOS Release 12.2SR, which is an early deployment (ED) release that is based on Release 12.2, Release 12.2S, Release 12.2SB, and Release 12.2SX. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features.

Chronological List of ED Releases for Cisco IOS Release 12.2SR

Table 1 shows the Cisco IOS Release 12.2SR early deployment releases in chronological order.

Table 1 Chronological List of 12.2SR Early Deployment Releases

Cisco IOS ED Release	Type of ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(33)SRC	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(33)SRC" section on page 21.	See the "New Hardware Features in Cisco IOS Release 12.2(33)SRC" section on page 19. Added support for Cisco 7200 series routers (Cisco 7200, Cisco 7200-NPE-G2, and Cisco 7201 routers) and Cisco 7301 router.	01/14/2008
12.2(33)SRB2	Rebuild	There are no new software features.	There are no new hardware features.	10/12/2007

Table 1 Chronological List of 12.2SR Early Deployment Releases (continued)

Cisco IOS ED Release	Type of ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(33)SRB1	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(33)SRB1" section on page 46.	See the "New Hardware Features in Cisco IOS Release 12.2(33)SRB1" section on page 46.	06/04/2007
12.2(33)SRB	Maintenance	See the See the "New Software Features in Cisco IOS Release 12.2(33)SRB" section on page 53.	See the "New Hardware Features in Cisco IOS Release 12.2(33)SRB" section on page 50.	02/28/2007
12.2(33)SRA6	Rebuild	There are no new software features.	There are no new hardware features.	10/29/2007
12.2(33)SRA5	Rebuild	There are no new software features.	There are no new hardware features.	07/30/2007
12.2(33)SRA4	Rebuild	There are no new software features.	There are no new hardware features.	05/29/2007
12.2(33)SRA3	Rebuild	There are no new software features.	There are no new hardware features.	03/05/2007
12.2(33)SRA2	Rebuild	There are no new software features.	There are no new hardware features.	12/07/2006
12.2(33)SRA1	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(33)SRA1" section on page 73.	There are no new hardware features.	09/06/2006
12.2(33)SRA	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(33)SRA" section on page 74.	See the"New Hardware Features in Cisco IOS Release 12.2(33)SRA" section on page 73.	06/19/2006

Hierarchical List of ED Releases for Cisco IOS Release 12.2SR

Table 2 shows the Cisco IOS Release 12.2SR early deployment releases in hierarchical order.

Table 2 Hierarchical List of 12.2SR Early Deployment Releases

Cisco IOS ED Release	Date of Release	Parent Release	Based on Releases
12.2(33)SRC	01/14/2008	• Release 12.2(33)SRB2 for Cisco 7600 • Release 12.2(31)SR10 for Cisco 7200, Cisco 7201, Cisco 7301	N/A
12.2(33)SRB2	10/12/2007	12.2(33)SRB	N/A
12.2(33)SRB1	06/04/2007	12.2(33)SRB	N/A
12.2(33)SRB	02/28/2007	12.2(33)SRA2	N/A
12.2(33)SRA5	05/29/2007	12.2(33)SRA	N/A
12.2(33)SRA4	05/29/2007	12.2(33)SRA	N/A
12.2(33)SRA3	03/05/2007	12.2(33)SRA	N/A
12.2(33)SRA2	12/07/2006	12.2(33)SRA	N/A

Table 2 Hierarchical List of 12.2SR Early Deployment Releases (continued)

Cisco IOS ED Release	Date of Release	Parent Release	Based on Releases
12.2(33)SRA1	09/06/2006	12.2(33)SRA	N/A
12.2(33)SRA	06/19/2006	Not applicable (first release)	• Release 12.2 • Release 12.2S up to and including Release 12.2(18)S • Release 12.2SX up to and including Release 12.2(18)SXF

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2SR and includes the following sections:

Memory Recommendations

Note Memory recommendations tables are not included in the Cisco IOS Release 12.2SR 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 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://www.cisco.com/support/FeatureNav/FNFAQ.html

Determining Memory Recommendations for Software Images (Feature Sets)

To determine memory recommendations for software images (feature sets) in Cisco IOS Release 12.2SR, 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 Select 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 additional 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 **12.2SR**.

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

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

Supported Hardware

Cisco IOS Release 12.2SR supports Cisco 7600 series routers, including the following models and supervisor engines:

- Cisco 7603-S, Cisco 7604, Cisco 7606, Cisco 7606-S, Cisco 7609, Cisco 7609-S, and Cisco 7613 routers
- Supervisor Engine 32, Supervisor Engine 720, Route Switch Processor 720
- RSP720-3CXL-10GE, RSP720-3C-10GE (The Cisco 7600 Series RSP 720-10GE is introduced on Cisco IOS 12.2(33)SRC on a limited orderability basis.)

Guide to Supported Hardware for Cisco 7600 Series Routers

For extensive information about all supported hardware for Cisco 7600 series routers, see the *Guide to Supported Hardware for Cisco 7600 Series Routers with Release 12.2SR*.

Note Cisco IOS Release 12.2SR supports Cisco 7600 series routers. Do not run this release on Cisco Catalyst 6500 series switches.

With the release of Cisco IOS Release 12.2(33)SRC, Cisco IOS Release 12.2SR also supports the following Cisco 7200 and Cisco 7300 series routers:

- Cisco 7200, Cisco 7200-NPE-G2, and Cisco 7201 routers
- Cisco 7301 router

For information about the new hardware features, see the "New and Changed Information" section on page 18.

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)SRB, EARLY DEPLOYMENT
RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

http://www.cisco.com/warp/public/130/choosing_ios.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/ps133/products_tech_note09186a0080094c07.shtml

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

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

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

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

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

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

Microcode Software

This section describes microcode software that is supported for the Cisco 7600 series shared port adapters in Cisco IOS Release 12.2SR and consists of the following subsections:

FPD Image Packages for the Cisco 7600 Series

Field-programmable device (FPD) image packages include read-only memory monitor (ROMmon), field-programmable gate array (FPGA), and other images. These images are referred to as FPD images. FPD image packages are used to update the FPD images for the shared port adapters (SPAs), SPA interface processors (SIPs), and FlexWAN modules. If a discrepancy exists between an FPD image and the Cisco IOS image that is running on the router, the SIP, SPA, or FlexWAN module for which the discrepancy exists will be deactivated until this discrepancy is resolved. For additional information on FPDs, including the upgrade process, see the “Field-Programmable Devices” section of the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

Note The maximum time to upgrade the FPD images on one SPA, SIP, or FlexWAN module is 6 minutes. The total FPD upgrade time depends on the number of SPAs, SIPs, and FlexWAN modules that are installed in the router.

FPD Image Package for Cisco IOS Release 12.2(33)SRB2

The FPD image package that is used to upgrade SPAs, SIPs, and FlexWAN modules on a router that runs Cisco IOS Release 12.2(33)SRB2 is the c7600-fpd-pkg.122-33.SRB2.pkg file. This FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com and is identical to the FPD package for Cisco IOS Release 12.2(33)SRBwith the exceptions that are listed in Table 3.

Table 3 Release 12.2(33)SRB1 FPD Image Package Content Changes

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
1-port STM1/OC3 CEM SPA (CEoP SPA)	5	IOFPGA	1.21	1.0
	8	UFE	1.13	1.0
	11	UFE	1.13	2.0
	2	SPAMON	1.4	1.0
24-port T1/E1 CEM SPA (CEoP SPA)	4	IOFPGA	1.30	1.0
	7	UFE	1.1	1.0
	1	SPAMON	1.3	1.0
SIP-600	2	SIP-600 I/O FPGA	0.4	0.1

FPD Image Package for Cisco IOS Release 12.2(33)SRB1

The FPD image package that is used to upgrade SPAs, SIPs, and FlexWAN modules on a router that runs Cisco IOS Release 12.2(33)SRB1 is the c7600-fpd-pkg.122-33.SRB1.pkg file. This FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com and is identical to the FPD package for Cisco IOS Release 12.2(33)SRB with the exceptions that are listed in Table 4.

Table 4 Release 12.2(33)SRB1 FPD Image Package Content Changes

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
1-port STM1/OC3 CEM SPA (CEoP SPA)	5	IOFPGA	1.18	1.0
	8	UFE	1.12	1.0
	11	UFE	1.12	2.0
24-port T1/E1 CEM SPA (CEoP SPA)	4	IOFPGA	1.28	1.0
	7	UFE	1.9	1.0
	1	SPAMON	1.1	1.0

FPD Image Package for Cisco IOS Release 12.2(33)SRB

The FPD image package that is used to upgrade SPAs, SIPs, and FlexWAN modules on a router that runs Cisco IOS Release 12.2(33)SRB is the c7600-fpd-pkg.122-33.SRB.pkg file. This FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com. Table 5 shows the image packet contents for Release 12.2(33)SRB.

Table 5 Release 12.2(33)SRB FPD Image Package Contents

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0
	2	T3E3 SPA I/O FPGA	1.0	0
	3	T3E3 SPA E3 FPGA	1.4	0
	4	T3E3 SPA T3 FPGA	1.4	0
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0
	2	T3E3 SPA I/O FPGA	1.0	0
	3	T3E3 SPA E3 FPGA	1.4	0
	4	T3E3 SPA T3 FPGA	1.4	0
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.14
	1	CTE1 SPA ROMMON NP	2.12	0
	2	CTE1 SPA I/O FPGA	2.7	0
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.1
	2	CT3 SPA I/O FPGA	2.7	0.1
	3	CT3 SPA T3 FPGA R1	0.11	0.1
	3	CT3 SPA T3 FPGA R2	1.4	0.2
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.1
	2	CT3 SPA I/O FPGA	2.7	0.1
	3	CT3 SPA T3 FPGA R1	0.11	0.1
	3	CT3 SPA T3 FPGA R2	1.4	0.2
2-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0
	1	POS SPA IOFPGA P2	3.4	0.2
4-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0
	1	POS SPA IOFPGA P2	3.4	0.2
1-port OC12 POS SPA	1	POS SPA IOFPGA P1	3.4	0
	1	POS SPA IOFPGA P2	3.4	0.2
2-port OC-48 POS/SRP HH SPA	1	Multi-Port OC48 POS/RPR SPA FPD	1.0	0
4-port OC-48 POS/SRP HH SPA	1	Multi-Port OC48 POS/RPR SPA FPD	1.0	0
1-port OC-192 POS/SRP FH SPA	1	1-Port POS/RPR SPA IOFPGA P1	1.2	0
1-port OC-192 POS/SRP HH SPA	1	1-Port POS/RPR SPA IOFPGA P1	1.2	0
	1	1-Port POS/RPR SPA IOFPGA P2	1.2	2.0
1-port OC-48 POS/SRP HH SPA	1	1-Port POS/RPR SPA IOFPGA P2	1.2	0

Table 5 Release 12.2(33)SRB FPD Image Package Contents (continued)

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
2-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.26	0
4-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.26	0
1-port OC12 ATM SPA	1	KATM SPA IOFPGA	1.26	0
1-port OC48 ATM SPA	1	KATM OC48 SPA IOFPGA	0.15	0
	2	SNOOP BUS FPGA	0.3	0
10-port GE SPA	1	GE SPA FPGA	1.1	0
5-port GE SPA	1	GE SPA FPGA	1.1	0
2-port GE SPA	1	GE SPA FPGA	1.1	0
10-port GE V2 SPA	1	GE SPA FPGA	1.1	0
5-port GE V2 SPA	1	GE SPA FPGA	1.1	0
2-port GE V2 SPA	1	GE SPA FPGA	1.1	0
1-port 10GE SPA	1	10GE SPA FPGA	1.9	0
1-port 10GE V2 SPA	1	10GE SPA FPGA	1.9	0
4-port FE SPA V2	1	FE SPA FPGA	1.1	0
8-port FE SPA V2	1	FE SPA FPGA	1.1	0
2-port IPsec SPA	1	PROM	1.1	0.1
	2	LODI	1.21	0.1
	3	Sequoia	1.1	0.1
1-port Channelized STM1/OC3 SPA	1	STM1/OC3 SPA ROMMON	2.12	0
	2	STM1/OC3 SPA I/O FPGA	1.7	0
	3	STM1/OC3 SPA ET3 FPGA	1.4	0
24-port T1/E1 CEM SPA (CEoP SPA)	4	IOFPGA	1.21	1.0
	7	UFE	1.6	1.0
	1	SPAMON	1.1	1.0

Table 5 Release 12.2(33)SRB FPD Image Package Contents (continued)

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
SIP-200	1	SIP-200 I/O FPGA P1	1.1	0.1
	1	SIP-200 I/O FPGA P4	1.1	0.4
	1	SIP-200 I/O FPGA P6	1.1	0.6
	1	SIP-200 I/O FPGA R2	1.3	2.0
	2	SIP-200 EOS FPGA P1	0.27	0.1
	2	SIP-200 EOS FPGA P450	1.211	0.45
	2	SIP-200 EOS FPGA P5	0.27	0.5
	2	SIP-200 EOS FPGA P550	1.211	0.55
	2	SIP-200 EOS FPGA P6	1.218	0.6
	2	SIP-200 EOS FPGA R2	1.22	2.0
	3	SIP-200 PEG TX FPGA P1	1.129	0.1
	3	SIP-200 PEG TX FPGA P6	1.131	0.6
	3	SIP-200 PEG TX FPGA R2	1.133	2.0
	4	SIP-200 PEG RX FPGA P1	1.3	0.1
	4	SIP-200 PEG RX FPGA P4	1.3	0.4
	4	SIP-200 PEG RX FPGA P6	1.3	0.6
	4	SIP-200 PEG RX FPGA R2	1.5	2.0
	5	SIP-200 ROMMON	1.3	0.1
SIP-400	1	SIP-400 ROMMON	1.3	0.1
	2	SIP-400 I/O FPGA	0.82	0.1
	3	SIP-400 SWITCH FPGA	0.39	0.1
SIP-600	1	SIP-600 ROMMON	1.3	0.1
	2	SIP-600 I/O FPGA	0.3	0.1
	3	SIP-600 PKT ENG FPGA	0.5	0.1
ESM20G (ES20 line cards)	1	ESM20G ROMMON	1.4	0.1
	2	ESM20G I/O FPGA	0.19	0.1
	3	ESM20G PKT ENG FPGA	0.5	0.1
	4	ESM20G 2x10GE LINK FPGA	0.9	0.1
	5	ESM20G 20x1GE LINK FPGA	0.6	0.1

Table 5 Release 12.2(33)SRB FPD Image Package Contents (continued)

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
SSC-600	1	SSC-600 I/O FPGA	1.0	0.3
	2	SSC-600 DP RX FPGA	1.1	0.3
	3	SSC-600 DP TX FPGA P3	0.12288	0.3
	3	SSC-600 DP TX FPGA P4	0.16384	0.4
	3	SSC-600 DP TX FPGA P5	1.3	0.5
	4	SSC-600 ROMMON	1.3	0.3
CWPA2	1	CWPA2 I/O FPGA P1	0.37	0.1
	1	CWPA2 I/O FPGA P7	0.39	2.0
	2	CWPA2 EOS FPGA P1	0.28	0.1
	2	CWPA2 EOS FPGA P7	0.48	2.0
	3	CWPA2 CPU0 ROMMON	1.3	0.1
	4	CWPA2 CPU1 ROMMON	1.3	0.1

FPD Image Package for Cisco IOS Release 12.2(33)SRA5

The FPD image package that is used to upgrade SPAs, SIPs, and FlexWAN modules on a router that runs Cisco IOS Release 12.2(33)SRA5 is the c7600-fpd-pkg.122-33.SRA5.pkg file. This FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com and is identical to the FPD package for Cisco IOS Release 12.2(33)SRA3.

FPD Image Package for Cisco IOS Release 12.2(33)SRA4

The FPD image package that is used to upgrade SPAs, SIPs, and FlexWAN modules on a router that runs Cisco IOS Release 12.2(33)SRA4 is the c7600-fpd-pkg.122-33.SRA4.pkg file. This FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com and is identical to the FPD package for Cisco IOS Release 12.2(33)SRA3.

FPD Image Package for Cisco IOS Release 12.2(33)SRA3

The FPD image package that is used to upgrade SPAs, SIPs, and FlexWAN modules on a router that runs Cisco IOS Release 12.2(33)SRA3 is the c7600-fpd-pkg.122-33.SRA3.pkg file. This FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com and is identical to the FPD package for Cisco IOS Release 12.2(33)SRA with the exceptions that are listed in Table 6.

Table 6 Release 12.2(33)SRA3 FPD Image Package Content Changes

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
1-port OC48 ATM SPA	1	KATM OC48 SPA IOFPGA	0.15	0
	2	SNOOP BUS FPGA	0.3	0

Table 6 Release 12.2(33)SRA3 FPD Image Package Content Changes (continued)

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
2-port IPsec SPA	1	PROM	1.1	0.1
	2	LODI	1.23	0.1
	3	Sequoia	1.1	0.1
SIP-400	1	SIP-400 ROMMON	1.3	0.1
	2	SIP-400 I/O FPGA	0.82	0.1
	3	SIP-400 SWITCH FPGA	0.39	0.1

FPD Image Package for Cisco IOS Release 12.2(33)SRA2

The FPD image package that is used to upgrade SPAs, SIPs, and FlexWAN modules on a router that runs Cisco IOS Release 12.2(33)SRA2 is the c7600-fpd-pkg.122-33.SRA2.pkg file. This FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com and is identical to the FPD package for Cisco IOS Release 12.2(33)SRA with the exceptions that are listed in Table 7.

Table 7 Release 12.2(33)SRA2 FPD Image Package Content Changes

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
1-port OC48 ATM SPA	1	KATM OC48 SPA IOFPGA	0.15	0
	2	SNOOP BUS FPGA	0.3	0
SIP-400	1	SIP-400 ROMMON	1.3	0.1
	2	SIP-400 I/O FPGA	0.82	0.1
	3	SIP-400 SWITCH FPGA	0.39	0.1

FPD Image Package for Cisco IOS Release 12.2(33)SRA1

The FPD image package that is used to upgrade SPAs, SIPs, and FlexWAN modules on a router that runs Cisco IOS Release 12.2(33)SRA1 is the c7600-fpd-pkg.122-33.SRA1.pkg file. This FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com and is identical to the FPD package for Cisco IOS Release 12.2(33)SRA with the exception that is listed in Table 8.

Table 8 Release 12.2(33)SRA1 FPD Image Package Content Changes

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
1-port OC48 ATM SPA	1	KATM OC48 SPA IOFPGA	0.15	0
	2	SNOOP BUS FPGA	0.3	0

FPD Image Package for Cisco IOS Release 12.2(33)SRA

The FPD image package that is used to upgrade SPAs, SIPs, and FlexWAN modules on a router that runs Cisco IOS Release 12.2(33)SRA is the c7600-fpd-pkg.122-33.SR.pkg file. This FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com. Table 9 shows the image packet contents for Release 12.2(33)SRA.

Table 9 Release 12.2(33)SRA FPD Image Package Contents

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0
	2	T3E3 SPA I/O FPGA	0.24	0
	3	T3E3 SPA E3 FPGA	1.4	0
	4	T3E3 SPA T3 FPGA	1.4	0
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0
	2	T3E3 SPA I/O FPGA	0.24	0
	3	T3E3 SPA E3 FPGA	1.4	0
	4	T3E3 SPA T3 FPGA	1.4	0
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.14
	1	CTE1 SPA ROMMON NP	2.12	0
	2	CTE1 SPA I/O FPGA	2.5	0
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.1
	2	CT3 SPA I/O FPGA	2.5	0.1
	3	CT3 SPA T3 FPGA R1	0.11	0.1
	3	CT3 SPA T3 FPGA R2	1.4	0.2
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.1
	2	CT3 SPA I/O FPGA	2.5	0.1
	3	CT3 SPA T3 FPGA R1	0.11	0.1
	3	CT3 SPA T3 FPGA R2	1.4	0.2
2-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0
	1	POS SPA IOFPGA P2	3.4	0.2
4-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0
	1	POS SPA IOFPGA P2	3.4	0.2
1-port OC12 POS SPA	1	POS SPA IOFPGA P1	3.4	0
	1	POS SPA IOFPGA P2	3.4	0.2
2-port OC-48 POS/SRP HH SPA	1	Multi-Port OC48 POS/RPR SPA FPD	1.0	0
4-port OC-48 POS/SRP HH SPA	1	Multi-Port OC48 POS/RPR SPA FPD	1.0	0
1-port OC-192 POS/SRP FH SPA	1	1-Port POS/RPR SPA IOFPGA P1	1.2	0

Table 9 Release 12.2(33)SRA FPD Image Package Contents (continued)

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
1-port OC-192 POS/SRP HH SPA	1	1-Port POS/RPR SPA IOFPGA P1	1.2	0
	1	1-Port POS/RPR SPA IOFPGA P2	1.2	2.0
1-port OC-48 POS/SRP HH SPA	1	1-Port POS/RPR SPA IOFPGA P2	1.2	0
2-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.24	0
4-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.24	0
1-port OC12 ATM SPA	1	KATM SPA IOFPGA	1.24	0
1-port OC48 ATM SPA	1	KATM OC48 SPA IOFPGA	0.14	0
	2	SNOOP BUS FPGA	0.3	0
10-port GE SPA	1	GE SPA FPGA	1.1	0
5-port GE SPA	1	GE SPA FPGA	1.1	0
2-port GE SPA	1	GE SPA FPGA	1.1	0
10-port GE V2 SPA	1	GE SPA FPGA	1.1	0
5-port GE V2 SPA	1	GE SPA FPGA	1.1	0
2-port GE V2 SPA	1	GE SPA FPGA	1.1	0
1-port 10GE SPA	1	10GE SPA FPGA	1.9	0
1-port 10GE V2 SPA	1	10GE SPA FPGA	1.9	0
4-port FE SPA V2	1	FE SPA FPGA	1.1	0
8-port FE SPA V2	1	FE SPA FPGA	1.1	0
2-port IPsec SPA	1	PROM	1.1	0.1
	2	LODI	1.21	0.1
	3	Sequoia	1.1	0.1
1-port Channelized STM1/OC3 SPA	1	STM1/OC3 SPA ROMMON	2.12	0
	2	STM1/OC3 SPA I/O FPGA	1.5	0
	3	STM1/OC3 SPA ET3 FPGA	1.4	0

Table 9 Release 12.2(33)SRA FPD Image Package Contents (continued)

Supported SPAs, SIPs, and FlexWAN modules	ID	Image Name	Image Version	Min. Required H/W Version
SIP-200	1	SIP-200 I/O FPGA P1	1.1	0.1
	1	SIP-200 I/O FPGA P4	1.1	0.4
	1	SIP-200 I/O FPGA P6	1.1	0.6
	2	SIP-200 EOS FPGA P1	0.27	0.1
	2	SIP-200 EOS FPGA P450	1.211	0.45
	2	SIP-200 EOS FPGA P5	0.27	0.5
	2	SIP-200 EOS FPGA P550	1.211	0.55
	2	SIP-200 EOS FPGA P6	1.218	0.6
	3	SIP-200 PEG TX FPGA P1	1.129	0.1
	3	SIP-200 PEG TX FPGA P6	1.131	0.6
	4	SIP-200 PEG RX FPGA P1	1.3	0.1
	4	SIP-200 PEG RX FPGA P4	1.3	0.4
	4	SIP-200 PEG RX FPGA P6	1.3	0.6
	5	SIP-200 ROMMON	1.3	0.1
SIP-400	1	SIP-400 ROMMON	1.3	0.1
	2	SIP-400 I/O FPGA	0.82	0.1
	3	SIP-400 SWITCH FPGA	0.29	0.1
SIP-600	1	SIP-600 ROMMON	1.3	0.1
	2	SIP-600 I/O FPGA	0.3	0.1
	3	SIP-600 PKT ENG FPGA	0.5	0.1
CWPA2	1	CWPA2 I/O FPGA P1	0.37	0.1
	1	CWPA2 I/O FPGA P7	0.39	2.0
	2	CWPA2 EOS FPGA P1	0.28	0.1
	2	CWPA2 EOS FPGA P7	0.48	2.0
	3	CWPA2 CPU0 ROMMON	1.3	0.1
	4	CWPA2 CPU1 ROMMON	1.3	0.1

Feature Support

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

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When

applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Note Feature set tables are not included in the Cisco IOS Release 12.2SR release notes to improve the usability of the release notes documentation. The feature-to-image mapping will be 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 unique to each software release and the features that the releases have in common.

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

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

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

http://www.cisco.com/support/FeatureNav/FNFAQ.html

Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.2SR support a specific feature, go to the Cisco Feature Navigator home page and perform the following steps.

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

Step 2 To find a feature, 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 Select 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 additional 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 **12.2SR**.

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

Step 7 From the Platform drop-down menu, select the appropriate hardware platform. The "Search Results" table will list all the software images (feature sets) that support the feature(s) that you selected.

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

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.2SR, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Compare Images**, and then **Search by Release**.

Step 2 In the "Find the features in a specific Cisco IOS release, using one of the following methods:" area, select **12.2SR** from the Cisco IOS Major Release drop-down menu.

Step 3 Click **Continue**.

Step 4 From the Release drop-down menu, select the appropriate maintenance release.

Step 5 From the Platform drop-down menu, select the appropriate hardware platform.

Step 6 From the Feature Set drop-down menu, select the appropriate feature set. The "Search Results" table will list all the features that are supported by the feature set (software image) that you selected.

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 12.2SR and contains the following subsections:

Note These release notes are not cumulative and list only features that are new to Cisco IOS Release 12.2SR, which is based on Release 12.2, Release 12.2S, Release 12.2SB, and Release 12.2SX. For information about inherited features, go to Cisco.com or Cisco Feature Navigator. For Cisco.com, either go to Cisco.com and select the appropriate software release under Products and Service and IOS Software, or go to http://www.cisco.com/univercd/home/index.htm and select the appropriate software release under Cisco IOS Software and Release Notes. You can use the Cisco Feature Navigator tool at http://www.cisco.com/go/cfn.

Note For extensive information about all supported hardware in Cisco IOS Release 12.2SR, see the *Guide to Supported Hardware for Cisco 7600 Series Routers with Release 12.2SR*.

New Hardware Features in Cisco IOS Release 12.2(33)SRC

This section describes new and changed features in Cisco IOS Release 12.2(33)SRC. Some features may be new to Cisco IOS Release 12.2SR 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 12.2(33)SRC. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included in this section. If a feature listed in this section 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 in this section.

Cisco 7201 Router

The Cisco 7201 router is a Cisco 7200 router with a NPE-G2 engine in a 1RU fixed configuration form factor. This is the next generation Cisco 7301 that is equipped with four built-in Gigabit Ethernet (GE) ports and a port adapter (PA) slot.

CT3 CEoP on Cisco 7600-SIP-400

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

PA-MC-T3-EC and PA-MC-2T3-EC

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

http://www.cisco.com/en/US/products/hw/modules/ps2033/products_module_installation_guide_chapter09186a0080796f7f.html

Port Adapter Enhancements—2 New Clear Channel Port Adapters and Channelized PA Hardware Acceleration of MLPPP/MLFR/LFI/FRF12

For detailed information about these feature, see the following documents:

- PA-T3/E3-EC Port Adapter Installation and Configuration at

  http://www.cisco.com/en/US/products/hw/modules/ps2033/products_module_installation_guide_book09186a008085de57.html
- PA-MC-T3-EC Port Adapter Installation and Configuration at

  http://www.cisco.com/en/US/products/hw/modules/ps2033/products_module_installation_guide_book09186a0080796e92.html

RSP720-3C-10GE

The Cisco 7600 Series RSP 720-10GE is introduced on Cisco IOS 12.2(33)SRC on a limited orderability basis. For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_book09186a0080800de5.html

RSP720-3CXL-10GE

The Cisco 7600 Series RSP 720-10GE is introduced on Cisco IOS 12.2(33)SRC on a limited orderability basis. For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_book09186a0080800de5.html

Service and Application Module for IP

The Cisco Service and Application Module for IP (SAMI) is a new-generation high performance Cisco IOS software application module that occupies a single slot in the Cisco 7600 series router platform.

With an IXP2800 network processor flow-distributor running at 1.4GHz, and six PowerPCs (PPCs) running at 1.25GHz, each of which can run an instance of the same Cisco IOS image, the SAMI offers a parallel architecture for Cisco IOS mobile wireless applications.

The benefits of the SAMI architecture include the following:

- Increased processing power and session density
- Reduced inter-CPU data sharing
- Separation of the control plane and the data plane
- Improved management capabilities
- Less complex configuration
- Easier debugging

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

http://www.cisco.com/en/US/products/hw/modules/ps5510/products_installation_and_configuration_guide_book09186a0080875d19.html

SFP-GE-T Support

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109a7.html

Shared Port Adapters

Cisco IOS Release 12.2(33)SRC introduces support for the following new shared port adapters (SPAs):

- Cisco 8-Port Channelized T1/E1 Shared Port Adapter (SPA-8XCHT1/E1)

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

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/sipspasw/index.htm
- Cisco Channelized T3 to DS0 Shared Port Adapter (SPA-2XCT3/DS0, SPA-4XCT3/DS0)

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

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109a7.html

- Cisco Clear Channel T3/E3 Shared Port Adapter (SPA-2XT3/E3, SPA-4XT3/E3)

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

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109a7.html

- SPA-1X10GE-L-V2

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

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

- SPA-1xCHSTM1/OC3

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

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109a7.html

WiSM Support on Cisco 7600 Platform

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

http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78_17121.html

WS-X6708-10G-3C, WS-X6708-10G-3CXL

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

New Software Features in Cisco IOS Release 12.2(33)SRC

This section describes new and changed features in Cisco IOS Release 12.2(33)SRC. Some features may be new to Cisco IOS Release 12.2SR 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 12.2(33)SRC. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included in this section. If a feature listed in this section 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 in this section.

32K EVC Scale

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a00807e5826.html

7600 VRF-Aware Lawful Intercept

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a00807e0acb.html

802.1P CoS—PPP & PPPoE Control Frames

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

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

ACFC and PFC Support on Multilink Interface on 7600/EnhancedFlexWAN/SIP200

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

AToM Tunnel Selection

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

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

Attribute Filtering Per-Domain and VRF Aware Framed-Routes

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

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

Attribute Screening for Access Requests

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

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

Authentication, Authorization, and Accounting (AAA) Features

Cisco IOS Release 12.2(33)SRC introduces support for the following AAA features.

- AAA Authorization and Authentication Cache

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

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_aaa_auth_cache.html
- AAA CLI Stop Record Enhancement

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

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

- AAA Double Authentication Secured by Absolute Timeout

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

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_aaa_double_auth.html
- AAA High Availability Support for Local PPPoX Sessions

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

  http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha_aaa_pppox.html
- AAA Interim Accounting

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

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_accountg.html
- AAA Method Lists Enhancement

  The number of method lists that can be configured has been increased from 8 to 250.
- AAA Per-User Scalability

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

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_authentifcn.html
- AAA Session MIB

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

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_accountg.html
- AAA-PPP-VPDN Non-Blocking

  Cisco IOS software created a statically configurable number of processes to authenticate calls. Each process would handle a single call, but in some situations the limited number of processes could not keep up with the incoming call rate. This resulted in some calls timing out. The AAA-PPP-VPDN Non-Blocking feature changes the software architecture such that the number of processes do not limit the rate of call handling.

BFD—VRF Support

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

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bfd.html

BFD—WAN Interface Support (STM, FR, POS, and Serial)

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

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bfd.html

BGP Per Neighbor Graceful Restart Configuration

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

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_adv_features.html

Call Home

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a00 80685955.html

Calling Station ID Attribute 31

The **radius-server attribute 31** command is a new command in Cisco IOS Release 12.2(31)SB2. This new command replaces the **radius-server attribute 31 remote-id** command, which was introduced in Release 12.2(28)SB. The new command adds two new keywords, **mac** and **send**, and includes the **remote-id** keyword from the original **radius-server attribute 31 remote-id** command.

Cisco Express Forwarding—SNMP CEF-MIB Support

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

http://www.cisco.com/en/US/docs/ios/ipswitch/configuration/guide/cef_snmp_mib.html

Cisco IOS Scripting with Tcl

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

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

CISCO-DATA-COLLECTION-MIB

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

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

CISCO-IP-URPF-MIB Support

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

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

CNS—Interactive CLI

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

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

CNS Config Retrieve Enhancement with Retry and Interval

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

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

Command Scheduler (Kron) Policy for System Startup

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

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

Config Change Tracking Identifier

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

Configuration Enhancements for Broadband Scalability

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

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

Configuration Generation Performance Enhancement

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

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/config_cache.html

Connect-Info RADIUS Attribute 77

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

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_rad_77_connect.html

Connection Accounting

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

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

CoPP Enhancements on SIP-400

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

Dynamic Host Configuration Protocol Features

Cisco IOS Release 12.2(33)SRC introduces support for the following Dynamic Host Configuration Protocol (DHCP) features.

DHCP—DHCP Server MIB

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_mib.html

DHCP—DHCPv6 Relay Agent Notification for Prefix Delegation

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

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

DHCP—Server Multiple Subnet

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_svr_cfg.html

DHCP—Static Mapping

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_svr_cfg.html

DHCP—Statically Configured Routes Using a DHCP Gateway

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_svr_cfg.html

DHCP Authorized ARP

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_acct_sec.html

DHCP ODAP Server Support

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_sod_apm.html

DHCP On Demand Address Pool (ODAP) Manager for Non-MPLS VPN Pools

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_sod_apm.html

DHCP Per Interface Lease Limit and Statistics

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_acct_sec.html

DHCP Relay—MPLS VPN Support

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rly_agt.html

DHCP Relay Option 82—Per Interface Support

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rly_agt.html

DHCP Release and Renew CLI in EXEC Mode

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_client.html

DHCP Secured IP Address Assignment

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_acct_sec.html#wp1094512

DHCP Server—On Demand Address Pool Manager

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_sod_apm.html

DHCP Server Import All Enhancement

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_svr_cfg.html

DHCPv6—Relay—Reload Persistent Interface ID Option

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

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

DHCPv6 Ethernet Remote ID Option

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

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

Digital Optical Monitoring

The Digital Optical Monitoring (DOM) feature allows you to display transceiver operating conditions, such as temperature and power levels, while the transceiver is in service. Use the **show interfaces transceiver** command to display operating conditions.

Dynamic Per VRF AAA

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

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

Embedded Syslog Manager (ESM)

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

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

Encrypted Vendor-Specific Attributes

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

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

Enhanced Test Command

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

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

EtherChannel Load Distribution

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

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

EVC PortChannel on ESM-20

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a00807e5826.html

Extended NAS-Port-Type and NAS-Port Support

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

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

FHRP—HSRP Group Shutdown

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

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html

Framed-Route in RADIUS Accounting

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

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

Hot Fabric Sync

The switch fabric module functionality is built into the Supervisor Engine 720 and the RSP720. When a supervisor engine switchover occurs, a fabric switchover also occurs. During this process, the line cards must resynchronize with the new active switch fabric. The Hot Fabric Sync feature, which is enabled by default, keeps both the active and standby fabric in sync at the same time, minimizing the switchover time and thereby minimizing any impact on switch fabric traffic. To verify the fabric sync status of active and standby supervisors, enter the **show fabric status** command.

This feature is supported on the following chassis: Cisco 7603-S, Cisco 7604, Cisco 7606-S, and Cisco 7609-S. All WAN modules with DFC, SIP-200, SIP-400, and WS-67xx with DFC or CFC are supported.

HTTP TACACS+ Accounting Support

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

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

H-VPLS N-PE Redundancy for MPLS Access

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

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

H-VPLS N-PE Redundancy for QinQ Access

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

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

IEEE 802.1x with DHCP

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a00880685955.html

IMA on SIP-400 for 24xT1/E1 CEOP and 1xOC3 CEOP SPAs

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

IP SLAs for MPLS Pseudo Wire (PWE3) via VCCV

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

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

IP Version 6 Features

Cisco IOS Release 12.2(33)SRC introduces support for the following IP version 6 (IPv6) features.

IPv6—CNS Agents

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

IPv6—Config Logger

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

IPv6—HTTP(S)

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

IPv6—IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)

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

IPv6—Netconf

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

IPv6—SOAP

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

IPv6—Tcl

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

Intelligent Service Gateway Features

Cisco IOS Release 12.2(33)SRC introduces support for the following ISG features.

ISG: Network Interface: IP Routed, VRF-Aware MPLS

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

ISG: Policy Control: Policy Server: SSG-SESM Protocol

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

ISG: Policy Control: Service Profiles

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

ISG: Accounting: Per Session, Service, and Flow

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

ISG: Accounting: Postpaid

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

ISG: Authentication: DHCP Option 82 Line ID—AAA Authorization Support

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

ISG: Flow Control: Flow Redirect (L4, Captive Portal)

For detailed information about this feature, see the following document:
http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/isg_l4_redirect.html

ISG: Instrumentation: Advanced Conditional Debugging

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

ISG: Instrumentation: Session and Flow Monitoring (Local and External)

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

ISG: Policy Control: DHCP Proxy

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

ISG: Policy Control: Multidimensional Identity per Session

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

ISG: Policy Control: Policy Server: CoA (QoS, L4 Redirect, User ACL, TimeOut)

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

ISG: Policy Control: Policy Server: CoA ASCII Command Code Support

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

ISG: Policy Control: Policy: Domain-Based (Auto-Domain, Proxy)

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

ISG: Policy Control: Policy: Triggers (Time, Volume, Duration)

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

ISG: Policy Control: User Profiles

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

ISG: Session: Auth: PBHK

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

ISG: Session: Auth: Single Sign On

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

ISG: Session: Authentication (MAC, IP, EAP)

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

ISG: Session: Creation: Interface IP Session: L2

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

ISG: Session: Creation: Interface IP Session: L3

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

ISG: Session: Creation: IP Session: Protocol Event (DHCP,RADIUS)

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

ISG: Session: Creation: IP Session: Subnet and Source IP: L2

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

ISG: Session: Creation: IP Session: Subnet and Source IP: L3

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

ISG: Session: Creation: P2P Session (PPPoE, PPPoXoX)

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

ISG: Session: LifeCycle: Idle Timeout

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

ISG: Session: LifeCycle: POD

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

ISG: Session: VRF Transfer

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

ISG: Session: Protection and Resiliency: Keepalive—ARP, ICMP

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

In-Service Software Upgrade (ISSU)

Cisco IOS Release 12.2(33)SRC and later releases support the following ISSU features:

- ISSU—AToM ATM Attachment Circuit
- ISSU—AToM FR/MFR Attachment Circuit
- ISSU—AToM HDLC Attachment Circuit

For detailed information about these features, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_trnsprt_mlps_atom.html#wp1115583

- ISSU—DHCP ODAP Client/Server
- ISSU—DHCP Proxy Client
- ISSU—DHCP Relay on Unnumbered Interface
- ISSU—DHCP Server

For detailed information about these features, see the following document:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp-sso_ha.html

- ISSU—PPPoE

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

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

- ISSU—Virtual Private LAN Service (VPLS)

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

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

- ISSU—Virtual Template Manager

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

http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha_inserv_updg.html

- ISSU—VRRP

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

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_vrrp.html

KEOPS Phase 2 Access Circuit Redundancy with Local Switching

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

LACP 1-1 Redundancy with Fast Switchover

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a0080685955.html

LACP Fast Rate

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

http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_book.html

LACP Single Fault Direct Load Balance Swap

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

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

Layer 2 Tunneling Protocol Version 3

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

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_l2_tun_pro_v3.html

Local AAA Server

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

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

Message Banners for AAA Authentication

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

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

MPLS EM—MPLS VPN MIB RFC4382 Upgrade

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

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_em_vpn_mib_4382.html

Multiprotocol Label Switching Label Distribution Protocol Features

Cisco IOS Release 12.2(33)SRC introduces support for the following Multiprotocol Label Switching Label Distribution Protocol (MPLS LDP) features.

MPLS LDP—Local Label Allocation Filtering

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

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

MPLS LDP—Lossless MD5 Session Authentication

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

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_lossless_md5.html

MPLS Pseudowire Status Signaling

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

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

Multiprotocol Label Switching Traffic Engineering Features

Cisco IOS Release 12.2(33)SRC introduces support for the following Multiprotocol Label Switching Traffic Engineering (MPLS TE) features.

MPLS TE—BFD-Triggered Fast Reroute (FRR)

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

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

MPLS TE—Bundled Interface Support (EtherChannel and MLPPP)

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

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

MPLS TE—Tunnel-Based Admission Control (TBAC)

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

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

MPLS TE—Fast Reroute Path Protection

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

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

Multiprotocol Label Switching Virtual Private Network Features

Cisco IOS Release 12.2(33)SRC introduces support for the following Multiprotocol Label Virtual Private Network (MPLS VPN) features.

MPLS VPN—Inter-AS Option AB

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

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

MPLS VPN Half Duplex VRF (HDVRF)

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

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

MPLS VPN PE-CE Link Protection

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

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

MQC—Traffic Shaping Overhead Accounting for ATM

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

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

Multicast VPN Extranet Support

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

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

NAS-Port Format E

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

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

NAS-Port ID Format C Enhancement

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

http://www.cisco.com/en/US/products/ps6566/products_feature_guide09186a0080792993.html

Network Accounting (RADIUS/TACACS+)

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

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

Nonstop Forwarding Stateful Switchover Features

Cisco IOS Release 12.2(33)SRC introduces support for the following Nonstop Forwarding (NSF) Stateful Switchover (SSO) features.

NSF/SSO—AToM ATM Attachment Circuit

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

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_trnsprt_mlps_atom.html#wp1115583

NSF/SSO—AToM FR/MFR Attachment Circuits

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

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_trnsprt_mlps_atom.html#wp1115583

NSF/SSO—AToM HDLC Attachment Circuit

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

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_trnsprt_mlps_atom.html#wp1115583

NSF/SSO—Virtual Private LAN Services

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

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

Offload Server Accounting Enhancement

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

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

OSPF Graceful Shutdown

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

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_ospf_ttl.html

OSPF TTL Security Check

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

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_ospf_ttl.html

OSPFv2 Local RIB

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

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_ospf_local_rib.html

OSPFv3 Fast Convergence—LSA and SPF Throttling

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

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

Per Session Queuing and Shaping for PPPoEoVLAN Using RADIUS

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

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

Per Subinterface MTU for Ethernet over MPLS (EoMPLS)

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

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

Per VRF AAA

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

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

Per-Session QoS

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

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

Per-User Access-List

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

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

Per-User QoS via AAA Policy Name

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

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

PPP MLP MRRU Negotiation Configuration

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

http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_pppmlp_mrru_neg.html

PPP-Max-Payload and IWF PPPoE Tag Support

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

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

PPPoE Support

Cisco IOS Release 12.2(33)SRC introduces support for the following PPPoE features.

PPPoE—QinQ Support

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

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

PPPoE—Session Limiting on Inner QinQ VLAN

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

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

PPPoE Agent Remote ID and DSL Line Characteristics Enhancement

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

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

PPPoE Circuit-ID Tag Processing

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

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

PPPoE Connection Throttling

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

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

PPPoE on Ethernet

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

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

PPPoE over Gigabit Ethernet Interface

The PPPoE over Gigabit Ethernet feature enhances PPP over Ethernet (PPPoE) functionality by adding support for PPPoE and PPPoE over IEEE 802.1Q VLANs on Gigabit Ethernet interfaces.

PPPoE over VLANs Scaling and PPPoE over VLANs Forwarding over PVC

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

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

PPPoE RADIUS Port Identification

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

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

PPPoE Service Selection

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

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

PPPoE Session Count MIB

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

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

PPPoE Session Limit

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

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

PPPoE Session Limit per NAS Port

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

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

PPPoE Session Recovery After Reload

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

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

PPPoE Tag Support with Agent Remote ID Field

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

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

PPPoEoE on SIP-400

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

Programmable BERT Patterns Enhancement on Channelized SPAs

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

QoS: Tunnel Marking for GRE Tunnels

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

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

RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

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

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_rad_5_pre_serv.html

RADIUS Attribute 52 and 53 Gigaword Support

The RADIUS Attribute 52 and Attribute 53 Gigaword Support feature introduces support for Attribute 52 (Acct-Input-Gigawords) and Attribute 53 (Acct-Output-Gigawords) in accordance with RFC 2869. Attribute 52 keeps track of the number of times the Acct-Input-Octets counter has rolled over the 32-bit integer throughout the course of the provided service; attribute 53 keeps track of the number of times the Acct-Output-Octets counter has rolled over the 32-bit integer throughout the delivery of service. Both attributes can be present only in Accounting-Request records where the Acct-Status-Type is set to “Stop” or “Interim-Update.” These attributes can be used to keep accurate track of and bill for usage.

RADIUS Attribute 77 for DSL

The RADIUS Attribute 77 for DSL feature introduces support for attribute 77 (Connect-Info) to carry the textual name of the virtual circuit class associated with the given permanent virtual circuit (PVC). (Although attribute 77 does not carry the unspecified bit rate (UBR), the UBR can be inferred from the classname used if one UBR is set up on each class.) Attribute 77 is sent from the network access server (NAS) to the RADIUS server via Accounting-Request and Accounting-Response packets.

RADIUS Attribute Value Screening

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

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

RADIUS Centralized Filter Management

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

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

RADIUS DNIS Screening, RADIUS Packet of Disconnect (POD), ISDN Guard Timer

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

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

RADIUS Logical Line ID

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

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

RADIUS NAS-IP-Address Configurability

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

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

RADIUS Per-VRF Server Group

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

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

RADIUS Progress Codes

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

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

RADIUS Push for MOD CLI Policies

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

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

RADIUS Route Download

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

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

RADIUS Server Load Balancing

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

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

RADIUS Server Reorder on Fail

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

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

Retransmit Counter for Exponential Backoff Accounting

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

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

RFC 4293 IP-MIB (IPv6 Only) and RFC 4292 IP-FORWARD-MIB (IPv6 Only)

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

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

RSVP Aggregation

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

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

SIP-400 Accelerated Lawful Intercept

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a00807e0acb.html

SLB (Server Load Balancing)

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

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_slb.html

SLB: KAL-AP Agent Support

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

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_slb.html

SLB: RADIUS Loadbalancing Accelerated Data Plane Forwarding

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

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_slb.html

Source IPv4 and Source MAC Address Binding

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

SPAN Destination Port Support on Etherchannels

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a0080685955.html

SPAN Egress Session Increase

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a0080685955.html

SSO—BFD (Admin Down)

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

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bfd.html

SSO—DHCP ODAP Client/Server

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp-sso_ha.html

SSO—DHCP Proxy Client

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

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp-sso_ha.html

SSO—PPPoE

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

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

SSO—Virtual Template Manager

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

http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-stfl_swovr.html

SSO—VRRP

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

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_vrrp.html

Static Routes for BFD

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

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bfd.html

Sticky IP

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

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_rad_8_accss_req.html

Subscriber Service Switch

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

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

Switch Port Analyzer (SPAN)—Input Packets with Don't Learn Option

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a00
80685955.html

TDM Local Switching

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

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guide
s_book09186a00802109bf.html

Throttling of AAA (RADIUS) Records

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

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

VPLS MAC Address Withdrawal

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

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

VTP v3

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

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a00080685955.html

New Hardware Features in Cisco IOS Release 12.2(33)SRB1

This section describes new and changed features in Cisco IOS Release 12.2(33)SRB1. Some features may be new to Cisco IOS Release 12.2SR 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 12.2(33)SRB1. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included in this section. If a feature listed in this section 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 in this section.

New Small-Form Factor Chassis

Cisco IOS Release 12.2(33)SRB1 introduces support for the following new routers:

Cisco 7603-S Router

For detailed information about the small-form factor Cisco 7603-S (CISCO7603-S), see the *Cisco 7600 Series Router Installation Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_chapter09186a008007c8bb.html

Cisco 7606-S Router

For detailed information about the small-form factor Cisco 7603-6 (CISCO7606-S), see the *Cisco 7600 Series Router Installation Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_chapter09186a008007c8bb.html

New Software Features in Cisco IOS Release 12.2(33)SRB1

This section describes new and changed features in Cisco IOS Release 12.2(33)SRB1. Some features may be new to Cisco IOS Release 12.2SR 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 12.2(33)SRB1. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included in this section. If a feature listed in this section 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 in this section.

1 Rate 2 Color per EVC Policer

For detailed information about this feature, see the "Configuring QoS on the Cisco 7600 Series Ethernet Services 20G Line Card" chapter in the *Cisco 7600-ES20 Ethernet Line Card Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f8d.html

AToM Support over GRE

For detailed information about this feature, see the "Configuring the Fast Ethernet and Gigabit Ethernet SPAs" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

ATM Pseudowire Redundancy

For detailed information about this feature, see the *L2VPN Pseudowire Redundancy* document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a0080606811.html

Backup Interface for Flexible UNI

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

- The "Configuring the Cisco 7600 Series Ethernet Services 20G Line Card" chapter in the *Cisco 7600-ES20 Ethernet Line Cards Configuration Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f97.html
- The "Configuring the Fast Ethernet and Gigabit Ethernet SPAs" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080523f3c.html

Enhanced Fast Software Upgrade (eFSU)

The Enhanced Fast Software Upgrade (eFSU) feature was introduced in Cisco 12.2(33)SRB. Cisco IOS Release 12.2(33)SRB1 adds support for the Route Switch Processor 720 (RSP720). For detailed information about this feature, see the "ISSU and eFSU on Cisco 7600 Series Router" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 12.2SR*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f1c85.html

In-Service Software Upgrade (ISSU)

Cisco IOS Release 12.2(33)SRB1 and later releases support the following ISSU features:

- MPLS OAM
- MPLS LDP

- MPLS TE
- MPLS VPN

For detailed information about these features, see the following document:

http://cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/iscli28.htm

- L2 Multicast
- EtherChannel
- IEEE 802.1x
- IPv4 ISSU
- MPLS
- Netflow
- SPAN and Remote SPAN
- STP

For detailed information about these features, see the "ISSU and eFSU on Cisco 7600 Series Router" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 12.2SR*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f1c85.html

- ARP
- ATM
- Frame Relay
- HDLC
- PPP/MLP
- QoS
- RIB/VRF
- SNMP

For detailed information about these features, see *Cisco IOS In Service Software Upgrade Process*:

http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a00807c9105.html

- MTR

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srmtrdoc.htm#wp1063633

- GLBP

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/glbpissu.htm

- HSRP

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/hsrpissu.htm

- IS-IS

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sbisissu.htm

IP SLAs Features

Cisco IOS IP SLAs features provide the capability to verify service guarantees, increase network reliability by validating network performance, proactively identify and alert users about network issues or deviations, and increase Return on Investment (ROI) by easing the deployment of new IP services. Cisco IOS IP SLAs use active probing techniques for end-to-end quantitative measurement of network performance, health, and connectivity for Voice over IP (VoIP), Multiprotocol Label Switching (MPLS), and TCP/IP networks. The IP SLAs features are also directly integrated with other Cisco IOS products such as Optimized Edge Routing (OER), Enhanced Object Tracker (EoT), and Embedded Event Manager (EEM).

Cisco IOS Release 12.2(33)SRB1 and later releases support the following IP SLAs features:

- IP SLAs - DHCP Operation
- IP SLAs - Distribution of Statistics
- IP SLAs - DNS Operation
- IP SLAs - FTP Operation
- IP SLAs - HTTP Operation
- IP SLAs - ICMP Echo Operation
- IP SLAs - ICMP Path Echo Operation
- IP SLAs - MPLS VPN Aware
- IP SLAs - Multi-Operation Scheduler
- IP SLAs - One-way Measurements
- IP SLAs - Path Jitter
- IP SLAs - Reaction Threshold
- IP SLAs - Scheduling
- IP SLAs - TCP Connect Operation
- IP SLAs - UDP Echo Operation
- IP SLAs - UDP Jitter Operation
- IP SLAs - UDP VoIP Operation
- IP SLAs - VoIP Threshold Traps

Cisco IOS IP SLAs configuration information is included in the *Cisco IOS IP SLAs Configuration Guide, Release 12.4T*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tsla_c/index.htm

Cisco IOS IP SLAs command reference information is included in the *Cisco IOS IP SLAs Command Reference, Release 12.2SR*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/srsla_r/index.htm

MPLS VPN 6VPE Support over IP Tunnels

For detailed information about this feature, see the "Implementing IPv6 VPN over MPLS (6VPE)" chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00807d26c0.html#wp1049404

MTU Support on MLP Interfaces

For detailed information about this feature, see the "Configuring the SIPs and SSC" chapter in the in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

Multi-VRF Selection using Policy Based Routing (PBR)

The Multi-VRF Selection using Policy Based Routing (PBR) feature allows a specified interface on a provider edge (PE) router to route packets to Virtual Private Networks (VPNs) based on match criteria defined in an Internet Protocol (IP) access list or based on packet length.

Out of Band Clocking

For detailed information about this feature, see the "Configuring the CEoP and Channelized ATM SPAs" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guid*e:

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a00807f9ea0.html

Session Border Controller

For detailed information about this feature, see the *Cisco 7600 Series Routers Session Border Controller Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00808565c1.html

New Hardware Features in Cisco IOS Release 12.2(33)SRB

This section describes new and changed features in Cisco IOS Release 12.2(33)SRB. Some features may be new to Cisco IOS Release 12.2SR 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 12.2(33)SRB. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included in this section. If a feature listed in this section 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 in this section.

New Chassis and Power Supply

Cisco IOS Release 12.2(33)SRB introduces support for the following chassis and power supply:

- Enhanced 9-Slot CISCO7609 Chassis: CISCO7609-S
  For detailed information about this chassis, see the *Cisco 7600 Series Router Installation Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_chapter09186a008007c8bb.html
- PWR-6000-DC
  For detailed information about this power supply, see the *Cisco 7600 Series Router Installation Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_chapter09186a008007c8bb.html

New Line Cards

Cisco IOS Release 12.2(33)SRB introduces support for the following line cards:

- Distributed Forwarding Cards 3CXL:
  - Distributed Forwarding Card 3CXL (DFC3CXL) for use on CEF720 modules: WS-F6700-DFC3CXL
  - Distributed Forwarding Card 3C (DFC3C) for use on CEF720 modules: WS-F6700-DFC3C

  For detailed information about these line cards, see the *Guide to Supported Hardware for Cisco 7600 Series Routers with Cisco IOS Release 12.2SR*:

  http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_chapter09186a008069bb90.html
- Ethernet Services (7600 ES20) Line Cards
  - 2-port version Ethernet Services (7600 ES20) Line Card: 7600-ES20-10G
  - 20-port Ethernet Services (7600 ES20) Line Card: 7600-ES20-GE

  For detailed information about these line cards, see the *Cisco 7600 Series Ethernet Services 20G Line Card Hardware Installation Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_chapter09186a00807f388c.html

New Modules

Cisco IOS Release 12.2(33)SRB introduces support for the following module:

- Application Control Engine Service Module

  For detailed information about this module, see the *Cisco Application Control Engine Module Installation Note*:

  http://www.cisco.com/en/US/products/hw/switches/ps708/prod_module_installation_guide09186a0080626334.html

New Route Switch Processors

Cisco IOS Release 12.2(33)SRB introduces support for the following Route Switch Processors (RSPs):

- RSP720-3C-GE
- RSP720-3CXL-GE

For detailed hardware information about these RSPs, see the "Route Switch Processors and Supervisor Engines" chapter in the *Cisco 7600 Series Router Supervisor Engine and Route Switch Processor Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/supeng/supe02.htm

For software configuration information and new feature descriptions, see the "Configuring a Route Switch Processor 720" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 12.2SR*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f1d89.html

New SPAs

Cisco IOS Release 12.2(33)SRB introduces support for the following shared port adapters (SPAs):

- Circuit Emulation over Packet (CEoP) SPAs, supported on the SIP-400:
  - 1-port channelized OC-3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM)
  - 24-port channelized T1/E1/J1 ATM CEoP SPA (SPA-24CHT1-CE-ATM)

  For detailed information about the CEoP SPA, see the "Overview of the CEoP and Channelized ATM SPAs" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

  http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a00807fa016.html
- SPA-2x1GE-V2, supported on the SIP-400

  For detailed information about the SPA-2x1GE-V2, see the "Overview: Cisco 7600 Series Router Shared Port Adapters" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Hardware Installation Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008043f6a6.html

Note The SPA-5x1GE-V2 was introduced in Cisco IOS Release 12.2(33)SRA for the SIP-600. Release 12.2(33)SRB adds support for the SPA-5x1GE-V2 on the SIP-400. For detailed information about the SPA-5x1GE-V2, see the "Overview: Cisco 7600 Series Router Shared Port Adapters" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Hardware Installation Guide*:
http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008043f6a6.html

New Software Features in Cisco IOS Release 12.2(33)SRB

This section describes new and changed features in Cisco IOS Release 12.2(33)SRB. Some features may be new to Cisco IOS Release 12.2SR 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 12.2(33)SRB. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included in this section. If a feature listed in this section 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 in this section.

1024 MLP Bundles

The number of MLP bundles that are supported on a SIP-200 has been increased from 256 to 1024.

For detailed information about the SIP-200, see the "Overview of the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008044013b.html

Alarm Filtering Support in the Cisco Entity Alarm MIB

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t4/nmhtalrm.htm

Any Transport over MPLS Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Any Transport over MPLS (AToM) features.

- Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: Packed Cell Relay
- Any Transport over MPLS (AToM) Graceful Restart
- Any Transport over MPLS (AToM): Ethernet over MPLS (EoMPLS)
- Any Transport over MPLS (AToM): Frame Relay over MPLS (FRoMPLS)
- Any Transport over MPLS (AToM): Static Pseudowire Provisioning
- Any Transport over MPLS (AToM): Tunnel Selection

For detailed information about the above-mentioned AToM features with the exception of the Any Transport over MPLS (AToM) Graceful Restart feature and the Any Transport over MPLS (AToM): Tunnel Selection feature, see the *Any Transport over MPLS* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/fsatom28.htm

For detailed information about the Any Transport over MPLS (AToM) Graceful Restart feature, see the *AToM Graceful Restart* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fsgratom.htm

For detailed information about the Any Transport over MPLS (AToM): Tunnel Selection feature, see the *Any Transport over MPLS (AToM): Tunnel Selection* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srtunsel.htm

Bandwidth-Based Local Call Admission Control (CAC) Policy for IP Multicast

For detailed information about this feature, see the *Per Interface Mroute State Limit with Bandwidth Based CAC for IP Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srmcac.htm

Bidirectional Forwarding Detection Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Bidirectional Forwarding Detection (BFD) features.

- BFD Echo Mode
- Bidirectional Forwarding Detection (BFD) Standard Implementation
- BFD Version 1 Support

For detailed information about these features, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fs_bfd.htm

Border Gateway Protocol Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Border Gateway Protocol (BGP) features.

BGP Neighbor Policy

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbgpnp.htm

BGP Per Neighbor SOO Configuration

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/htbgpsoo.htm

BGP Route-Map Continue Support for Outbound Policy

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbgprco.htm

BGP Selective Address Tracking

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbgpsn.htm

BGP Support for MTR

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbgpmtr.htm

BGP Support for the L32VPN Address Family

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbgpl2v.htm

BITS Clock Support - Receive and Distribute

For detailed information about this feature, see the "Configuring the CEoP and Channelized ATM SPAs" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a00807f9ea0.html

CNS Image Agent

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbcnsia.htm

Compact Generic Attribute Registration Protocol (cGVRP)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbcgvrp.htm

Configuration Partitioning

The Configuration Partitioning feature provides modularization ("partitioning") of the running configuration state to provide granular access to the running configuration in Cisco IOS software. This feature is enabled by default in Cisco IOS software images that include this feature.

The Configuration Partitioning feature allows the system to group the configuration state of the device into parts (called "partitions") so that only the configuration state the user wishes to review is retrieved when a user issues the **show running-config partition** *part* command. This feature improves performance for high-end systems with complex configurations because only a part of the running configuration state is processed when generating the running configuration command list, as opposed to the existing method of processing the entire system configuration state.

Default configuration partitions are provided by the introduction of this feature; other Cisco IOS software features may define their own command partitions in later releases.

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/cnfprts.htm

Connectivity Fault Management-2

The Connectivity Fault Management-2 (CFM-2) feature consists of the following features.

802.1ag and 802.3ah Interworking

For detailed information about this feature, see the *Ethernet Connectivity Fault Management* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/srethcfm.htm

Configuring Ethernet Local Management Interface on a Provider Edge Device

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbpelmi.htm

Ethernet Local Management Interface

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t9/htethlmi.htm

IEEE 802.3ad Link Bundling

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sbcelacp.htm

Outward Facing MEP

For detailed information about this feature, see the *Ethernet Connectivity Fault Management* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/srethcfm.htm

Control Plane DSCP Support for RSVP

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/dscprsvp.htm

Disk File System Enhancements - ATA Enhancements and FAT32 Support

The Disk File System Enhancements - ATA Enhancements and FAT32 Support feature adds support in Cisco IOS software-based devices for flash cards that have been formatted with partitions on external devices. This feature also provides support for larger disk sizes through FAT32 support and support for disk partitions. In most scenarios, no user configuration is required to take advantage of this feature. Additional file system information is now available through existing command-line interface (CLI) commands. See the documentation of the **format** command for additional information about reformatting flash-based devices.

Additional file system enhancements that are introduced with this feature improve the performance and reliability of the system as a whole. The disk file system enhancements implemented as part of this feature include shared data structures, control structures, and other file system functions that apply to flash disks in various formats, such NVRAM, ATA flash disks, linear flash, USB flash, and the system RAM.

Dynamic Host Configuration Protocol Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Dynamic Host Configuration Protocol (DHCP) features. For detailed information about these features, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbdhcpf.htm

- DHCP Accounting: see the *Configuring DHCP Services for Accounting and Security* chapter.
- DHCP Address Allocation Using Option 82: see the *Configuring the Cisco IOS DHCP Server* chapter.
- DHCP Relay Subscriber Identifier Suboption of Option 82: see the *Configuring the Cisco IOS DHCP Relay Agent* chapter.

In addition, support for the following DHCP feature is introduced:

- DHCP Server Multiple Subnet.

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbmultd.htm

For the most recent information about the DHCP Server feature, see the *Configuring the Cisco IOS DHCP Server* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tiad_c/dhcp/htdhcpsv.htm

For the most recent information about the DHCP Relay Agent, see the *Configuring the Cisco IOS DHCP Relay Agent* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tiad_c/dhcp/htdhcpre.htm

Dual Priority Queue Support

For detailed information about this feature, see the “Configuring the SIPs and SSC” chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

Enhanced Fast Software Upgrade

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

- *Cisco IOS In Service Software Upgrade and Enhanced Fast Software Upgrade Processes*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/sbisefsu.htm

- The “Enhanced Fast Software Upgrade on the Cisco 7600 Series Routers” chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 12.2SR*:

  http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f1c85.html

EIGRP MIB

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gteigmib.htm

EIGRP Support for MTR

For detailed information about this feature, see the *Multi-Topology Routing* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srmtrdoc.htm

Embedded Event Manager (EEM) 2.2

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/sr_eem22.htm

Embedded Resource Manager (ERM)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/nm_erm.htm

Embedded Resource Manager (ERM) - MIB

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/ermmib.htm

Ethernet Local Management Interface (LMI) at Provider Edge (PE)

For detailed information about this feature, see the *Configuring Ethernet Local Management Interface on a Provider Edge Device* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbpelmi.htm

Ethernet OAM-Phase2/ELMI-PE

For detailed information about this feature, see the "Configuring the Fast Ethernet and Gigabit Ethernet SPAs" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080523f3c.html

FHRP - HSRP Multiple Group Optimization

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbhsrmg.htm

FHRP - Integration of Embedded Event Manager with Enhanced Object Tracking

For detailed information about this feature, which is also known as the FHRP - EOT integration with EEM feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbeotem.htm

Flexible Mapping of QinQ (2-2, 2-1, 1-2, 1-1) and QinQ Service Awareness

For detailed information about this feature, see the "Configuring the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

Flexible QinQ Mapping and Service Awareness

For detailed information about this feature, see the "Configuring the Cisco 7600 Series Ethernet Services 20G Line Card" chapter in the *Cisco 7600-ES20 Ethernet Line Cards Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f97.html

Hierarchical Quality of Service (HQoS) with Multipoint Bridging (MPB)

For detailed information about this feature, see the "Configuring QoS on the Cisco 7600 Series Ethernet Services 20G Line Card" chapter in the *Cisco 7600-ES20 Ethernet Line Cards Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f8d.html

HSRP for IPv6

For detailed information about these features, see the "Implementing IPv6 Addressing and Basic Connectivity" chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/v6addres.htm

IGMP/PIM Snooping for VPLS Pseudowire

For detailed information about this feature for the Ethernet Services 20G line cards, see the "Configuring the Cisco 7600 Series Ethernet Services 20G Line Card" chapter in the *Cisco 7600-ES20 Ethernet Line Cards Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f97.html

For detailed information about this feature for the SIP-400, see the "Configuring the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

Interfaces MIB: SNMP Context-based Access

The interface MIB (IF-MIB) has been modified to support context-aware packet information in Virtual Route Forwarding (VRF) environments. VRF environments require that contexts apply to Virtual Private Networks (VPNs) so that clients can be given selective access to the information stored in the IF-MIB. Clients that belong to a particular VRF can access information about the interface from the IF-MIB that belongs to that VRF only. When a client tries to get information from an interface that is associated with a particular context, the client can see only the information that belongs to that context and cannot see IF-MIB information that is associated with interfaces that are connected to another VRF to which it is not entitled. No commands have been modified or added to support this feature.

The IF-MIB supports all tables that are defined in RFC 2863 and the CISCO-IFEXTENSION-MIB.

IP Multicast Load Splitting—Equal Cost Multipath (ECMP) Using S, G and Next Hop

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbmpath.htm

IP SLAs Features

Cisco IOS Release 12.2(33)SRB introduces support for the following IP Service Level Agreements (SLAs) features.

IP SLAs for Metro-Ethernet

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/sr_meth.htm

IP SLAs - LSP Health Monitor with LSP Discovery

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srpdisc.htm

IP SLAs Random Scheduler

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/sr_slars.htm

IP Version 6 Features

Cisco IOS Release 12.2(33)SRB introduces support for the following IP version 6 (IPv6) features.

IPv6 ACL Extensions for Mobile IPv6

For detailed information about this feature, see the “Implementing Mobile IPv6” chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00804160bf.html

IPv6 Routing - EIGRP Support

For detailed information about this feature, see the "Implementing IPv6 VPN over MPLS (6VPE)" chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_vpnv6.htm

IPv6 VPN over MPLS (6VPE)

For detailed information about this feature, see the "Implementing Mobile IPv6" chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00804160bf.html

Intermediate System-to-Intermediate System Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Intermediate System-to-Intermediate System (IS-IS) features.

IS-IS MIB

For detailed information about these features, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sg25/ismibspt.htm

IS-IS Support for an IS-IS Instance per VRF for IP

For detailed information about these features, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/vrf_isis.htm

IS-IS Support for MTR

For detailed information about this feature, see the *Multi-Topology Routing* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srmtrdoc.htm

Layer 2 Virtual Private Network Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Layer 2 Virtual Private Network (L2VPN) features.

L2VPN Pseudowire Redundancy

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/fspseudo.htm

For information about limitations of the L2VPN Pseudowire Redundancy feature in Cisco IOS Release 12.2(33)SRB, see the "Limitations and Restrictions in Cisco IOS Release 12.2(33)SRB" section on page 97.

L2 VPN Pseudowire Switching

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/fsstitch.htm

VPLS Autodiscovery: BGP-Based

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/fs_vpls.htm

Lawful Intercept

For detailed information about this feature, see the following *Cisco 7600 Lawful Intercept Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76licfg/index.htm

For information about the Lawful Intercept feature on the SIP-400, see the "Overview of the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008044013b.html

Layer 2 Local Switching - Same-Port Switching for Frame Relay

For detailed information about this feature, see the following *Layer 2 Local Switching* document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00801ea88d.html

Logging to Local Non-Volatile Storage (ATA Disk)

For detailed information about this feature, see the *SYSLOG Writing to Flash* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/cs_sysls.htm

Multiprotocol Label Switching Embedded Management Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Multiprotocol Label Switching Embedded Management (MPLS EM) features.

MPLS EM - MPLS LDP MIB - RFC 3815

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/ldpmbrfc.htm

MPLS EM - MPLS LSR MIB - RFC 3813

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/lsrmbrfc.htm

MPLS EM - MPLS Multipath (ECMP) LSP Tree Trace

For detailed information about this feature, see the *MPLS EM—MPLS LSP Multipath Tree Trace* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sb_mmtr.htm

Multiprotocol Label Switching Label Distribution Protocol Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Multiprotocol Label Switching Label Distribution Protocol (MPLS LDP) features.

MPLS LDP - Autoconfiguration

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/fsldpaut.htm

MPLS LDP - IGP Synchronization

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/fsldpsyn.htm

MPLS LDP - MD5 Global Configuration

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sb_md5.htm

MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/ht_lspng.htm

Multiprotocol Label Switching Traffic Engineering Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Multiprotocol Label Switching Traffic Engineering (MPLS TE) features.

MPLS TE - DS-TE (RFC-3270)

For detailed information about this feature, see the *MPLS Traffic Engineering—DiffServ Aware (DS-TE)* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/dsteietf.htm

MPLS TE - Fast Reroute over ATM

For detailed information about this feature, see the *MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/fslnph30.htm

MPLS TE - Fast Tunnel Interface Down Detection

For detailed information about this feature, see the *MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/fslnph30.htm

MPLS TE - Node Protection Desired Bit

For detailed information about this feature, see the *MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/fslnph30.htm

Multiprotocol Label Switching Virtual Private Network Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Multiprotocol Label Virtual Private Network (MPLS VPN) features.

MPLS VPN - Show Running VRF

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sb_svrf.htm

MPLS VPN - VRF CLI for IPv4 & IPv6 VPNs

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/sr_mpvrf.htm

MPLS VPN VRF Selection Using Policy Based Routing

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fs_pbrsv.htm

MultiPoint Bridging over Ethernet

For detailed information about this feature, see the “Configuring the Cisco 7600 Series Ethernet Services 20G Line Card” chapter in the *Cisco 7600-ES20 Ethernet Line Cards Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f97.html

Multiprotocol BGP (MP-BGP) Support for CLNS

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tbgp_c/brbclns.htm

Multi-Topology Routing

For detailed information about this feature, see the *Multi-Topology Routing* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srmtrdoc.htm

NDE for VRF Interfaces

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/nfvrfsrb.htm

Netconf Access for Configuration over BEEP

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbnetbe.htm

NetFlow v9 for IPv6

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/nfv6xsrb.htm

Network Clock Support

For detailed information about this feature, see the "Configuring the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

Optimized Edge Routing (OER)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/sr_oer.htm

Open Shortest Path First Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Open Shortest Path First (OSPF) features.

Area Command in Interface Mode for OSPFv2

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/ospfarea.htm

OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/htostats.htm

OSPF SNMP ifIndex Value for Interface ID

For detailed information about this feature, see the *OSPF: SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/ht_ifndx.htm

OSPF Support for MTR

For detailed information about this feature, see the *Multi-Topology Routing* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srmtrdoc.htm

Outward Facing MEP

For detailed information about this feature, see the *Ethernet Connectivity Fault Management* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/srethcfm.htm

PBR over TE Tunnel

In Cisco IOS Release 12.2(33)SRB, hardware switching support is introduced for policy-based routing (PBR) packets that are sent over a traffic engineering (TE) tunnel interface on a Cisco 7600 series router. When a TE tunnel interface is configured by using the **set interface** command in a policy, the packets are processed in hardware. In previous releases, PBR packets that were sent over TE tunnels were fast-switched by route-processor software.

Per Interface Mroute State Limit

For detailed information about this feature, see the *Per Interface Mroute State Limit with Bandwidth Based CAC for IP Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srmcac.htm

Per Interface NetFlow

For detailed information about this feature, see the “Configuring NetFlow and NDE” chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 12.2SR*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sr/swcg/nde.htm

Note The configuration granularity for IPv4 NetFlow Data Export (NDE) has changed from global to per-interface configuration granularity. Global enabling of NDE collection for IPv4 L3 interfaces is not available in Cisco IOS Release 12.2(33)SRB. For a Cisco 7600 series that perform NDE, configurations must be reviewed and modified to conform to the per-interface configuration guidelines.

Per IP Subscriber DHCP Triggered RADIUS Accounting

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/ipradacc.htm

Per Subscriber/Per Protocol CoPP Support

For detailed information about this feature, see the "Overview of the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008044013b.html

Percent Priority/Percent Bandwidth Support

For detailed information about this feature, see the "Overview of the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008044013b.html

Private Hosts

For detailed information about this feature, see the "Private Hosts (Using PACLs)" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 12.2SR*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f5d19.html

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services

For detailed information about this feature, see the *Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbpweatm.htm

Quality of Service Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Quality of Service (QoS) features.

QoS Enhancement for Dual Priority Queues

For detailed information about this feature, see the "Configuring QoS on the Cisco 7600 Series Ethernet Services 20G Line Card" chapter in the *Cisco 7600-ES20 Ethernet Line Cards Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f8d.html

QoS/MQC Support for MTR

For detailed information about this feature, see the *Multi-Topology Routing* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srmtrdoc.htm

Rate Limiting Support for DAI and DHCP Snooping

For detailed information about this feature, see the "Configuring Denial of Service Protection" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 12.2SR* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sr/swcg/dos.htm

In addition, see the **mls rate-limit unicast ip** command in the *Cisco 7600 Series Internet Router IOS Commands Reference, 12.2 SX*:

http://www.cisco.com/en/US/partner/products/hw/routers/ps368/products_command_reference_chapter09186a0080172751.html

Reliable Delivery and Filtering for Syslog

For detailed information about this feature, see the *Reliable Delivery for Syslog over BEEP* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/htnmsylg.htm

Remote Port Shutdown

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbrpsdn.htm

RFC 3020 Multilink Frame Relay MIB Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t9/mfr_mib.htm

Role-Based Access Control CLI Commands

For detailed information about this feature, see the *Role-Based CLI Access* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtclivws.htm

Resource-Reservation Protocol Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Resource-Reservation Protocol (RSVP) features.

RSVP Application ID Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/ht_appid.htm

RSVP Fast Local Repair (RSVP FLR)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/rsvp_flr.htm

RSVP Interface-Based Receiver Proxy

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxf18/rsvpprox.htm

RSVP Refresh Reduction and Reliable Messaging

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fsrelmsg.htm

RSVP Scalability Enhancements

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/rsvpscal.htm

Scalable EoMPLS

For detailed information about this feature, see the "Configuring the Cisco 7600 Series Ethernet Services 20G Line Card" chapter in the *Cisco 7600-ES20 Ethernet Line Cards Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f97.html

Scale for IP Subscriber Awareness over Ethernet

For detailed information about this feature, see the "IP Subscriber Awareness over Ethernet" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 12.2SR*:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f1c8b.html

Security ACLs

For detailed information about this feature, see the "Overview of the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008044013b.html

Simple Network Management Protocol Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Simple Network Management Protocol (SNMP) features.

SNMP over IPv6

For detailed information about these features, see the "Managing Cisco IOS Applications over IPv6" chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mgev6.htm

SNMP Support for MTR

For detailed information about this feature, see the *Multi-Topology Routing* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srmtrdoc.htm

SNMPv3 - 3DES and AES Encryption Support

For detailed information about this feature, see the following *AES and 3-DES Encryption Support for SNMP Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t2/snmpv3ae.htm

SLB: GPRS Load Balancing Maps

For detailed information about this feature, see the *IOS Server Load Balancing Feature in IOS Release 12.2(33)SRB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/slbsrb1.htm

SLB: RADIUS Load Balancing Maps

For detailed information about this feature, see the *IOS Server Load Balancing Feature in IOS Release 12.2(33)SRB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/slbsrb1.htm

Stateful Switchover Features

Cisco IOS Release 12.2(33)SRB introduces support for the following Stateful Switchover (SSO) features.

SSO - DHCP Relay on Unnumbered Interface

For detailed information about this feature, see the *ISSU and SSO—DHCP High Availability Features* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sbdhcpha.htm

SSO - DHCP Server

For detailed information about this feature, see the *ISSU and SSO—DHCP High Availability Features* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sbdhcpha.htm

SSO - GLBP

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/srbssogl.htm

SSO - Multilink Frame Relay

For detailed information about this feature, see the *Stateful Switchover* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fssso20s.htm

SSO - PPP

For detailed information about this feature, see the *Stateful Switchover* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fssso20s.htm

Support for IP-TUNNEL-MIB as per RFC4087

For detailed information about this feature, see the *IP Tunnel MIB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/iptunmib.htm

Syslog over IPV6

For detailed information about these features, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/v6addres.htm

System Logging - EAL4 Certification Enhancements

Note Official EAL4 certification is not claimed by Cisco. This feature is part of current and planned enhancements which may qualify Cisco IOS Software for future certification.

This feature includes the following enhancements:

- The system logging process will now generate “audit start” and “audit stop” messages.
- The system logging process will now generate messages that include the date and time of an event, the type of event, the subject identity, and the outcome (success or failure) of an event.
- Changes to logging parameters will be logged.
- Further enhancements to minimize lost audit records.

VPLS and SVI-Based EoMPLS - Routed Pseudowire Support

The VPLS and SVI-Based EoMPLS - Routed Pseudowire Support feature makes it possible to route (Layer 3) as well as switch (Layer 2) frames for pseudowire connections between provider edge (PE) devices. Both point-to-point PE connections, in the form of Ethernet over MPLS (EoMPLS), and multipoint PE connections, in the form or Virtual Private LAN Services (VPLS), are supported. The ability to route frames to and from these interfaces now makes it possible to terminate a pseudowire into a Layer 3 network (VPN or global) on the same router, or to tunnel Layer 3 frames over a Layer 2 tunnel (EoMPLS or VPLS). The feature supports faster network convergence in the event of a physical interface or device failure through the MPLS Traffic Engineering (MPLS-TE) and Fast Reroute (FRR) features of the network. In particular, the feature enables MPLS TE-FRR protection for Layer 3 multicast over a VPLS domain.

To configure routing support for the pseudowire, configure an IP address and other Layer 3 features for the Layer 3 domain (VPN or global) in the virtual LAN (VLAN) interface configuration. The following example assigns the IP address 10.10.10.1 to the VLAN 100 interface, and enables Multicast PIM. (Layer 2 forwarding is defined by the VFI VFI100.)

```
int vlan 100
     xconnect vfi VFI100
     ip address 10.10.10.1 255.255.255.0
     ip pim sparse-mode
```

The following example assigns an IP address 20.20.20.1 of the VPN domain VFI200. (Layer 2 forwarding is defined by the VFI VFI200.)

```
int vlan 200
     xconnect vfi VFI200
     ip vrf forwarding VFI200
     ip address 20.20.20.1 255.255.255.0
```

New Hardware Features in Cisco IOS Release 12.2(33)SRA1

There are no new hardware features in Cisco IOS Release 12.2(33)SRA1.

New Software Features in Cisco IOS Release 12.2(33)SRA1

This section describes new and changed features in Cisco IOS Release 12.2(33)SRA1. Some features may be new to Cisco IOS Release 12.2SR 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 12.2(33)SRA1. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included in this section. If a feature listed in this section 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 in this section.

Per VRF for TACACS+ Servers

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_pvt.htm

New Hardware Features in Cisco IOS Release 12.2(33)SRA

This section describes new and changed features in Cisco IOS Release 12.2(33)SRA. Some features may be new to Cisco IOS Release 12.2SR 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 12.2(33)SRA. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included in this section. If a feature listed in this section 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 in this section.

Shared Port Adapters

Cisco IOS Release 12.2(33)SRA introduces support for the following new shared port adapters (SPAs):

- Channelized SPA
  - 1-port CHOC-3/CHSTM-1 SPA (SPA-1xCHSTM1/OC3)
- Ethernet SPAs
  - 1-Port 10 Gigabit Ethernet SPA, LANPHY XFP Optics (SPA-1XTENGE-XFP-V2)
  - 4-port 10/100 Ethernet SPA TX (SPA-4X1FE-TX-V2)
  - 8-port 10/100 Ethernet SPA TX (SPA-8X1FE-TX-V2)
  - 5-port Gigabit Ethernet SPA, SFP Optics (SPA-5X1GE-V2)
  - 10-Port Gigabit Ethernet SPA, SFP Optics (SPA-10X1GE-V2)
- POS SPAs
  - 1-Port OC-48 POS/RPR SPA with SFP Optics (SPA-1XOC48POS/RPR)
  - 2-Port OC-48 POS/RPR SPA with SFP Optics (SPA-4XOC48POS/RPR)
  - 4-Port OC-48 POS/RPR SPA with SFP Optics (SPA-4XOC48POS/RPR)

For a complete list of all supported SPAs in Cisco IOS Release 12.2SR, see the *Guide to Supported Hardware for Cisco 7600 Series Routers with Release 12.2SR*.

For further information about SPAs, see the *Cisco 7600 Series Router SIP, SSC, and SPA Hardware Installation Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109a7.html

New Software Features in Cisco IOS Release 12.2(33)SRA

This section describes new and changed features in Cisco IOS Release 12.2(33)SRA. Some features may be new to Cisco IOS Release 12.2SR 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 12.2(33)SRA. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included in this section. If a feature listed in this section 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 in this section.

Any Transport over ATM Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Any Transport over ATM (AToM) features.

Any Transport over MPLS (AToM) Graceful Restart

Any Transport over MPLS (AToM) Graceful Restart (GR) assists neighboring routers that have MPLS AToM stateful switchover/nonstop forwarding (SSO/NSF) support and Graceful Restart to recover gracefully from an interruption in service. In Cisco IOS Release 12.2(33)SRA, AToM GR functions strictly in helper mode, which means it can only help other routers that are enabled with AToM SSO/NSF and GR to recover. If the router with AToM GR fails, its peers cannot help it recover. AToM GR is based on MPLS Label Distribution Protocol (LDP) Graceful Restart.

Note The NSF/SSO: Any Transport over MPLS and Graceful Restart feature (which is also referred to as "AToM SSO/NSF") is not supported in Release 12.2(33)SRA. The AToM GR feature that is supported in Release 12.2(33)SRA refers to AToM GR helper mode.

For detailed information about this feature, see the *AToM Graceful Restart* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fsgratom.htm

Any Transport over MPLS (AToM): Tunnel Selection

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srtunsel.htm

AToM—VP Mode Cell Relay

The AToM—VP Mode Cell Relay feature is supported on the following shared port adapters:

- SPA-2XOC3-ATM
- SPA-4XOC3-ATM

- SPA-1XOC12-ATM
- SPA-1XOC48-ATM

For more information about the AToM—VP Mode Cell Relay feature, which is also referred to as the AToM: ATM Cell Relay over MPLS: VP Mode feature, see the "Configuring ATM VP to VP Local Switching with AAL0 Encapsulation" section and the "Layer 2 Local Switching-ATM to ATM" section in the *Configuring Multiprotocol Label Switching on FlexWAN and Enhanced FlexWAN Modules* document:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00803f3770.html

Also, see the *Configuring the ATM SPAs* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/sipspasw/76atmspa/76cfgatm.htm

AutoRP Enhancement

For detailed information about this feature, which is also referred to as the PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srautorp.htm

BCP Support on MLPPP

For detailed information about this feature, see the "Configuring the 2-Port and 4-Port Channelized T3 SPAs" and "Configuring the 8-Port Channelized T1/E1 SPA" chapters in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

- Configuring the 2-Port and 4-Port Channelized T3 SPAs

  http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008043ff57.html
- Configuring the 8-Port Channelized T1/E1 SPA

  http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008043ff58.html

For information about how to configure this feature on the Enhanced FlexWAN module, see the "Configuring BCP over MLPPP (Trunk Mode Only)" section in the *Cisco 7600 FlexWAN and Enhanced FlexWAN Modules Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/features.htm#wp157170

Border Gateway Protocol Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Border Gateway Protocol (BGP) features.

BGP MIB Support Enhancements

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_bmibe.htm

BGP Multicast Inter-AS (IAS) VPN

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/cs_bmiav.htm

BGP Reduction in Transient Memory Usage

Cisco IOS Release 12.2(33)SRA has implemented a reduction in transient memory usage by BGP when BGP updates are built.

BGP Support for BFD

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srbgpbfd.htm

BGP Support for Dual AS Configuration for Network AS Migrations

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srbgpdas.htm

BGP Support for Fast Peering Session Deactivation

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srbsfda.htm

BGP Support for IP Prefix Import from Global Table into a VRF Table

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_bgivt.htm

BGP Support for Named Extended Community Lists

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srnextcl.htm

BGP Support for Next-Hop Address Tracking

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srbhnt.htm

BGP Support for Sequenced Entries in Extended Community Lists

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srextseq.htm

BGP Support for TCP Path MTU Discovery per Session

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srbgpmtu.htm

Per-VRF Assignment of BGP Router-ID

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srbgprid.htm

Suppress BGP Advertisement for Inactive Routes

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/sr_sbair.htm

Bidirectional Forwarding Detection (BFD) Standard Implementation

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fs_bfd.htm

Call Admission Control for IKE

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gtcallik.htm

Certificate - ISAKMP Profile Mapping

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gt_isakp.htm

Certificate - Storage Location Specification

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srpkicsl.htm

Cisco IOS Login Enhancements

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_login.htmm

Cisco Networking Services

Cisco IOS Release 12.2(33)SRA introduces support for the following Cisco Networking Services (CNS) features.

CNS

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/sr_cns.htm

CNS Configuration Agent

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/sr_cnsca.htm

CNS Enhanced Results Message

The CNS - Enhanced Results Message feature is documented as the **cns config partial** command change in the *Cisco IOS Network Management Command Reference, Release 12.2 SR* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/srnm_r/index.htm

CNS Event Agent

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/sr_cnsea.htm

CNS Security Enhancement

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t9/ht_cnsse.htm

CLNS Support for GRE Tunneling of IPv4 and IPv6 Packets in CLNS Networks

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtclnsv6.htm

Command Scheduler

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hnm_c/ch30/hg_kron.htm

Configuration Change Notification and Logging

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtconlog.htm

Configuration Logger Persistency

The Configuration Logger Persistency feature implements a “quick save” functionality. The aim is to provide a “configuration save” mechanism in which the time to save changes from the startup configuration is proportional to the size of the incremental changes (with respect to the startup configuration) that must be saved. The persisted commands from the Cisco IOS Configuration logger are used as an extension to the startup configuration. The saved command, which is used as an extension to the startup configuration, provides a quick-save ability. Rather than saving the entire startup configuration, Cisco IOS software now saves just the commands that were entered since the last startup configuration was generated.

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srmgtint.htm

Configuration Replace and Configuration Rollback

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtrollbk.htm

Configuration Versioning

For detailed information about this feature, see the *Configuration Replace and Rollback* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtrollbk.htm

Contextual Configuration Diff Utility

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_diff.htm

Easy VPN

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

- *Easy VPN Server*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftunity.htm

- *Cisco Easy VPN Remote*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/ftezvpnr.htm

Easy VPN Client RSA - Signature Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtevcrsa.htm

EIGRP Support for Route Map Filtering

For detailed information about this feature, see the *EIGRP Route Map Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gteigrpr.htm

Embedded Event Manager (EEM) 2.1

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/sr_eem.htm

Encrypted Multicast over GRE

The Encrypted Multicast over GRE feature, also referred to as secure multicast over Generic Routing Encapsulation (GRE), is integrated in Cisco IOS Software Release 12.2(33)SRA. This feature provides a secure and scalable solution to protect multicast traffic in an enterprise or managed service-provider environment. Each head-end device that is configured with an IP Security (IPsec) Virtual Private Network (VPN) shared port adapter (SPA) can support IPsec encrypted multicast traffic for up to 500 remote tunnels. The practical applications include voice, video, and data broadcast.

Note that this feature requires specific hardware, including a Cisco Catalyst 6500 series switch or a Cisco 7600 series router with an IPsec VPN SPA and a Services SPA Carrier (SSC) module: either an SPA-IPsec-2G or an 7600-SSC-400.

For detailed information, see the IPsec VPN Shared Port Adapter documentation:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/sipspasw/76vpnspa/index.htm

Enhanced Crashinfo File Collection

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gt_cricm.htm

Enhanced Tracking Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/sretrac.htm

Ethernet Connectivity Fault Management

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srethcfm.htm

Ethernet Operations, Administration, and Maintenance

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srethoam.htm

Exclusive Configuration Change Access and Access Session Locking

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_exclu.htm

Extended ACL Support for IGMP to Support SSM in IPv4

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srmcxacl.htm

FHRP - Enhanced Object Tracking of IP SLAs

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/sreotsla.htm

FHRP - Object Tracking List

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srobtrls.htm

Front Side VRF for the IPsec VPN SPA

The VRF-Aware IPsec feature provides IP Security (IPsec) tunnel mapping to Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). By using the VRF-Aware IPsec feature, you can map IPsec tunnels to Virtual Routing and Forwarding (VRF) instances by using a single public-facing address.

A VRF instance is a per-VPN routing information repository that defines the VPN membership of a customer site attached to the Provider Edge (PE) router. A VRF comprises an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table. A separate set of routing and CEF tables is maintained for each VPN customer.

Front Door VRF (FVRF) and Inside VRF (IVRF) are central to understanding the feature.

Each IPsec tunnel is associated with two VRF domains. The outer encapsulated packet belongs to one VRF domain, called the FVRF, while the inner protected IP packet belongs to another domain called the IVRF. Another way of stating the same thing is that the local endpoint of the IPsec tunnel belongs to the FVRF while the source and destination addresses of the inside packet belong to the IVRF.

One or more IPsec tunnels can terminate on a single interface. The FVRF of all these tunnels is the same and is set to the VRF that is configured on that interface. The IVRF of these tunnels can be different and depends on the VRF that is defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile that is attached to a crypto map entry.

In previous releases of the IPsec VPN SPA, VRF-Aware IPsec was supported, but FVRF was not; as of Cisco IOS Release 12.2(33)SRA, FVRF is supported.

For more information about the VRF-Aware IPsec feature, including Front Door VRF, see the *VRF-Aware IPSec* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_vrfip.htm

For information about configuring Front Side VRF on the IPsec VPN SPA, see the documents at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/sipspasw/76vpnspa/index.htm

GRE Tunnel IP Source and Destination VRF Membership

For detailed information about this feature, see the *Generic Routing Encapsulation Tunnel IP Source and Destination VRF Membership* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/fsgrevrf.htm

HQoS Support for Ethernet Over MPLS (EoMPLS) VCs on the SIP-400

For detailed information about this feature, see the "Configuring the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

HSRP MD5 Authentication

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/sr_hsmd.htm

HTTPS—HTTP Server and Client with SSL 3.0

The HTTPS—HTTP Server and Client with SSL 3.0 feature provides Secure Socket Layer (SSL) version 3.0 support for the HTTP 1.1 server and HTTP 1.1 client within Cisco IOS software. SSL provides server authentication, encryption, and message integrity to allow secure HTTP communications. SSL also provides HTTP client authentication. HTTP over SSL is abbreviated as HTTPS.

H-VPLS with MPLS Edge on the SIP-400

For detailed information about this feature, see the "Configuring the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

Ingress/Egress CoS Classification with Ingress Policing per VLAN or EoMPLS VC (L2 and L3 QoS)

For detailed information about this feature, see the "Configuring the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

Inter-AS Support for Multicast VPN

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/iasmcvpn.htm

Interface Management Improvements - Scalability and Reliability

The Interface Management Improvements - Scalability and Reliability feature provides enhancements to the IF-MIB:

- The scalability and reliability of the interface management are improved.
- The extensibility of the interface management infrastructure is ensured.

For more information about the IF-MIB, see the *Cisco 7600 Series Router MIB Specifications Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/7600mibs/index.htm

Internet Protocol Security Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Internet Protocol Security (IPsec) features.

IPsec Anti-Replay Window: Expanding and Disabling

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_iarwe.htm

IPsec Dead Peer Detection (DPD) Periodic Message Option

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtdpmo.htm

IPsec Preferred Peer

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_ipspp.htm

IPsec VTI - Virtual Tunnel Interface

For detailed information about this feature, see the *IPsec Virtual Tunnel Interface* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gtipsctm.htm

Internet Protocol version 6 Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Internet Protocol version 6 (IPv6) features.

IPv6 Anycast Address

For detailed information about these features, see the "Implementing IPv6 Addressing and Basic Connectivity" chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/v6addres.htm

IPv6 Default Router Preferences

For detailed information about these features, see the "Implementing IPv6 Addressing and Basic Connectivity" chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/v6addres.htm

Internet Protocol version 6 Multicast Features

Cisco IOS Release 12.2(33)SRA supports the following Internet Protocol version 6 (IPv6) multicast features:

- IPv6 Multicast: Bootstrap Router (BSR)
- IPv6 Multicast: Explicit Tracking of Receivers
- IPv6 Multicast: MLD Access Group
- IPv6 Multicast: PIM Accept Register
- IPv6 Multicast: PIM Embedded RP Support
- IPv6 Multicast: Routable Address Hello Option
- IPv6 Multicast: RPF Flooding of Bootstrap Router (BSR) Packets
- IPv6 Multicast: Static Multicast Routing (mroute) for IPv6

For detailed information about these features, see the "Implementing IPv6 Multicast" chapter in the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm

IPMROUTE-STD-MIB

The IPMROUTE-STD-MIB, as defined in RFC 2932, is a module for managing IP multicast routing, independent of the specific multicast routing protocol in use. Support for this MIB replaces the draft form of the IPMROUTE-MIB.

The IPMROUTE-STD-MIB supports all the MIB objects of the IPMROUTE-MIB and also supports the following four new MIB objects:

- ipMRouteEntryCount
- ipMRouteHCOctets
- ipMRouteInterfaceHCInMcastOctets
- ipMRouteInterfaceHCOutMcastOctets

Note The ipMRouteScopeNameTable MIB object is not supported because it is not relevant to multicast routers.

IP SLAs - LSP Health Monitor

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/sbchmon.htm

IS-IS Support for Priority-Driven IP Prefix RIB Installation

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fslocrib.htm

Layer 2 Virtual Private Network Interworking Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Layer 2 Virtual Private Network (L2VPN) Interworking features:

- L2VPN Interworking: Ethernet VLAN to ATM AAL5
- L2VPN Interworking: Ethernet VLAN to Frame Relay
- L2VPN Interworking: Ethernet VLAN to PPP

For detailed information about these features, see the *L2VPN Interworking* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srinterw.htm

Memory Leak Detector

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gtmleakd.htm

Memory Pool - SNMP Notification Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtmemnot.htm

Multiprotocol Label Switching Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Multiprotocol Label Switching (MPLS) features.

MPLS Embedded Management - High Capacity Counter

For detailed information about this feature, see the "Restrictions for MPLS Enhancements to Interfaces MIB" section in the *MPLS Enhancements to Interfaces MIB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/ftifemib.htm

MPLS Enhancements to Interfaces MIB

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/ftifemib.htm

MPLS Label Distribution MIB: MPLS LDP Trap Enhancement

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

- *MPLS Label Distribution Protocol MIB*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ldpmib13.htm

- *MPLS Label Distribution Protocol MIB Version 8 Upgrade*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/fs27ldp8.htm

MPLS LDP - Graceful Restart

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fsgr29s.htm

MPLS LDP - Session Protection

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/fssespro.htm

MPLS over RBE

The ATM SPAs and Enhanced FlexWAN module support MLPS over Routed Bridge Encapsulation (RBE) on a Cisco 7600 series SIP-200. RBE is similar in functionality to RFC 1483 ATM half-bridging, except that ATM half-bridging is configured on a point-to-multipoint PVC, while RBE is configured on a point-to-point PVC.

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

- *Configuring the ATM SPAs*

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/sipspasw/76atmspa/76cfgatm.htm

- *Configuring Multiprotocol Label Switching on FlexWAN and Enhanced FlexWAN Modules*

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/flexmpls.htm

MPLS Static Labels

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/fs_stlab.htm

MPLS VRF Aware Static Labels

For detailed information about this feature, see the *VRF Aware MPLS Static Labels* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsvrflab.htm

Multiprotocol Label Switching Traffic Engineering Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) features.

MPLS Traffic Engineering (TE) - AutoTunnel Mesh Groups

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/gsamg2.htm

MPLS Traffic Engineering (TE) - AutoTunnel Primary and Backup

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/gsautotn.htm

MPLS Traffic Engineering (TE) - Class-Based Tunnel Selection

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/gscbts.htm

Also, see the “Configuring the SIPs and SSC” chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

MPLS Traffic Engineering (TE) - Fast Reroute MIB

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/frr_mib.htm

MPLS Traffic Engineering (TE) - Fast Reroute Link and Node Protection

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/gslnh29.htm

MPLS Traffic Engineering (TE) - Inter-AS TE

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/gsintast.htm

MPLS Traffic Engineering (TE) - LSP Attributes

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fslspatt.htm

MPLS Traffic Engineering (TE) - RSVP Hello State Timer

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/gsrsvpht.htm

MPLS Traffic Engineering (TE) - Shared Risk Link Groups (SRLG)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fs29srlg.htm

MPLS Traffic Engineering (TE) - Verbatim Path Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsvbmlsp.htm

Multiprotocol Label Switching Virtual Private Network Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) features.

MPLS VPN - eBGP Multipath support for CSC and InterAS MPLS VPNs

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbmulti.htm

MPLS VPN - Explicit Null Label Support with BGP IPv4 Label Session

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/gsxnlbsp.htm

MPLS VPN - Loadbalancing Support for Inter-AS and CSC VPNs

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srmplc.htm

MPLS VPN-MIB Support - MPLS VPN Trap Enhancement

For detailed information about this feature, see the "Command Reference" section in the *MPLS VPN—MIB Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsvnmb25.htm#wp1032378

MPLS VPN - Multi-Path Support for Inter-AS VPNs

For detailed information about this feature, see the *MPLS VPN—Interautonomous System Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fsiaseb.htm

MPLS VPN - Route Target Rewrite

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsrtrw4.htm

MPLS VPN - VPN Aware LDP MIB

For detailed information about this feature, see the *MPLS Label Distribution Protocol MIB Version 8 Upgrade* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/fs27ldp8.htm

MSDP Compliance with IETF RFC 3618

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_msdp.htm

Multicast VPN MIB Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/mcvpnmib.htm

Multilink Frame Relay (FRF.16.1) - Variable Bandwidth Class

For detailed information about this feature, see the following *Multilink Frame Relay (FRF.16.1)* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs_mfr.htm

Multipoint Bridging on the SIP-400

For detailed information about this feature, see the "Configuring the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

Multi-VC to VLAN Scalability

For information about this feature, see the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://www.cisco.com/en/US/partner/products/hw/routers/ps368/module_installation_and_configuration_guides_book09186a00802109bf.html

MUX UNI Support on the SIP-400 (MPB on GE)

For detailed information about this feature, see the "Configuring the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

MUX UNI Support on LAN Cards

For detailed information about this feature, which is also referred to as the 7600-MUX-UNI Support on LAN Cards feature, see the "Configuring PFC3BXL and PFC3B Mode Multiprotocol Label Switching" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide, Release 12.2SR*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sr/swcg/pfc3mpls.htm

NETCONF over SSHv2

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t9/srnetcon.htm

NetFlow Layer 2 and Security Monitoring Exports

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/sronfsc.htm

NetFlow MPLS Label Export

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sx_pal.htm

Nonstop Forwarding Stateful Switchover Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Nonstop Forwarding (NSF) Stateful Switchover (SSO) features.

NSF/SSO—MPLS LDP and LDP Graceful Restart

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsldpgr.htm

NSF/SSO—MPLS LDP MIB

For detailed information about this feature, see the "MIBs" section in the *NSF/SSO—MPLS LDP and LDP Graceful Restart* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsldpgr.htm

NSF/SSO—MPLS TE and RSVP Graceful Restart

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/gsrsvpgr.htm

NSF/SSO—MPLS VPN

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsvpngr.htm

NSF/SSO—MPLS VPN MIB

For detailed information about this feature, see the "MIBs" section in the *NSF/SSO—MPLS VPN* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsvpngr.htm

SSO HSRP

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srssohsr.htm

Optional OCSP Nonce

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srpkinon.htm

Open Shortest Path First Features

Cisco IOS Release 12.2(33)SRA introduces support for the following Open Shortest Path First (OSPF) features.

OSPF Area Transit Capability

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/ospfatc.htm

OSPF Per-Interface Link-Local Signaling

For detailed information about this feature, which is also referred to as the OSPF Link-local Signaling (LLS) Per Interface Basis feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/ospflls.htm

OSPF RFC 3623 Graceful Restart

For detailed information about this feature, which is also referred to as the NSF - OSPF RFC 3623 Graceful Restart feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s32/gr_ospf.htm

OSPF Sham-Link MIB Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/ospfslms.htm

Periodic MIB Data Collection and Transfer Mechanism

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/gdatacol.htm

Persistent Self-Signed Certificates

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srpkissc.htm

PIM RPF Vector

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/pimrpfvr.htm

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbpweatm.htm

QoS Support on Bridging Features

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

- The "Configuring the SIPs and SSC" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

  http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html

- "Configuring QoS on Bridged Interfaces" section in the *Configuring QoS on the FlexWAN and Enhanced FlexWAN Modules* document:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/flexqos.htm#wp1291431

Reliable Static Routing Back-Up Using Object Tracking

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xe/dbackupx.htm

Reverse Route Injection (RRI)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_rrie.htm

RFC 1490 Spanning-Tree Interoperability Enhancements

For detailed information about this feature, see the "Enhancements to RFC 1483 and RFC 1490 Spanning Tree Interoperability" section in the *Cisco 7600 FlexWAN and Enhanced FlexWAN Modules Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/features.htm#wp123609

RSVP Message Authentication

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fsrsvpnk.htm

Scalable EoMPLS (SIP-Based)

For detailed information about this feature, see the "Configuring Fast Ethernet and Gigabit Ethernet SPAs" chapter in the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*:

http://cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080523f3c.html

Secure SNMP Views

The USM, VACM and Community MIBs have information that can potentially be used to gain access to the router using SNMP. Therefore, the USM, VACM, and Community MIBs are excluded from the default SNMP access view so as not to allow remote access unless specifically configured. However, when an SNMP view is created with any parent object identifier (OID) of these MIBs included (for example "internet included"), these MIBs also get included in the view. To increase security, the Secure SNMP Views enhancement excludes these MIBs from SNMP access views even when parent OIDs are included in the view. Prior to this release, when configuring SNMP views with parent OIDs that include the USM, VACM, or Community OIDs, the user was required to explicitly exclude them. For example, the following configuration can be used for excluding security-sensitive MIBs from the SNMP view named "test":

```
! - include all MIBs under the parent tree "internet" snmp-server view test internet
included
! -- exclude snmpUsmMIB snmp-server view test 1.3.6.1.6.3.15 excluded
! -- exclude snmpVacmMIB snmp-server view test 1.3.6.1.6.3.16 excluded
! -- exclude snmpCommunityMIB snmp-server view test 1.3.6.1.6.3.18 excluded
```

Beginning in Cisco IOS Releases 12.0(26)S and 12.2(2)T, the USM, VACM, and Community MIBs are excluded from any parent OIDs in a configured view by default. If you wish to include these MIBs in a view, you must now explicitly include them.

SNMP Support for VPNs

For detailed information about this feature, see the *SNMP Notification Support for VPNs* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/cs23vpn.htm

TCP MSS Adjustment

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_admss.htm

Two-Rate Policer

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/ft2plc26.htm

VPLS Multiple VCs per Spoke

For detailed information about this feature, see the "Virtual Private LAN Services on the Optical Services Modules" section in the *Configuring Multiprotocol Label Switching on the Optical Services Modules* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sr/mpls.htm#wp1423607

VRF Aware Multicast Error Messages

The VRF Aware Multicast Error Messages feature improves the troubleshooting of MPLS VPN environments by allowing service providers to track the multicast error messages that are associated with a particular MVPN customer.

VRF Aware System Message Logging (Syslog)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/srvrfslg.htm

MIBs

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

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

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

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

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

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

Limitations and Restrictions

The following sections contain information about limitations and restrictions in Cisco IOS Release 12.2SR that can apply to the Cisco 7600 series routers. With the release of Cisco IOS Release 12.2(33)SRC, Cisco IOS Release 12.2SR supports the Cisco 7200 series routers (Cisco 7200, Cisco 7200-NPE-G2, and Cisco 7201 routers) and the Cisco 7301 router.

Limitations and Restrictions in Cisco IOS Release 12.2(33)SRC

This section describes limitations and restrictions in Cisco IOS Release 12.2(33)SRC and later releases.

Cisco 7600 Platform Restrictions for Broadband Support with Cisco IOS Release 12.2SRC

Physical Interface Restrictions

- The Broadband/ISG sessions are only supported on Gigabit (GE) Ethernet interfaces. See the Hardware Restriction section in the documentation for the specific type of GE interfaces that are required.
- The Broadband/ISG sessions are not supported on ATM interfaces.

Hardware Restrictions

- The Broadband/ISG sessions are only supported on Cisco 7600 series routers with RSP720 as the supervisor.
- The Broadband/ISG sessions are only supported on Cisco 7600 series routers with 7600-SIP-400 as the subscriber facing line card.
- The Broadband/ISG sessions are only supported on Cisco 7600 series routers with SPA-5X1GE-V2 or SPA-1X10GE-L2 as the subscriber facing port adaptor.

Restriction on Session Types

The Broadband/ISG sessions are *not* supported with following access protocols:

- L2TPv2/VPDN
- PPPoA
- PPPoEoA
- PPPoL2TP
- RBE

Configuration Restriction

The Broadband/ISG sessions are *only* supported with access subinterfaces, which were introduced in Cisco IOS Release 12.2(33)SRB. For more information on this restriction, see the following document:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f1c8b.html#wp1060177

ISG Specific Restrictions

- Traffic classes are not supported on Cisco 7600 series routers.
- Prepaid accounting is not supported on Cisco 7600 series routers.

- Per flow accounting using Traffic Classes is not supported on Cisco 7600 series routers.
- ISG Rate limiting via (QU,QD) is not supported on Cisco 7600 series routers.
- Layer 4 Redirect and PBHK are performed on the Centralized Route processor (RP) on Cisco 7600 series routers.

HA Support for DHCP Initiated IP Sessions When ISG Is a DHCP Relay Content

When ISG is configured as a DHCP relay, high availability for DHCP initiated IP sessions is supported only on "unnumbered" interfaces. On numbered interfaces, where the IP address is configured directly on the interface, HA is not supported.

HA Support for ISG Features Includes Change of Authorization but not Per-feature Push

ISG features can be dynamically changed through Change of Authorization (COA). The COA commands are supported for SSO/ISSU. But if a feature is changed, dynamically via per-feature push, HA support is not provided.

VLAN Mobility Is Not Allowed for ISG Sessions

For IP sessions initiated through DHCP, ISG does not allow the users to roam from one VLAN to the other. ISG expects the VLAN to remain the same throughout the user session.

If the user moves from one VLAN to the other, the user needs to reboot the Customer Premise Equipment (laptop or the modem) to initiate a new session.

Limitations and Restrictions in Cisco IOS Release 12.2(33)SRB

This section describes limitations and restrictions in Cisco IOS Release 12.2(33)SRB and later releases.

L2VPN Pseudowire Redundancy

The following restrictions affect the L2VPN Pseudowire Redundancy feature on the Cisco 7600 series in Cisco IOS Release 12.2(33)SRB:

- IP (routed) Ethernet to VLAN Interworking is not supported.
- Data traffic may switch from the primary pseudowire to the backup pseudowire when the primary attachment circuit at the tail-end goes down. However, when the MPLS switching path for the primary pseudowire goes down, data traffic is not switched from the primary pseudowire to the backup pseudowire.

Limitations and Restrictions in Cisco IOS Release 12.2(33)SRA

This section describes limitations and restrictions in Cisco IOS Release 12.2(33)SRA and later releases.

ADM and AGM Modules

In Cisco IOS Release 12.2(33)SRA and later releases, traffic Anomaly Detection Module (ADM) and Anomaly Guard Module (AGM) modules are supported on the Supervisor Engine 720 but not on the Supervisor Engine 32.

Advanced QinQ Service Mapping

In Cisco IOS Release 12.2(33)SRA and later releases, Advanced QinQ Service Mapping is not supported on the OSM-2+4GE-WAN+ Optical Services Module (OSM).

Content Switching Modules

In Cisco IOS Release 12.2(33)SRA and later releases, the Content Switching Module (CSM) and Content Switching Module with SSL (CSM-S) are not supported

IP Services Bundle Image

In the IP services bundle image of Cisco IOS Release 12.2(33)SRA and later releases, you cannot configure both MPLS and IPv6.

L2VPN Interworking

The Cisco 7600 series does not support IP (routed) Ethernet to VLAN Interworking. This restriction affects the L2VPN Interworking feature in Cisco IOS Release 12.2(33)SRA.

Maximum Number of IPsec Tunnels with PKI

In Cisco IOS Release 12.2(33)SRA and later releases, when Public Key Infrastructure (PKI) is configured with the IPsec VPN SPA, a maximum number of 2000 IP security (IPsec) tunnels is supported.

OSM-1CHOC12/T1-SI and QoS Packet Counts

On an OSM-1CHOC12/T1-SI, when Class-Based Weighted Fair Queueing (CBWFQ) or Low Latency Queueing (LLQ) is configured in combination with any feature that requires MSFC or PFC processing, the counters in the output of the **show policy-map interface** command do not increment. This situation occurs because the MSFC and PFC do not support CBWFQ or LLQ and do not count packets for QoS purposes.

Examples of configurations for which the counters do not increment are the following:

- **frame-relay ip tcp header-compression**
- **frame-relay ip rtp header-compression**
- **access-list** *access-list-number* **permit ip any any log**

Note that the **log** keyword in the **access-list** command causes packets to be processed by the MSFC or PFC.

- CSCsg58652

  Symptoms: On a Cisco 7600 series that is configured with a Supervisor Engine 720 and an OSM-1CHOC12/T1-SI, the output of the **show policy-map interface** command may display a packet counter of 0 for a serial interface.

  This symptom is observed on a Cisco 7600 series that has a Class-Based Weighted Fair Queueing (CBWFQ) or Low Latency Queueing (LLQ) configuration when packets are process-switched in software on the MSFC or PFC instead of being fast-switched, and then the router is reloaded with one of the following saved configurations:

  – When you have entered and saved commands such as the following to configure an access control list (ACL):

  ```
  access-list 199 permit ip any any log
  interface s1/1.1/1:0.2
  ip access-group 199 out
  ```

  – When you have entered and saved commands such as the following to configure IP header compression:

  ```
  interface serial1/1.1/1:0
  encapsulation frame-relay
  frame-relay ip tcp header-compression
  service-policy output TEST
  ```

  Workaround for the ACL symptom: Remove the **log** keyword from the **access-list** command, and then reload the router.

  Workaround for the header compression symptom: Enter the **no frame-relay ip tcp header-compression** command or the **no frame-relay ip rtp header-compression** command, and then reload the router.

SNMP Version 1 BGP4-MIB Limitations

You may notice incorrect BGP trap OID output when you use the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). The problem is not due to any error with Cisco IOS software. This problem occurs because the BGP4-MIB does not follow RFC 1908 rules regarding version 1 and version 2 trap compliance. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2SR that can apply to the Cisco 7600 series routers.

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/kobayashi/sw-center/sw-ios-advisories.shtml

Field Notices and Bulletins

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

http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/index.shtml

- Field Notices—We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account with Cisco.com, you can find field notices at http://www.cisco.com/kobayashi/support/tac/fn_index.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/public/support/tac/fn_index.html.
- Product Bulletins—If you have an account with Cisco.com, you can find product bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find product bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.

Important Notes for Cisco IOS Release 12.2(33)SRB

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(33)SRB and later releases.

CEoP SPA and APS

When a pseudowire is configured on an interface of a Circuit Emulation over Packet (CEoP) SPA, Automatic Protection Switching (APS) for the interface is useful only in conjunction with pseudowire redundancy.

CEoP SPA and ATMoMPLS

When ATM over MPLS (ATMoMPLS) is configured on a Circuit Emulation over Packet (CEoP) SPA, you cannot connect an ATM network to an OC-3 link nor can you connect an OC-12 network to a T1 link. In order for AToM tunnels that are configured for AAL0 encapsulation or VP mode to function over non-symmetric links, shape the VC or VP to a rate that can be carried by interfaces at both ends by configuring CBR, UBR, or UBR+.

CEoP SPA and Clock Recovery Configuration Guidelines

When configuring clock recovery in Cisco IOS Release 12.2(33)SRB, consider the following guidelines:

- Adaptive Clock Recovery:
  - Only the 24-port channelized T1/E1 ATM CEoP SPA can be used as a clock source.
  - Only a single clock can be sourced for a router if adaptive clock recovery mechanism is used.
  - The clock must be the same as used by the router as the network-clock. Any pseudowire in this case can carry the clock.
  - The minimum bundle size of CEM pseudowires on the network which delivers robust clock recovery is 4 DS0s.
  - The minimum packet size of CEM pseudowires on the network which delivers robust clock recovery is 64 bytes.
- Differential Clocking:
  - The maximum number of differential clocks sourced from a 24-port channelized T1/E1 ATM CEoP SPA is 24.
  - The 24-port channelized T1/E1 ATM CEoP SPA can recover up to 24 T1/E1 clocks.
  - There are several bundles sent from the same port, the bundle which is used for carrying clock of the port is the first created bundle of the port. Only pseudowires which include the first DS0 of a port can carry differential clock.

Important Notes for Cisco IOS Release 12.2(33)SRA2

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(33)SRA2 and later releases.

BPDU Support on dot1q Tunnels [CSCsf98713]

A Bridge Protocol Data Unit (BPDU) is now supported between a CE and PE router that are connected through only a Layer 2 protocol tunnel, that is, the BPDU is supported even when there is no dot1q tunnel between the CE and PE router.

Important Notes for Cisco IOS Release 12.2(33)SRA

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(33)SRA and later releases.

Detection Mechanism for the MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Node Protection, with RSVP Hellos Support Feature

When the detection mechanism for the MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Node Protection, with RSVP Hellos Support feature is configured with a refresh interval and missed refresh limit that are too short, a neighbor may be declared down while the neighbor is actually up, and a warning message may be generated. To prevent this situation, configure the refresh interval and missed refresh limit in the following ways:

- Ensure that the *interval-value* argument in the **ip rsvp signalling hello refresh interval** *interval-value* command is 200 milliseconds or longer.
- Ensure that the *msg-countip* argument in the **rsvp signalling hello** [**fast-reroute**] **refresh misses** *msg-count* command has a value of 4 or more.

The detection interval for the detection mechanism should be at least 800 milliseconds (that is, 200 milliseconds of the *interval-value* argument multiplied by the value 4 of the *msg-countip* argument) or longer.

ip routing protocol purge interface Command

As of Cisco IOS Release 12.2(33)SRA, you can use the **ip routing protocol purge interface** command in global configuration mode to enable routing protocols to purge their routes when an interface goes down in the global configuration mode. To disable this function, use the **no** form of this command.

For detailed information about this command, see the "IP Routing Protocol-Independent Commands" section of the *Cisco IOS IP Routing Protocols Command Reference, Release 12.2 SR*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/sripr_r/irp_pisr.htm#wp1037055

Caveats

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

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

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

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

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Support: Tools & Resources: Bug Toolkit** (which is listed under Troubleshooting). Another option is to 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.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

This section consists of the following subsections:

Open Caveats—Cisco IOS Release 12.2(33)SRC

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRC. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsk05653

  Symptoms: The **aaa group server radius** subcommand **ip radius source-interface** will cause the standby to fail to sync.

```
c10k-6(config)#aaa group server radius RSIM
 c10k-6(config-sg-radius)#ip radius source-interface GigabitEthernet6/0/0


 c10k-6#hw-module standby-cpu reset
 c10k-6#
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
 Aug 13 14:49:31.793 PDT: %C10K_ALARM-6-INFO: ASSERT MAJOR RP A Secondary
removed
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_DOWN)
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_DOWN)
 Aug 13 14:49:31.813 PDT: %REDUNDANCY-3-IPC: cannot open standby port no such
port
 Aug 13 14:49:32.117 PDT: %RED-5-REDCHANGE: PRE B now Non-participant(0x1C11 =>
0x1421)
 Aug 13 14:49:32.117 PDT: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a
standby insertion (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

 Aug 13 14:50:52.617 PDT: %RED-5-REDCHANGE: PRE B now Standby(0x1421 => 0x1411)
 Aug 13 14:50:54.113 PDT: %C10K_ALARM-6-INFO: CLEAR MAJOR RP A Secondary
removed
 Aug 13 14:51:33.822 PDT: -Traceback= 415C75D8 4019FB1C 40694770 4069475C
 Aug 13 14:51:33.822 PDT: CONFIG SYNC: Images are same and incompatible

 Aug 13 14:51:33.822 PDT: %ISSU-3-INCOMPATIBLE_PEER_UID: Image running on peer
uid (2) is the same
 -Traceback= 415CCC2C 415C75FC 4019FB1C 40694770 4069475C
 Aug 13 14:51:33.822 PDT: Config Sync: Bulk-sync failure due to Servicing
Incompatibility. Please check full list of mismatched commands via:
   show issu config-sync failures mcl

 Aug 13 14:51:33.822 PDT: Config Sync: Starting lines from MCL file:
 aaa group server radius RSIM
  ! <submode> "sg-radius"
```

```
 - ip radius source-interface GigabitEthernet6/0/0
```

Conditions: This symptom is observed if the **aaa group server radius** subcommand **ip radius source-interface** CLI is configured on a box with dual PREs.

Workaround: If the customer does not use the **aaa group server radius** subcommand **ip radius source-interface** *interface*, this will not be a problem.

If they use the **aaa group server radius** subcommand **ip radius source-interface** *interface* on a Cisco 10000 router in simplex mode (a single PRE), this will not be a problem.

If they run with dual PREs, then they will need to remove the **aaa group server radius** subcommand **ip radius source- interface** *interface* from the configuration as a workaround.

Removing the **aaa group server radius** subcommand **ip radius source-interface** *interface* from the configuration could cause problems for the customer. The radius server may be expecting the request to come from a specific source address. The router will now use the address of the interface the packet egresses the router from, which may change over time as routes fluctuate.

- CSCsl59184

  Symptoms: Some VTYs remain stuck on incoming telnet access. When the problem occurs, the banner is displayed but no login prompt. Tacacs logs seem to be normal.

  Conditions: This symptom occurs on a Cisco 7613 router that is running Cisco IOS Release 12.2(33)SRA5.

  Workaround: There is no workaround. Customer has to switchover the supervisor manually when the problem occurs.

- CSCsl61164

  Symptoms: Router may crash at ipflow_fill_data_in_flowset when changing flow timeout.

  Conditions: This symptom occurs when netflow is running fully with data export going on. User manually changes a cache timeout with the **ip flow-cache timeout inactive** *N* command.

  Workaround: Do not change the netflow cache timers while the router is exporting data and routing traffic.

IP Routing Protocols

- CSCsl30069

  Symptoms: A Cisco Catalyst 6500/7600 might crash due to memory corruption on the Route Processor (RP).

  Conditions: This symptom occurs when running Cisco IOS Release 12.2(33)SRB2 and when BGP is configured on the box.

  Workaround: There is no workaround.

- CSCsl49628

  Symptoms: When a VRF is deleted through the CLI, the VRF deletion never completes on the standby RP, and the VRF cannot be reconfigured at a later time.

  Conditions: This symptom is observed when BGP is enabled on the router.

  Workaround: There is no workaround.

- CSCsl55521

  Symptoms: Router may experience BGP convergence issues.

  Conditions: This problem has been seen when a lot of aggregates are configured on a router.

Workaround: Add all aggregates after router has fully converged.

- CSCsl83415

  Symptoms: After executing the following CLI (steps mentioned alphabetically) via a script (not reproducible manually), the router sometimes crashes:

  ```
  Test10 :
  a. clear ip bgp 10.0.101.46 ipv4 multicast out
  b. clear ip bgp 10.0.101.47 ipv4 multicast out
  Test 1:
  c. show ip bgp ipv4 multicast nei 10.0.101.2
  d. show ip bgp ipv4 multicast [<prefix>]
  e. config t
  ```

  Crash does not happen for each of the following cases:

  1. if same CLI is cut-paste manually, there is no crash.

  2. if **clear cli** is not executed, there is no crash.

  2. if **config term** is not entered, there is no crash.

  Conditions: The symptom occurs after executing the above CLI.

  Workaround: There is no workaround.

Miscellaneous

- CSCej33698

  Symptoms: A router that is running Cisco IOS software may mistakenly fail a CRC check on files in NVRAM.

  Conditions: This symptom has been observed with large files, such as large startup configurations.

  Workaround: There is no workaround.

- CSCsi30175

  Symptoms: “Success” is sent by router instead of “Error Code 404 (Invalid Request)”.

  Conditions: This symptom is seen when LI intercept-Identifier is >8 octets and encryption is used on Cisco 7200 platform.

  Workaround: Do not use encryption.

- CSCsi88974

  Symptoms: While configuring MD, if the MediationSrcInterface is set to loopback interface, then on sending traffic, MALLOC failures are seen.

  Conditions: Problem is seen when traffic rate is equal to or greater than 8000 packets per second.

  Workaround: There is no workaround.

- CSCsk04724

  Symptoms: High line card CPU utilization and low session bring up rates on SIP400.

  Conditions: This symptom occurs when the HQoS configuration is applied on sessions in egress direction at time of session bring up.

Workaround: The session bring up rate improves if sessions are spread across multiple ports on the SIP400. However, the line card CPU utilization will remain high.

- CSCsk41134

  Symptoms: ISAKMP SA negotiation will fail for RSA signature w/cef switching and in tunnel mode.

  Workaround: There is no workaround.

- CSCsk86642

  Symptoms: SPA-2xOC3-POS is not seeing the correct K1/K2 bytes on working group 1 APS, when switching from Protect to Working port.

  Conditions: This was observed in a lab environment with a Cisco 7604 router back to back with a Cisco 7206 router. Code tested Cisco IOS Release SRA1 and Cisco IOS Release SRA2.

  Workaround:

  1. Hw-slot reset on the Sip400-SPA corrects the problem.
  2. A shut/no shut on the protect interface corrects the problem.

- CSCsk99465

  Symptoms: A Cisco 7600series router that is configured with MPB in a SSO HA configuration may display a message as follows:

  ```
  %ISSU-3-NOT_FIND_MSG_SES: Cannot find message session(0) to get msg mtu
  ```

  Conditions: This behavior exists for MPB in Cisco IOS Release 12.2SR since Release 12.2SRC. The problem is seen when the Standby Supervisor and the line card on which MPB is configured get reset. After this, if the line card comes back online before the ISSU negotiation between the Active Supervisor and the Standby Supervisor is completed, this error message will be seen.

  Workaround: The workaround is to avoid a double-fault situation which the Standby supervisor and the line card get reset at the same time.

- CSCsl10412

  Symptoms: A router CPU hits 100% when SPA-OCx3-ATM is reset.

  Conditions: This symptom is observed on a Cisco 7600 router with Cisco IOS Release 12.2(33)SRB1. It has an ATM interface with approximately 400 VCs. If the main interface is reset, the CPU hits 100%. When the CPU process is queried, SNMP is holding the CPU cycle.

  ```
  Router: C7600
  IOS: 12.2(33)SRB1
  SIP-400
  2xOC3 ATM SPA
  ```

  Customer ATM interface has approximately 400 VCs. A reset hits the CPU at 100%, and SNMP process holds the cycle.

  Workaround: Disable bgp traps.

- CSCsl19375

  Symptoms: A Cisco 7600 series router that is configured with VPLS under SVI, the state of the VPLS VCs may show as UP even when the SVI is down.

  Conditions: This behavior exists for VPLS in SR releases since SRA. The VPLS VCs are allowed to be provisioned and be UP as soon as the **no shutdown** command is applied. The interface VLAN reflects the state of the Ethernet switchports connected, and the VC state indicates if the VFI was provisioned. The VPLS VC circuit was able to come up.

Workaround: There is no workaround.

- CSCsl22117

  Symptoms: A Cisco 1000BaseT gigabit interface goes down/down (not connect) unexpectedly. No errors nor logs were observed, a part to the usual sequence of %LINEPROTO-5-UPDOWN:, %LINK-3-UPDOWN:, %LINEPROTO-SP-5-UPDOWN:, %LINK-SP-3- UPDOWN: (if the **logging events link-status** command is enabled on the interface).

  Conditions: This symptom is observed on multiple Cisco 7613 routers that are running Cisco IOS Release 12.2(33)SRB2 and equipped with WS-X6724-SFP + DFC + GLC-T (1000BaseT adapters). All affected interfaces are directly connected to Unix servers.

  Workaround:

  – OIR (unplug and plug back) the GLC-T adapter is currently the only workaround while running Cisco IOS Release 12.2(33)SRB2.

  – These symptoms were never observed with Cisco IOS Release 12.2(33)SRA3, so downgrading may be another workaround, if applicable

- CSCsl28931

  Symptoms: On a Cisco 7600 router that is configured with VPLS if the traffic on the ingress direction and egress direction follows different Forwarding Engines (DFC or CFC), the dynamically learned entries may not be synchronized after a line card OIR, resulting in the traffic being flooded for those MAC entries.

  Conditions: See the following conditions:

  1. The traffic flow needs to be asymmetrical. For example in a VPLS scenario, the ingress traffic comes from a switchport in a ES-20 line card (which has a distributed forwarding engine) and is forwarded to a core facing line card like SIP-400. In this flow, the ingress traffic is forwarded by the ES-20 local forwarding engine, and the opposite traffic (MPLS core to access) is forwarded by the central forwarding engine.
  2. Line card OIR (removal/reinsertion) happens.

  Workaround: Clear mac address-table dynamic entries.

- CSCsl33956

  Symptoms: MLFR interfaces might flap when the T3 controller is shut.

  Conditions: The problem might occur under the following conditions:

  1. On a Cisco 7200 router having member links spread across two controllers on the same PA-MC-T3-EC Port adapter.
  2. When we do shut and no shut of one controller.
  3. Occurs only under scaled configuration of more than 40 MFR interfaces.

  Workaround: Configure a higher number LMI retries on the MFR interface using the following commands. Examples:

  interface MFR0 (on the DTE side) frame-relay lmi-n392dte 3

  or

  interface MFRO (on the DCE side) frame-relay lmi-n392dce 3

- CSCsl37041

  Symptoms: Not able to configure channel-group after RPR+ switchover.

  Conditions: After RPR+ switchover, if the channel-group is deleted and then try to configure it immediately again, the channel creation fails.

Workaround: Wait for few seconds after deletion of channel-group (after RPR+ switchover) and then create it again.

- CSCsl41325

  Symptoms: A router crashes when BGP adjacency goes down. Lots of spurious memory access is seen.

  Conditions: This symptom is observed on a Cisco 7600 series router with Supervisor 720-3BXL that is running Cisco IOS Release 12.2(33)SRB2.

  Workaround: Issue is not seen when running Cisco IOS Release 12.2(33)SRA5.

- CSCsl43546

  Symptoms: On the Cisco 7600 platform a reset of a line card may cause all MPLS over GRE adjacencies on the interfaces using that line card to be lost. Traffic will no longer be forwarded.

  Conditions: This problem can be caused on a Cisco 7600 by issuing the **hw-module** *module-number* **reset** command.

  Workaround: Reconfigure the interface to be admin down and then up. int *interface name* shutdown/no shutdown.

- CSCsl49705

  Symptoms: ISSU between SRB-2 & SRB-3 done, with tunnels configured on active, causes “IDBINDEX_SYNC-4-RESERVE” messages on standby (SRB-2) & a delay (wait) of around 3 sec per tunnel, which causes a standby reset in case there is a large number of tunnels configured.

  Conditions: This symptom occurs when tunnels are configured.

  Workaround: Remove tunnels configs before doing ISSU.

- CSCsl50569

  Symptoms: A SIP-400 module may drop all ingress packets destined for another fabric-enabled module. Prior to this, the module would be operating correctly.

  Conditions: This problem has only been seen with Cisco IOS Release 12.2(33) SRB2. The exact trigger is still unknown.

  Workaround: To recover connectivity, issue the **hw-module module** *mod* **reset** command.

- CSCsl51914

  Symptoms: On Cisco 7600/SIP400 supporting MLP interfaces, “priority percent” does not work.

  Conditions: The conditional police rate values will not get updated:

  a) when ever there is a member link addition or deletion happens from the bundle

  b) when all the members of the multilink is down and come back

  c) SPA / LC OIR

  Workaround: Use priority and with absolute-value (explicit) policer.

  Further Problem Description: The SIP-400 has a different HQF mechanism which does not use the Cisco IOS HQF structures. These structures are supposed to be updated when there is a request from the hqf common code. HQF common code is looking for some variables which are not set at the SIP-400 structure level. Hence the updates are not received by the SIP-400, by which this problem is being caused.

- CSCsl51945

  Symptoms: The HSRP IPv6 config on the standby RP may loose its address, such that the config on the standby RP appears as:

standby 1 ipv6 ::

The standby resets as well.

Conditions: This will occur if group is in init state while doing the configuration or changes its state to init after applying the configuration. If you reapply the command on the active RP without first removing it, then a config sync error will occur and the standby RP will reload.

Trigger: Standby RP on switchover stuck in standby-cold state.

Impact: Secondary RP resets, configuration sync failure.

Workaround: There is no workaround.

- CSCsl57023

  Symptoms: After switchover happens on Cisco 7600 and new Active is reset, PVC recreation fails.

  Conditions: This switchover happens on Cisco 7600 from Active to Standby.

  Workaround: There is no workaround.

  Further Problem Description: Sounds like VC is locked.

  ```
  76b(config-if)#int ATM9/1/0
  76b(config-if)#pvc 12/100
  %ATM: Exceeded the VC limit. Max VCs allowed is 8191
  76b(config-if)#
  *Dec 3 10:52:18.543: %ATM-3-FAILCREATEVC: ATM failed to create VC(VCD=0, VPI=0, VCI=0) on Interface ATM9/1/0, (Cause of the failure: ATM interface temporarily unavailable)
  -Traceback= 4069D894 4069DDD8 4021864C 4023ABC0 40625030 4229DC5C 40650128 4176D2A4 4176D290
  ```

- CSCsl58384

  Symptoms: When a switchport is configured for port-security feature and line rate traffic of a highly scaled mac-addresses is sent (more than 4k), the router crashes due to all layer 2 traffic getting punted to SP (switch processor).

  Conditions: This symptom occurs when port-security feature is enabled.

  Workaround: User must rate-limit the layer 2 data using the **mls rate- limit layer2 port-security 5000** command.

- CSCsl58941

  Symptoms: The VPN SPA on a Cisco 7600 series router stops decrypting traffic for all the tunnels suddenly. All tunnels are up, but from the **show crypto session** command, the packets decrypted counter is not increasing. Encrypted counters are increasing. BGP and PIM traffic is affected.

  Conditions: This symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRB2. This has not occurred with Cisco IOS Release 12.2(33)SRA3.

  Workaround: Reload the SPA module.

- CSCsl60168

  Symptoms: System unexpected reloads due to memory corruption in the IO memory pool. This occurs 7 minutes after the switch has been commanded to reload.

  ```
  %SYS-3-OVERRUN: Block overrun
  %SYS-6-BLKINFO: Corrupted redzone blk
  ```

  Conditions: This symptom occurs in normal operation.

  Workaround: There is no workaround.

- CSCsl61806

  Symptoms: All BW queues will be having en eir of 10g odd and maxrate of 0. LC throws the message “Exceed eir” as the sum of all queue eir is exceeding 540G.

  Conditions: It will affect an environment which has a large config with 1000 EVCs under a port channel. When shape rate is changed dynamically on the cass default and make a shut/ no shut on the port channel eir is going out of bound and maxrate is going zero. It is not consistent.

  Workaround: An LC reload in problem condition will recover the condition.

- CSCsl62851

  Symptoms: The router experiences XDRDISABLE condition and prints the following two messages:

  ```
  %XDR-6-XDRDISABLEREQUEST: Peer in slot 9/1 (23) requested to be disabled due
   to: XDR Keepalive Timeout. Disabling linecard
   %FIB-2-FIBDISABLE: Fatal error, slot 9/1 (23): XDR disabled
  ```

  Conditions: This symptom happens when there are a lot of IPC failures in the RP => LC path, but there is no specific trigger. Primary causes of this failure could be:

  1. There is a lot of control traffic between RP and LC.
  2. IPC failures/error conditions which in turn could have led to application (XDR) level failure.

  Workaround: Do an OIR of LC.

- CSCsl63272

  Symptoms: Traffic does not go through some of the HW Ethernet over MPLS (EoMPLS) VCs in port mode.

  Conditions: The symptom is not known yet.

  Workaround: Remove the Xconnect from the configuration and add it again.

  Further Problem Description: There are two TCAM entries for the same VC. The first one is associated with a wrong adjacency. The second one is associated with correct adjacency. Since the first one is used the traffic loss is observed.

- CSCsl65179

  Symptoms: Setting priority queue limit for PFC QoS configurations resets non-priority queue limits to default values.

  Conditions: Changing the priority queue limit to default setting will reset non-priority queue limits to default values. If CoS values are mapped to queues with default queue limits of 0 then traffic with these CoS values will be dropped until non-default configuration is reapplied.

  Workaround: After changing priority queue limit reapply non default non-priority queue limits.

- CSCsl67938

  Symptoms: Memory leak in “XDR LC Background” process is observed on SP.

  Conditions: This symptom is observed on a Cisco 7606 router that is running Cisco IOS Release 12.2(33)SRB2. This is also seen on Cisco IOS Release 12.2(33)SRA2.

  Workaround: There is no workaround.

- CSCsl68034

  Symptoms: Traffic might fail on dMLP bundles when the SPA OIR is done.

  Conditions: This symptom occurs when a SPA is OIRed on a SIP-200 on a Cisco 7600 router having dMLP bundles with member links from a SPA.

Workaround: OIR of the SIP-200 line card will bring back the traffic up.

- CSCsl70667

  Symptoms: A line card crash is observed after the following error messages:

  ```
  FIBXDRINV: Invalid XDR format. FIB entry XDR has bogus routecount
  ```

  Conditions: This error message and crash are seen very rarely after OIR of the line card.

  Workaround: There is no workaround.

- CSCsl72073

  Symptoms: Virtual-access keeps flapping on a Cisco 7200 series router under traffic.

  Conditions: This symptom occurs when LFIoFR (LFI over Frame Relay) is configured on a Cisco 7200 series router. The flapping occurs only when there is data traffic on the link at line rate and QoS is active.

  Workaround: Define a class to match keep-alive packets using the **match not protocol ip** command. No flaps are seen with this configuration.

- CSCsl72281

  Symptoms: After a Cisco 7600 series router reloads, host routes created by DHCP relay process for DHCP clients that are connected to unnumbered VLAN interfaces point to wrong VLAN interface.

  Conditions: This symptom occurs when interface-index value parameter on the router changes after the router reloads. This parameter is stored in DHCP bindings database on TFTP or FTP server. It is recalculated in case of the router reloading and may change if a new interface is added or existing interface is removed from the configuration. For example, a single interface VLAN is added to the configuration prior to the router reloading.

  Workaround: There is no workaround.

- CSCsl72636

  Symptoms: A Cisco router may experience traffic drop on frame-relay point-to- point subinterfaces during a SSO/NSF failover. This only occurs when a large number of frame-relay point-to-point interfaces are used.

  Conditions: This symptom is observed on a Cisco router that is running either Cisco IOS Release 12.2(32)SB or later releases, or Cisco IOS Release 12.2(32) SRB or later releases, that is configured for Stateful-Switchover (SSO) and Nonstop Forwarding (NSF).

  Workaround: There is no workaround.

- CSCsl72677

  Symptoms: SNMP counters produce inconsistent results on WS-X6724-SFP when subinterfaces are configured and polled.

  Conditions: This symptom occurs when using the following SNMP OID:

  ```
  .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets.
  ```

  Workaround: There is no workaround.

- CSCsl72774

  Symptoms: A router may run out of memory and fail malloc due to a memory leak.

  Conditions: This problem only occurs on distributed platforms (like the Cisco 7600/Catalyst 6500) when the CEF consistency checkers have been enabled. By default, the CEF consistency checkers are disabled. When the CEF consistency checkers are turned on, memory is leaked on the RP, SP and line cards.

If you want to use the consistency checkers, then do so for only short periods of time. For example, use the consistency checkers while diagnosing network problems.

Workaround: Disable the CEF consistency checkers by using the following commands:

no cef table consistency-check ipv4

no cef table consistency-check ipv6

- CSCsl74289

  Symptoms: An IPsec tunnel between a Cisco 7600 router and a Cisco 2811 router works without NAT box in the middle. When the NAT box is present, the tunnel does not come up stopping at Phase 2.

  Conditions: This symptom occurs in the NAT-T in an IPSec and VRF scenario.

  Workaround: There is no workaround.

- CSCsl76647

  Symptoms: The **clear crypto isakmp** command deletes SA with connection ID from 0 to 32766. The SA created with the VPN SPA has a connection ID higher than 32766, and cannot be singularly deleted.

  Conditions: This symptom occurs when SA is established using the VPN SPA.

  Workaround: There is no workaround.

- CSCsl76939

  Symptoms: After shut/no shut and SSO, some IMA groups may not pass traffic.

  Conditions: With 2k ATOM MPLS VCs configured on 42 IMA groups, if we perform the (shut/no shut + switchover), then some of the MPLS VC circuits are not passing the traffic. This is not real test scenario, which customer will be performing in real time scenario.

  Workaround: If we perform the SIP module OIR or SPA OIR, then all the MPLS circuits will come UP and traffic will pass at line rate.

- CSCsl77920

  Symptoms: IP addresses are not assigned from the desired DHCP pool.

  Conditions: This happens when the DHCP class-name is downloaded via the Per-User Profile.

  Workaround: If the solution requires the DHCP class-name download, then do it via the Service-Profile and download the service.

- CSCsl80385

  Symptoms: While reconfiguring an EVC under port channel after a sequence of steps, the following error message might be seen:

  ```
  %GENERAL-DFC3-2-CRITEVENT: ETHER EFP CLIENT: Could not add qinq
  ```

  Conditions: This occurs (not consistently) when following steps are being done:

  1. Boot up the router with a port-channel and 1000 xconnect EVCs.
  2. Unconfigure one of the service instance and add the config to a physical interface.
  3. Unconfigure the same service instance in step 2 and reconfigure it back under the same port-channel as before.

  Workaround: There is no workaround.

  Further Problem Description: When this error is seen the service instance will stop passing traffic in ingress direction.

- CSCsl80722

  Symptoms: L2 protocols are not tunneled with Cisco Route Switch Processor 720 (RSP720).

  Conditions: This symptom occurs with RSP720.

  Workaround: Use SUP720-3BXL instead.

- CSCsl80899

  Symptoms: Rare crash occurs when a peer 7600 router is reloaded.

  Conditions: This symptom is seen when a Peer 7600 router is reloaded in a back to back Cisco 7600 topology with thousands of locally terminated subscriber sessions.

  Workaround: There is no workaround.

- CSCsl83212

  Symptoms: Traceback error message is shown every 10 seconds in the log on both Active and Standby RPs:

  ```
  *Dec 17 20:48:47.342: assert failure: NULL!=tinfo: ../const/common-
   rp/const_macedon_tunnel.c: 3875: macedon_tunnel_check_takeover_criteria
   *Dec 17 20:48:47.342: -Traceback= 42C53118 42C59EB0 42C61938 42C621CC
  ```

  Conditions: This symptom is observed when an autotemplate interface is deleted from router configuration.

  Workaround: Recreating the same autotemplate interface that is being deleted will stop this traceback error message.

- CSCsl85297

  Symptoms: Supervisor 720 keeps reloading after loading as SSO standby mode, with Cisco IOS Release 12.2(33)SRB2.

  Conditions: The problem occurs with configuration sync:

  ```
  %SCHED-3-SEMLOCKED: rf proxy rp agent attempted to lock a semaphore, already
  locked by itself -Traceback
  %IP_DEVICE_TRACKING-4-TABLE_LOCK_FAILED: Table already locked by process-id xx
  (rf proxy rp agent)
  Config Sync: Bulk-sync failure due to PRC mismatch. Please check the full list
  of PRC failures via: show redundancy config-sync failures prc

  Config Sync: Starting lines from PRC file:
  interface xxx
   ! <submode> "interface"
  - ip route-cache same-interface
   ! </submode> "interface"
  ```

  Workaround: There is no workaround.

- CSCsl86316

  Symptoms: VPN subsystem: Excessive CPU utilization/Tracebacks in VTEMPLATE Backgr results in the rtr becoming unstable.

  Conditions: L2TP scenario.

  Workaround: There is no workaround.

- CSCsl86633

  Symptoms: SCHED-2-EDISMSCRIT: Critical/high priority process rf_cc_clear_counter_process may not dismiss message seen on supervisor switchover with SSO operating mode. There is no known impact because of this message.

  Conditions: This message can be seen if port-channel configuration exists on the Cisco 7600.

  Workaround: There is no workaround.

- CSCsl87445

  Symptoms: Traceback is generated by DHCP process:

  ```
  %DHCP_SNOOPING-3-DHCP_SNOOPING_INTERNAL_ERROR
  ```

  and finally crashes:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header
  ```

  Conditions: With DHCP relaying and snooping working, and receiving DHCP packets with Option 82 inserted, the switch will cause several DHCP tracebacks and finally crashes due to memory errors. This is seen in Cisco IOS Release 12.2(33)SRB2 but not in the Cisco IOS Release 12.2SXF train.

  Workaround: There is no workaround.

- CSCsl88651

  Symptoms: SP crashes the router on reload of an adjacent core router.

  Conditions: In a typical mVPN scenario with Edge (PE) and Core (P) routers, with Bi-Dir in the core and PIM-SM on the mvrf. It is observed that on reloading one of the core routers, the edge router i.e. the PE router crashes. The crash if observed when the core router is trying to come up after reload. The scenario in which this issue is discovered is mVPN+L3VPN on the PE router. I have 100mVPNs and 500 L3VPNs.

  Workaround: There is no workaround. Issuing the **reload** command on core router creates the problem. This is specific to Cisco IOS Release12.2SRC.

- CSCsl88658

  Symptoms: A Cisco 7600 router that is having a large scaled configuration (eg, 20k+ VPLS VCs + 4k+ Scalable EoMPLS), configured in SSO Redundant mode and without LDP targeted session Graceful Restart, after an SSO Supervisor redundant failure, may experience a series of messages %L2-SP-4-NOMEM: Malloc failed: L2-API purge all earl entries failed 0 and some MAC Entries in the L2 MAC Table are not purged, resulting in the corresponding entries in the MAC Address table not being flushed. Under normal circumstances of bidirectional conversation, the new packets will repopulate the MAC tables and no external visible effect is observed. If the conversation is not bidirectional, the traffic ma y be interrupted until the entry ages out, and the traffic should resume as normal.

  Workaround: This problem may not cause any impact in most of the cases. If desired, one workaround is to reduce the aging timer for the dynamic mac address entry or clear the mac address table for the corresponding VPLS VLANS after an SSO switchover (which will happen automatically if there is no traffic sourced by the corresponding MAC address).

- CSCsl88708

  Symptoms: Flapping MPLS IP while there is VPN traffic through, or flapping MPLS IP after SSO or sending MPLS traffic with EoS bit =0 causes the router to crash.

  Conditions: The problem has been seen on s72033-adventerprisek9-mz.122-32.8.11.SRC3 and s72033-adventerprisek9-mz.nightly.src_throttle_121507 images.

  Workaround: There is no workaround.

- CSCsl88931

  Symptoms: When a SPA-SER-4XT is being used, the following error message is seen:

  ```
  %SERIAL_12IN1-3-SPI4_HW_ERR: SPA 4/3: Port0 SNK SPI4 DIP4 Error was encountered.
  ```

  Conditions: A SPA-SER-4XT should be present in a MCP platform to hit this problem.

  Workaround: There is no workaround.

  Further Problem Description: Apart from the above error message, the SPA functions normally and packet continues to pass through

- CSCsl91046

  Symptoms: Traffic coming into GigabitEthernet interface on OSM card is dropped on the LC.

  Conditions: On router boot-up, GigabitEthernet interface on the OSM card with scaled swEoMPLS configurations, drops traffic that ingresses into the card. Transmit side, however works fine.

  Workaround: Shut / no shut of the interface resolves the issue.

  Further Problem Description: Issue has not been seen consistently. Issue is seen with SRC image.

- CSCsl92632

  Symptoms: On ATM interface on Flexwan after removing service-policy and shut/no shut cause ALIGN-3-SPURIOUS and then OIR the LC cause RP crash.

  Conditions: This symptom occurs when ATM interface with multilink PPP resets after shut/no shut.

  Workaround: There is no workaround.

- CSCsl94621

  Symptoms: For the ATM Multi-VLAN to VC feature, when the remote end of the link flaps, the spanning tree instance for the VLAN gets lost, and traffic is no longer forwarded.

  Conditions: Link flap when the ATM VC is the only instance of that VLAN in the router.

  Workaround: If there is at least one other port on the same VLAN, spanning-tree remains, and there is no impact. Configure a switchport and allow all VLANs that are in the ATM Multi-VLAN VC.

- CSCsl94829

  Symptoms: There was ESM20 line card crash observed during bootup of SRC6 image.

  Conditions: During router reload this problem was reported once so far.

  Workaround: The line card comes up fine after recovery.

- CSCsl96417

  Symptoms: Result is router crash.

  Conditions: This symptom occurs on ISSU upgrade with ATM ACs (configured with xconnect), the router crashes on running the **issu runversio**n command.

  Trigger: During the router upgrade with ATM ACs (configured with xconnect), configuration from rsp72043-adventerprisek9-mz.122-33.SRB2 to rsp72043-adventerprisek9-mz.122-32.8.11.SRC6 and in the **issu runversion**.

  Impact: Router crashes.

  Workaround: There is no workaround.

- CSCsl97835

  Symptoms: In a system with scaled configuration, with a operational rep segment, when a rep port role is configured as non-edge and then swapped to edge, the standby supervisor can crash.

Workaround: The port where the rep config is being changed (to rep edge or non-edge role) should be shut down first before making these changes, make the required changes and then unshut the port. This would prevent the standby from crashing.

- CSCsm04643

  Symptoms: PPPoA Client unable to obtain IPv6 Auto config address.

  Conditions: This is observed on Cisco 7200 routers that are loaded with Cisco IOS 12.2 Release SRC images configured for PPPoA with PAP enabled.

  Workaround: There is no workaround

Wide-Area Networking

- CSCsk15296

  Symptoms: When more than one dLFIoATM bundle is configured between 2 routers on an ATM SPA the ping fails across all the bundles except the first one.

  Conditions: This happens only if I have the same VPI and multiple VCIs.

  That is, in the below output, I have associated every ATM subint to a diff virtual-template. The ping goes through across 4/1/0.1 and 4/1/0.5 (which have same VC and diff VP) but does not go through 4/1/0.2,3 and 4 (with same VP as 4/1/0.1 but diff VC)

```
76A#sh atm pvc
VCD /                                            Peak Av/Min Burst
Interface  Name         VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
2/0/0.1    1              1   101 PVC     SNAP       UBR  599040              UP
2/0/0.2    2              1   102 PVC     SNAP       UBR  599040              UP
2/0/0.3    3              1   103 PVC     SNAP       UBR  599040              UP
2/0/0.4    4              1   104 PVC     SNAP       UBR  599040              UP
2/0/0.5    5              2   102 PVC     SNAP       UBR  599040              UP
76A#
```

  Workaround: Configure the virtual-template first and the ATM PVC next.

- CSCsk30718

  Symptoms: The memory of LAC and LNS exceeds the set target when PPPoE sessions are initiated.

  Conditions: This issue is seen when PPPoE sessions are initiated.

  Workaround: There is no workaround.

- CSCsl47374

  Symptoms: When CPS values for autobahn76 with LAC as Cisco 7200 G2 Ix Access as LNS and LNS as Cisco 7200 G2 Ix Access as LAC are low when compared with CPS results from Images SB4, XN3 and XD9.

  Conditions:

  1. Cisco 7200 G2 as LAC using autobahn76 image and Ix Access as LNS.
  2. Cisco 7200 G2 as LNS using autobahn76 image and Ix Access as LAC. This only happens when there are multiple tunnels/vpdn-groups on the LAC with the same local name going to the same vpdn-group on the LNS.

  Workaround: There is no workaround.

Further Problem Description: When CPS Result for Autobahn76 was compared with CPS results from Images SB4,XN3 and XD9.it indicates a degradation on AB76.

CPS was Calculated with Standalone LNS and LAC using Ix Access.

For Image c7200p-advipservicesk9-mz.autobahn76_102207 results are give below:

```
7200 G2 as LAC and Ix Access as LNS.

 4k pppoe sessions/4k L2tp Tunnels-----111.11 CPS   99 % CPU utilisation of LAC
was observed
 8k pppoe sessions/8k L2TP tunnels-----69.57  CPS   99 % CPU utilisation of LAC
was observed

 Standalone LNS and Ix Access as LAC.

 4k pppoe sessions/4k L2tp Tunnels-----108.11 CPS
 8k pppoe sessions/8k L2TP tunnels-----117.65 CPS
```

This is an uncommon configuration. Normally when one needs to have multiple tunnels from the LAC to the same LNS, one configured multiple vpdn-groups on the LAC with different local-names and for each of these a corresponding vpdn-group is created on the LNS with the corresponding terminate-from name.

- CSCsl51607

  Symptoms: A router is not able to ping the second hop through the serial link that is configured with multilink virtual-template and encap ppp, although it can ping the next hop. Packets directed to other router through static route via virtual-access are getting dropped.

  Conditions: This symptom is seen in the Cisco IOS Release 12.2SR images c7200-ipbase-mz.autobahn76_111707 and c7200-ipbase-mz.122-32.8.99.SR.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRC

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SRC. This section describes only severity 1, severity 2, and select severity 3 caveats. See also Resolved Caveats—Cisco IOS Release 12.2(33)SRB1, page 252 and Resolved Caveats—Cisco IOS Release 12.2(33)SRB2, page 195.

Basic System Services

- CSCdv48842

  Multiple Cisco products contain vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages. The vulnerabilities can be repeatedly exploited to produce a denial of service. In most cases, workarounds are available that may mitigate the impact. These vulnerabilities are identified by various groups as VU#617947, VU#107186, OUSPG #0100, CAN-2002-0012, and CAN-2002-0013.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml

- CSCed73481

  Symptoms: When “sh ip cache ver flow” on the router, it fails to display the AS numbers for each flow. This does not affect traffic forwarding.

  Conditions: This symptom occurs during normal use.

  Workaround: There is no workaround.

- CSCed93927

  Symptoms: The “%RADIUS-3-NOSERVERS: No Radius hosts configured” error message appears after the receipt of a RADIUS Access-Accept packet, preventing accounting updates from being sent.

  Conditions: This symptom is observed on a router with a very specific RADIUS server host configuration after you have reloaded the router.

  Workaround: Perform the following steps:

  1. Remove specific RADIUS commands by entering the following:

  no radius-server host 10.0.0.1 auth-port 1645 acct-port 0 non-standard key 7

  no radius-server host 10.0.0.1 auth-port 0 acct-port 1646 non-standard key 7

  2. Remove all server group configurations by entering the following commands:

  no aaa group server radius ACS

  no aaa group server radius RAD

  3. Reinstall the server group configurations by entering the following commands:

  aaa group server radius ACS server 10.0.0.1 auth-port 1645 acct-port 1646 deadtime 10 ! aaa group server radius RAD server 10.0.0.2 auth-port 1645 acct-port 1646 deadtime 10

- CSCef64439

  Symptoms: A PRE requires a long time to enter the STANDBY HOT state after a switchover.

  Conditions: This symptom is observed on a Cisco 10000 series when two PREs are forced to switchover back and forth.

  Workaround: Enter the **snmp-server ifindex persist** command.

- CSCef78565

  Symptoms: Port-ID TLV advertised by the current CDP implementation (which corresponds to cdpCacheDevicePort in CISCO-CDP-MIB and identifies the port CDP packet is sent on) does not always consistently correspond to the value of ifName object across various interface types.

  Conditions: The issue is observed for different interface types, including POS, Port-channel, FastEthernet subinterfaces.

  Workaround: There is no workaround.

- CSCeh64791

  Symptoms: A memory leak may occur when you delete a RADIUS server group.

  Conditions: This symptom is observed when the server is configured with a key.

  Workaround: There is no workaround.

- CSCej57779

  Symptoms: A reload of a Cisco 7600 router, with a huge number (for example, 1000) of VRF configured with BGP/VPN learning redistributed routers, may cause some VRFs to not learn distributed routes from the peer.

Conditions: This symptom has been observed in Cisco IOS Release 12.2SRA when a huge number of VRF are configured. This symptom is not applicable to Cisco IOS Release 12.4.

Workaround: The symptom can be resolved on the per VRF basis by removing the VRF instance and the BGP/VPN configuration for this instance and then adding them back.

- CSCek32177

  Symptoms: A TACACS+ AV address that is defined as “255.255.255.254” may not be processed correctly.

  Conditions: The symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(5.8)T or a later release but may not be release-specific.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when RADIUS is configured.

- CSCek39431

  Symptoms: On a Cisco 7500 platform, a Cisco IOS Image can not be loaded from an ATA Flash disk if it is formatted with Cisco IOS Release 12.2(31.04.04)SRB or Release 12.2(32.08.01)SR.

  Conditions: This symptom occurs when formatting the ATA disk with Cisco IOS Release 12.2(31.04.04)SRB or Release 12.2(32.08.01)SR.

  Workaround: Format the disk with an older Cisco IOS version.

- CSCek58840

  Symptoms: When a new PPP session is set up, the following warning message is generated, and the session fails:

  ```
  LAC: %IDMNGR-3-ALLOCFAIL: Warning: Failed to allocate memory for keylist in
  event_init
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB1. The PPP sessions start failing after the router has been up for about two weeks with many policy-map changes on the PVCs, a few cleared sessions by the clients, and one switchover. The symptom appears to be both platform- and release-independent.

  Workaround: There is no workaround.

- CSCek63810

  Symptoms: A Cisco 10000 series may run out of memory after a number of ATM port flaps have occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 28,000 PPPoA Point-to-Point Termination and Aggregation (PTA) sessions. Each time that the ATM ports that carry the sessions flap and in this process remain down long enough for the sessions to time-out, more memory is lost. The symptom appears to be both platform- and release-independent.

  Workaround: There is no workaround.

- CSCek69519

  Symptoms: When the execution of the **show aaa user all** command waits at the “More” prompt and when you cancel the command, the console is locked up for up to one minute and the CPU usage increases to near 100 percent during this time.

  Conditions: This symptom is observed on a Cisco router that is configured with many broadband sessions.

  Workaround: There is no workaround.

- CSCek78644

  Symptoms: SNMP does not use the source address in a VRF.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T. However, the symptom may also affect other releases.

  Workaround: Ensure that an SNMP interface is not defined in a VRF.

- CSCir01027

  Symptoms: SNMP over IPv6 does not function.

  Conditions: This symptom is observed on a Cisco router that integrates the fix for caveat CSCsg02387. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg02387. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Use SNMP over IPv4.

- CSCsa40461

  Symptoms: A Cisco router that is running Cisco IOS Release 12.3(7)T or later releases and configured to use the VRF-aware TACACS+ feature will be unable to perform TACACS+ authentication for enable authentications if the TACACS+ server lies within a VRF.

  Workaround: Use a TACACS+ server that is reachable via the global routing table.

- CSCsc99912

  Symptoms: The MPLS forwarding table entry contains no CE information.

  Conditions: This symptom occurs when two PEs are connected without any P routers, the MPLS routing information are not propagated to the PE on each end.

  Workaround: There is no workaround.

- CSCsd70700

  Symptoms: A traceback is generated on the standby RP after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7500 series that has an ATA disk installed in any of the PCMCIA slots.

  Workaround: There is no workaround.

- CSCse85200

  Symptoms: Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  Conditions: Since CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

  Workaround: Disable on interfaces where CDP is not necessary.

- CSCsf12539

  Symptoms: Tracebacks may be generated for all accounting messages.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA.

  Workaround: There is no workaround.

- CSCsf98394

  Symptoms: When the **initiator radius-proxy** command is enabled on an ISG, extra characters are shown with the identifier in the output of **show sss session** and **show radius-proxy client session** commands.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the user name has at least 8 characters.

  Workaround: Use a user name with less than 8 characters.

- CSCsg24971

  Symptoms: A memory leak may occur on a line card, eventually causing IPC to fail.

  Conditions: This symptoms is observed on a Cisco platform that is configured for NetFlow. The symptom affects distributed platforms only.

  Workaround: There is no workaround.

- 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.

- CSCsh19482

  Symptoms: A Cisco 10000 series may crash and generate a "%C10K-2-RPRTIMEOUT_CRASH:" error message.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for NetFlow.

  Workaround: There is no workaround.

- CSCsh76038

  Symptoms: AAA enable authentication via a TACACS+ server fails.

  Conditions: This symptom occurs when the **aaa authentication enable default group tacacs+** command or the **aaa authentication enable default group** command pointing towards a TACACS+ server group is configured.

  Workaround: There are two possible workarounds.

  1. On the TACACS+ server, configure a user named "$enab{x}$", where {x} is the desired privilege level, such as using "$enab15$" for regular enable mode. This user's password will be the enable password.
  2. Change to a Cisco IOS release that does not yet include CSCin98780.

  Further Problem Description: When using a RADIUS server, enable authentication is done by authenticating a user named "$enab{x}$". When using a TACACS+ server, enable authentication is done by using the user's actual username, which allows TACACS+ to define separate enable passwords for each user.

  CSCin98780 erroneously caused the Cisco IOS software to authenticate "$enab{x} $" as a username for enable authentication for TACACS+ servers. This causes enable authentications in existing installations to fail, since TACACS+ server user databases do not normally contain a "$enab{x}$" user. This fix, CSCsh76038, corrects the issue, and any Cisco IOS release with this fix will transmit the user's actual username again in any enable authentication request.

- CSCsi04892

  Symptoms: When you enter the **no ip sla schedule** *operation-number* command, error messages may be generated.

  Conditions: This symptom is observed on a Cisco router when you unconfigure an Ethernet SLA feature.

  Workaround: There is no workaround.

- CSCsi13207

  Symptoms: The output of the **show ip cache flow** command for NetFlow on an LNS shows the physical ingress interface as the source interface for packet flows instead of the virtual-access interface.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.2(28)SB3 and that functions as an LNS when the following configuration is present:

  – The physical ingress interface that faces the LAC is “fas0/0” and has the **ip flow ingress** command enabled.

  – The **flow-sampler one-in-hundred** command is enabled on the virtual-template interface.

  Workaround: Do not enter the **ip flow ingress** command on the physical ingress interface. Rather, enter the **ip flow ingress** command on the virtual-template interface, bring down the tunnel, and then bring up the tunnel.

- CSCsi28884

  Symptoms: The attribute list may not be downloaded for a particular service.

  Conditions: This symptom is observed on a Cisco platform that is configured for AAA when local authorization is configured and when the attribute list is downloaded. The following shows a configuration in which the symptom occurs:

```
policy-map type service abcd
 aaa attribute list cisco
 service local

aaa attribute list cisco
 attribute type addr-pool "cisco" protocol ip
 attribute type ppp-author-list "cisco"
 attribute type ppp-authen-list "cisco"
```

  Workaround: Ensure that the same name is used for the *policy-map-name* argument of the **policy-map type service** *policy-map-name* command (abcd in the example above) and the *list-name* argument of the **aaa attribute list** *list-name* command (Cisco in the example above).

- CSCsi48665

  Symptoms: When you configure SNMPv3 group access to contexts, each context may need to be configured with a separate CLI command. For large configurations, thousands of CLI command may need to be entered, which is not acceptable.

  Conditions: This symptom is observed, for example, when the **snmp-server group** *groupame* **v3 auth context** *context-name* command must be entered for each group and each context. If there are many VLANs, the command must be entered for each group that is given access to each VLAN, which may mean that thousands of CLI command must be entered.

Workaround: SNMP allows you to specify that a context name is a prefix, and match any context that starts with that name. Use SNMP to create rows in the vacmAccessTable and ensure that the vacmAccessContextMatch object is set to a prefix instead of match. Note that after you reboot the router, you must reconfigure this workaround.

- CSCsi80159

  Symptoms: A Cisco router that functions as an ISG may not send RADIUS attribute 44 in the RADIUS Access Request when the **vrf default** keywords are present in the command line, as in the following example:

  ```
  radius-server attribute 44 include-in-access-req vrf default
  ```

  This situation affects the prepaid billing service for ISG-based customers because the billing system cannot re-authorize a subscriber after its quota runs out. The billing system is not able to consolidate the AAA accounting sessions without RADIUS attribute 44 in the RADIUS Access Request for re-authorization. Even if the ISG prepaid threshold is zero, re-authorization fails because the service quota is exhausted, but subscriber's session remains active.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB or one of its rebuilds because in these releases the **vrf default** keywords are added by default.

  Workaround: There is no workaround.

- CSCsj16007

  Symptoms: A PDSN member reloads at find_elt.

  Conditions: This symptom is observed on a PDSN using Cisco IOS Release 12.3 (14)YX8.

  Workaround: There is no workaround.

- CSCsj55691

  Symptoms: There is a crash on the router.

  Conditions: For the problem to occur, there needs to multiple https requests sent in quick succession to an HTTPS server that is up and running, but the service or application processing the request should be unavailable.

  Workaround: There is no workaround.

  Further Problem Description: The crash will not occur if the HTTPS server and the service handling the request are operating normally.

- CSCsj83966

  Symptoms: The message CPU HOG will appear in the screen

  Conditions: When a lot of interfaces are coming up/down at the same time, the syslog use to process 100 trap at one time which causes CPU HOG.

  WorkAround: The condition will not appear if there are comparatively less number of interfaces. Also, unconfigure the trap from sh run will prevent from this issue

- CSCsj89470

  Symptoms: An LNS that has sampled NetFlow enabled may crash.

  Conditions: This symptom is observed on a Cisco 7200 series that functions as an LNS.

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

Interfaces and Bridging

- CSCef80036

  Symptoms: Issuing a microcode reload causes %IPC-5-INVALID message with tracebacks to appear on the router console.

  Conditions: This symptom occurs on a Cisco 7500 (RSP4) series router that is loaded with Cisco IOS Release 12.2(25)S1.

  Workaround: There is no workaround.

- CSCeg55131

  Symptoms: Spurious memory access occurs when removing channel groups in the T1/E1 cards.

  Conditions: This symptom has been observed with a PA-MC-8TE1+ port adapter on a Cisco 7500 router that is running Cisco IOS Release 12.0S.

  Workaround: There is no workaround.

- CSCeh17935

  Symptoms: When you perform an Online Insertion and Removal (OIR) of an ATM port adapter, tracebacks are generated.

  Conditions: This symptom is observed on a Cisco 7200 series when the ATM port adapter is up and has a VC configured, when traffic passes through the ATM interface of the port adapter during the OIR, and when the ATM interface of the port adapter is oversubscribed.

  Workaround: There is no workaround.

- CSCek65222

  Symptoms: A non-parseable Ethernet configuration is nvgened for a VLAN.

  Conditions: This symptom is observed when you enter the **encap dot1q 1 native** command, and the command is rejected. When you enter the **encap dot1q 1** command, the command is accepted. However, in this situation, the output of the **show running-config** command shows that the **encap dot1q 1 native** command is present, which would have been rejected.

  Workaround: There is no workaround.

- CSCek76288

  Symptoms: With MLPoATM configured, a router crashes when using the **show ppp multilink** command after disabling the PA by the **hw-module slot** *slot- number* **stop** command.

  Conditions: This symptom has been observed on a Cisco 7200 NPE-G1 loaded with Cisco IOS interim Release 12.4(13.13)T2.

  Workaround: There is no workaround.

- CSCin46297

  Symptoms: In a High Availability routers set-up having Sonet controllers and configured for Multi-router APS, a SSO switchover will lead to inconsistent Sonet APS state.

  Conditions: The inconsistent APS state is seen only when we do a SSO switchover.

  Workaround: After the SSO switchover, a manual shut/no shut on the Sonet Controller is needed on the new Active Sup card, to restore the correct APS state.

- CSCsf20174

  Symptoms: An enhanced FlexWAN module may reload with certain traffic flows.

Conditions: This symptom is observed rather rarely on a Cisco 7600 when the enhanced FlexWAN module is configured with an ATM port adapter, has 1483 configurations, and processes traffic.

Workaround: There is no workaround.

- CSCsi41769

  Symptoms: A PVC that is shut down by OAM may continue to receive and forward traffic. This situation causes problems in an APS 1+1 redundancy configuration in which the standby router has a PVC that is shut down by OAM but continues to receive all traffic.

  Conditions: This symptom is observed on a Cisco router that has an ATM port adapter.

  Workaround: In an IPv4 configuration, shut down the subinterface manually or enter the **ip verify unicast reverse-path** command. In an MPLS configuration, shut down the subinterface manually.

- CSCsi56413

  Symptoms: The output may be stuck on a POS interface that is configured for Frame Relay encapsulation. When this situation occurs, the output queue is not emptied, and LMI remains down.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(12) or later. This happens only with very specific hardware configurations including NPE-G1 and PA-POS-OC3SMI. The issue observed when aforementioned Port Adapter is located at slot 4 and not seen with other hardware configurations.

  Workaround: Place POS PA in other slot(s). PA location reconfiguration in chassis should fix the problem.

- CSCsi66859

  Symptoms: A router crashes when both “xconnect” and “bridge-group” are configured on an interface and packets are received on that interface.

  Conditions: This symptom happens only when “xconnect” and “bridge-group” are configured on an interface, and packets are received on the interface.

  Workaround: Do not configure both “xconnect” and “bridge-group” on an interface. These commands are mutually exclusive in terms of functionality, so there is no deployment scenario in which they would be configured together.

- CSCsi85935

  Symptoms: Alignment errors drive the router to crash due to a bus error (TLB exception). These reloads can occur about 2-3 times day.

  Conditions: This symptom occurs on a Cisco 3745 with NM-8AM running Cisco IOS Release 12.3(7)T11 and Release 12.4(13a) while there is great volume of the traffic through module NM-8AM. Replacement of all the HW equipment did not solve the issue.

  Workaround: Reduce traffic through NM module or install Cisco IOS 12.3 (not T train or 12.4 image) provokes that reloads stop.

IP Routing Protocols

- CSCdy42103

  Symptoms: A watchdog timeout may cause a software-forced reload on a router.

  Conditions: This symptom is observed on a Cisco 7500 router that is using the Border Gateway Protocol (BGP).

  Workaround: There is no workaround.

- CSCec68752

  Symptoms: A router may crash when you enter a long string for the *name* argument in the **ip nat outside source route-map** *name* **pool** *pool-name* command.

  Conditions: This symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCed68668

  Symptoms: A Cisco router that runs Cisco IOS Release 12.3(5.13)T may reload because of a bus error. The output of the **show version** command may show the following:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xYYYYYYYY
  ```

  Conditions: These symptoms occur when **clear ip nat *** is executed on the CLI.

  Workaround: Do not perform **clear ip nat ***.

  The following link provides general information about bus errors:
  http://www.cisco.com/warp/public/122/crashes_buserror_troubleshooting.shtml

- CSCef24703

  Symptoms: OSPF may continue to originate a default route when using default-information originate route-map xxxx and watching a learned route via bgp to satisfy the route-map. Thus far, this problem has been seen in 12.2 through the most recent 12.3T code.

  Conditions: This problem is observed when the watched route is in the bgp table as an ibgp route, even if the preferred path is the ebgp path.

  Workarounds: Either filter the watched route between the ibgp routers so it isn't learned via ibgp, only ebgp, or use "bgp redistribute-internal" under router bgp instead.

- CSCef41448

  Symptoms: BGP update replication is not good.

  Conditions: This symptom is observed on Cisco IOS 12.2(25.04)S01.

  Workaround: There is no workaround.

- CSCef45830

  Symptoms: A stale BGP route does not time out, which can be observed in the output of the **show ip route vrf** command.

  Conditions: This symptom is observed in a BGP multipath configuration.

  Workaround: Enter the **clear ip route vrf** *vrf-name* command.

- CSCef97738

  Symptoms: BGP may pass an incorrect loopback address to a multicast distribution tree (MDT) component for use as the source of an MDT tunnel.

  Conditions: This symptom is observed when you reload a Cisco router that runs Cisco IOS Release 12.0(28)S1 and when there is more than one source address that is used in BGP, such as Lo0 for IPv4 and Lo10 for VPN. If the IPv4 peer is the last entry in the configuration, the MDT tunnel interface uses lo0 as the source address instead of lo10. The symptom may also occur in other releases.

  Workaround: Remove and add the MDT statement in the VRF.

- CSCeh01390

  Symptoms: MSDP does not create (S,G) state and does not trigger (S,G) joins for the relevant entries in the MSDP cache, when (*,G) changes to Non NULL.

Conditions: This happens only when IGMP modifies the (*,G) olist from NULL to Non-NULL.

Workaround: There is no workaround.

- CSCeh11675

  Symptoms: Ping passes from inside to outside only when the NAT translation entry in NAT router (uut) is empty. When the first ping passes and an entry is made in NAT translation table all further pings fail. Packets are dropped at NAT router, and ICMP, host unreachable messages are returned. When the entry in the NAT translation table expires, ping passes again.

  Workaround: There is no workaround.

- CSCeh15802

  Symptoms: OSPF has been configured to be redistributed into a specific VRF in another routing protocol, which uses the **address-family ipv4 vrf VRFNAME** command. For example:

```
router eigrp 1
  address-family ipv4 vrf vrf1
  redistribute ospf 32 vrf vrf1
```

  But using the **show run** command, the VRF is not seen on the redistribute command line. For example:

```
router eigrp 1
 auto-summary
 !
 address-family ipv4 vrf vrf1
 redistribute ospf 32
 auto-summary
 exit-address-family
```

  This is incorrect, and after reload, the OSPF process will be created such that it is attached to the default routing table instead of the VRF.

  Conditions:

  – OSPF process is associated to a VRF

  – OSPF is redistributed in EIGRP address-family vrf

  Workaround: There is no workaround.

- CSCeh49504

  Symptoms: BGP redistribution into EIGRP based on a standard community or AS path does not work as expected.

  Conditions: This symptom is observed when the **match community** or **match as-path** route-map commands are enabled.

  Workaround: There are two steps to this workaround:

  1. Apply an inbound route map on the BGP neighbor. The inbound route map must include the **set metric** command to set the BGP multi-exit discriminator (MED) based on the standard community or AS path.
  2. Match on the BGP MED in the route map that is used in the BGP redistribution.

  Further Problem Description: Set actions in one particular statement that includes the **match community** or **match as-path** command are applied to all routes that match any subsequent statement in the same route map, instead of only to the routes that match the particular statement to which the set actions were applied.

- CSCej78303

  Symptoms: A router may crash when you disable the **ipv6 multicast-routing** command.

  Conditions: This symptom is observed when you enable and disable the **ipv6 multicast-routing** command multiple times while IPv6 Multicast traffic is being processed.

  Workaround: There is no workaround.

- CSCek35039

  Symptoms: A route map may not match a BGP IP next-hop address in the VPNv4 table.

  Conditions: This symptom is observed on a Cisco router when a route map is used to control the redistribution of BGP into EIGRP by matching the IP next-hop address.

  Workaround: There is no workaround.

- CSCek64468

  Symptoms: TE tunnels do not come up in the rsvp_aggregation branch.

  Conditions: This symptom occurs with the development image trying to setup TE tunnels.

  Workaround: There is no workaround.

- CSCek68469

  Symptoms: A router may reload during the “ip_static_delete_dlroute_entry” process.

  Conditions: This symptom is observed when you enter the **no aaa route download 5** command.

  Workaround: There is no workaround.

- CSCek78315

  Symptoms: A router may give spurious memory access or crash when the **debug ip ospf hello** command is enabled on the router, which has sham-links configured.

  Conditions: This symptom has been observed with sham-links configured. Only Cisco IOS images with the fix CSCse35155 integrated are affected. The **debug ip ospf hello** command is enabled during the adjacency start on the sham-link interface.

  Workaround: Do not start the **debug ip ospf hello** command in a sham-link environment.

- CSCsa53394

  Symptoms: When SNMP traps are generated on a Cisco IOS router the s**how alignment** command displays spurious memory access and tracebacks in the OSPF trap generation routine.

  Conditions: This symptom occurs on a router that is running Cisco IOS Release 12.2(18)SX with the Open Shortest Path First (OSPF) MIB.

  Workarounds: There is no workaround.

- CSCsa65155

  Symptoms: IS-IS may not update redistributed BGP network changes.

  Conditions: This symptom is observed when the **network** *network-number* command is enabled to introduce connected networks into a BGP topology and when, afterwards, BGP is redistributed into IS-IS. The symptom occurs after one of the interfaces that forms a network connection goes down and comes up again; the network re-enters the BGP topology but is no longer redistributed into IS-IS.

  Workaround: There is no workaround.

- CSCsb85290

  Symptoms: Reverse Path Forwarding may not occur for IPv6 Bootstrap Router message (BSM) packets.

  Conditions: This symptom is observed on a Cisco platform that receives and needs to forward BSMs.

  Workaround: There is no workaround.

- CSCsc35609

  Symptoms: In certain circumstances, if the static reservations are configured via the **ip rsvp listener** commands, an interface going down can cause the router to crash.

  Conditions: This problem is seen under the following conditions:

  1. Router is running RSVP; the **ip rsvp bandwidth** command is enabled.
  2. Router has configured a receiver proxy with the **ip rsvp listener** command.
  3. Router receives Path messages matching the proxy and sends out Resv messages corresponding to the received Path messages.
  4. The interface on which the Path message is received goes down.

  The problem is not seen if any of these conditions do not hold. For example, routers not running RSVP, or running RSVP only as a midpoint, or routers running MPLS/TE, do not see this problem.

  Workaround: There is no workaround. Discontinuing the use of the **ip rsvp listener** command will prevent the crash.

- CSCsc96746

  Symptoms: PIM may not select the path with the highest IP address when it should do so.

  Conditions: This symptom is observed on a Cisco router that functions in a topology with equal-cost RPF paths.

  Workaround: There is no workaround.

- CSCsc98828

  Symptoms: PIM becomes disabled on an output interface, preventing packets from being sent, and causing the SR flag to be set after 60 seconds on the router that functions as the first hop.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 PIM.

  Workaround: There is no workaround.

- CSCsd39528

  Symptoms: Duplicate Interface Index (ifIndex) numbers may be assigned to the multicast tunnel interfaces. This situation may prevent traffic from being switched from these multicast interfaces, and may cause the router to crash with a bus error when these multicast tunnels are deleted and then re-created.

  You can verify that the symptom has occurred by entering the **show idb** command and by looking for duplicate ifIndex entries for the multicast tunnel interfaces.

  Conditions: This symptom is observed on a Cisco router that is configured with IPv6 PIM tunnels.

  Workaround: There is no workaround.

- CSCsd63038

  Symptoms: An MDT address-family session in a BGP environment may not come up between two PE routers. This situation prevents the tunnel interface from being shown in the output of the **show ip pim vrf** *vrf-name* **neighbor** command on one of the PE routers.

Conditions: This symptom is observed on PE routers that are configured for Multicast VPN and that have the following commands enabled:

address-family ipv4 mdt

neighbor *neighbor-ip-address* **activate neighbor**

neighbor *neighbor-ip-address* **send-community extended**

Workaround: Reconfigure the **address-family ipv4 mdt** command in the BGP environment.

- CSCsd68993

  Symptoms: IPv6 multicast traffic forwarding may fluctuate.

  Conditions: This symptom is observed on a Cisco router that is configured for PIM and that is configured with more than 2000 multicast streams.

  Workaround: There is no workaround.

- CSCse05106

  Symptoms: When NAT is configured and flow is sent, no netflow entries are software-installed, and no shortcut is created.

  Conditions: This symptom occurs if no netflow IP entries are software-installed.

  Workaround: There is no workaround.

- CSCsg07742

  Symptoms: The attributes that are configured in a site map may not automatically be applied to the BGP table when the associated interface is running other routing protocols such as RIP or OSPF.

  Conditions: This symptom is observed on a Cisco router when routes are redistributed into BGP.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the associated interface.

- CSCsg84690

  Symptoms: A default route with an incorrect mask may not be installed.

  Conditions: This symptom is observed on a Cisco router that is configured for OSPF.

  Workaround: There is no workaround.

- CSCsh12384

  Symptoms: Removing a loopback interface when RSVP sessions are active causes a traceback.

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

  Workaround: There is no workaround. However, there is no functional impact to the router.

- CSCsh14457

  Symptoms: A Cisco router that is running modular image (-vz- version) configured for OSPF and BFD may experience corner case crash.

  Conditions: This symptom occurs with a high number of very unstable OSPF/BFD neighbors.

  Workaround: Upgrade to fixed software version.

- CSCsh20140

  Symptoms: A small memory leak may occur when ISPF is enabled. When you deconfigure OSPF, the following error message and traceback are generated:

  ```
  %SYS-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk
  30E3268.
  ```

```
-Process= "Exec", ipl= 0, pid= 3,
-Traceback= 0x69F968 0x813670 0x8137C4 0xD57928 0xD6A230 0xB37824 0xB38550
0x6E33F0 0x706EBC 0x7ABDD0 0x7ABDCC
```

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsb38978. A list of the affected releases can be found at http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsb38978. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: Do not configure ISPF.

- CSCsh42565

  Symptoms: Traffic engineering (TE) tunnels go down when an intermediate link has the **ip ospf network non-broadcast** command enabled.

  Conditions: This symptom is observed in an OSPF network over TE tunnels that are established on non-broadcast links.

  Workaround: Do not use non-broadcast links. Rather, use another OSPF network type. If this is not an option, there is no workaround.

- CSCsh68376

  Symptoms: Routes that are learned from a route reflector may not be refreshed.

  Conditions: This symptom is observed on a Cisco router that is configured for EBGP.

  Workaround: Perform a soft clear on the affected router to refresh the route.

- CSCsh96955

  Symptoms: The next hop for a BGP route is marked as "inaccessible," preventing the route from being advertised to peers or installed in the routing table.

  Conditions: This symptom is observed on a Cisco router when all of the following conditions are present:

  – The route is an IPv6 route with an IPv6 next hop.
  – The route is learned from an IPv6 eBGP router that is one hop away.
  – Peering occurs between loopback addresses.
  – The **disable-connected-check** command is configured for the peer from which the route is learned.

  Workaround: Disable the **disable-connected-check** command on the peer from which the route is learned. Rather, configure eBGP multihop.

- CSCsi01481

  Symptoms: Error messages are seen when the IPv6 Static RP address is unconfigured.

  Conditions: This problem is a platform independent failure.

  Workaround: There is no workaround.

- CSCsi16903

  Symptoms: An IGMPv3 mode 4 group report with empty source list {} gets translated incorrectly to a mode 6 group report when using an ssm-mapped source. Expected behavior would be to translate to a mode 5 group report.

  Conditions: This symptom occurs when IGMPv3 mode 4 group report with empty source list {} is translated by static ssm-map.

Workaround: Avoid using empty source list {} by specifying source and therefore not needing SSM static mapping.

- CSCsi33147

  Symptoms: Prefix LSA does not get updated after interface un-shutdown.

  Workaround: There is no workaround. Bounce the interface again will fix the issue.

  Further Problem Description: This is rare timing issue. So far it is seen in a lab only when virtual link is configured.

- CSCsi35541

  Symptoms: An CPUHOG may be experienced after executing the **clear ip route *** command.

  Conditions:

  – Many connected routes, CPUHOG seen with 1000+ subinterfaces.

  – OSPF process which is not running, because it can not pick up a router-id.

  Workaround: Avoid having configured OSPF process which can not start because no router-id is available.

- CSCsi47635

  Symptoms: The configuration of a deleted subinterface may show up on a new subinterface and may cause a traffic outage.

  Conditions: This symptom is observed on a Cisco router that has IP interface commands enabled when a script adds and deletes ATM subinterfaces on a regular basis.

  Workaround: Verify the subinterface configuration. When the configuration of a subinterface cannot be deleted, delete the subinterface, and then create a dummy subinterface that will pull the configuration that could not be deleted. Then recreate the first subinterface with a new configuration.

- CSCsi48304

  Symptoms: After a reload, the following error message may be displayed if an OSPFv3 router redistributes large numbers of the external routes:

  ```
  %OSPFv3-3-DBEXIST: DB already exist
  ```

  No impact to the operation of the router has been observed.

  Conditions: Redistribution is configured, then router is reloaded.

  Workaround: There is no workaround.

- CSCsi59438

  Symptoms: When you enter the **ip multicast limit rpf** command, protection may fail after the RPF link becomes operational.

  Conditions: This symptom is observed on a Cisco router that is configured for APS switchover.

  Workaround: Clear the state of the corresponding multicast route by entering the **clear ip mroute** command.

- CSCsi97586

  Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

  Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

  Workaround: There is no workaround.

- CSCsj00161

  Symptoms: OSPFv3 may install into the routing table IPv6 routes load balancing between paths to Null0 and reachability path over the physical interface.

  Conditions: This problem may be seen if the **summary-address** command is configured with exactly the same address as one of external routes received from a different router.

  Workaround: There is no workaround.

- CSCsj15027

  Symptoms: If the length field of the message header is less than 19 or greater than 4096, then the Error Subcode MUST be set to Bad Message Length. The Data field MUST contain the erroneous Length field in the notification message, but those are not set in notification message.

  Workaround: There is no workaround.

- CSCsl49628

  Symptoms: When a VRF is deleted through the CLI, the VRF deletion never completes on the standby RP and the VRF cannot be reconfigured at a later time.

  Conditions: This symptom is observed when BGP is enabled on the router.

  Workaround: There is no workaround.

- CSCsl65407

  Symptoms: A routing loop was formed in MPLS/VPN network topology with EIGRP as the PE-CE routing protocol.

  A receiving Provider Edge (PE) router does not update the EIGRP topology entry for a prefix to match the metric information advertised in the BGP ext.community attribute from the neighboring PE router.

  EIGRP is ignoring the metric information within the BGP ext. community attribute and opting to use the metric defined within the **redistribute bgp** *AS* **metric k1 k2 k3 k4 k5** command.

  Workaround: As a temporary solution, modify the **redistribute bgp** *AS* **metric k1 k2 k3 k4 k5** command to **redistribute bgp** *AS* and then add a **default-metric k1 k2 k3 k4 k5** command. Clearing the routing table of the PE may be necessary as well.

- CSCuk54975

  Symptoms: Routes are not redistributed into BGP and network statements to originate routes in BGP do not work.

  Conditions: This symptom is observed when the **redistribute static** command is enabled.

  Workaround: There is no workaround.

ISO CLNS

- CSCei36669

  Symptoms: A CPUHOG and traceback occur when a malicious IS-IS LSP packet is received.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S.

  Workaround: There is no workaround.

- CSCsh63324

  Symptoms: The following error message may be generated when IS-IS is configured:

```
%SYS-2-CHUNKPARTIAL: chuck name ISIS NSF cp ch
```

Conditions: This symptom is observed on a Cisco router that functions in an MPLS configuration when the **nsf cisco** command is configured under the **router isis** command.

Workaround: There is no workaround. However, the error message appears to be of a cosmetic nature and does not appear to affect the functionality of the router.

- CSCuk55515

  Symptoms: Fifty percent of the packets that are destined for an IP-over-CLNS tunnel (CTunnel) are dropped by CEF.

  Conditions: This symptom is observed when the router is configured for IPv4 CEF switching and when the next hop for the CEF-switched packets must be reached via the CTunnel.

  Workaround: There is no workaround.

Miscellaneous

- CSCdv07156

  Symptoms: A router that is configured with thousands of RIP routes may crash when multiple links flap.

  Conditions: This symptom is observed on a Cisco router that is configured for RIP.

  Workaround: There is no workaround.

- CSCeb02520

  Symptoms: A Cisco Route Processor Module (RPM-PR) router that is configured as an Edge Label Switch Router (ELSR) may reset when you enter the **show queue sw1** EXEC command when there is a Multiprotocol Label Switching (MPLS) interface.

  Conditions: This symptom is observed on a Cisco RPM-PR when multiple virtual circuits (VCs) are enabled under an MPLS interface. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCeb77318

  Symptoms: When a load-balanced server uses the Don’t Fragment (DF) bit in its responses, and fragmentation is needed in order to reach the client, a gateway may report this situation by using Internet Control Message Protocol (ICMP), message type 3 (destination unreachable), code 4 (datagram too big). The gateway message is translated at a router and forwarded to the correct server, but the checksum may be invalid, causing the server to ignore the message and preventing the segment size from being decreased.

  Conditions: This symptom is observed when you use Cisco IOS Server Load Balancing (SLB) with Network Address Translation (NAT).

  Workaround: Do not configure NAT when you use Cisco IOS SLB.

- CSCeb78526

  Symptoms: A router that is configured for LAN Emulation (LANE) may reload because of a bus error, and the following error message may appear:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX
  ```

  Conditions: This symptom is observed on a Cisco router only when the creation of switched virtual circuits (SVCs) fails.

  Workaround: There is no workaround.

- CSCec90275

  Symptoms: Packets are duplicated on the Provider Edge (PE) router. A packet is switched out once in the fast switching path and another time in the process path.

  Conditions: This symptom is observed when the path between the source and the receiver goes through multiple PE routers, and all the PEs have fast-switching enabled.

  Workaround: Unconfiguring ip mroute-cache from the interfaces solves the duplication.

- CSCed76056

  Symptoms: TTL is not decreased for packets, coming from GRE Tunnel interface, when CEF is enabled.

  Conditions: This symptom was seen on Cisco 2600 and Cisco 3725 routers that are running Cisco IOS Release 12.3(6).

  Workaround: Configure the **no ip route-cach cef** command on Tunnel interface.

- CSCee20888

  Symptoms: IPv6 over ISDN does not work.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(7)T1.

  Workaround: There is no workaround.

- CSCee49035

  Symptoms: An incorrect update-source interface is selected for a multicast tunnel interface in an MVPN configuration.

  Conditions: This symptom is observed when the provider edge (PE) router is also an ASBR with eBGP peers or has non-VPNv4 peers with higher IP addresses than the peer that has VPNv4 enabled. MVPN requires that the BGP update source address of a VPNv4 peer is selected as the MTI source address.

  Workaround: There is no workaround.

- CSCee66058

  Symptoms: SNMP users that have MD5 configured may become lost after a switchover in an RPR+ environment.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 12000 series that run Cisco IOS Release 12.0(27)S1 in RPR+ mode.

  Workaround: There is no workaround.

- CSCee77867

  Symptoms: A standby PRP that functions in SSO mode continues to reset.

  Conditions: This symptom is observed on a Cisco 12406 that runs a Cisco IOS interim release for Release 12.0(29)S and that is has an ATM VC bundle configuration.

  Workaround: Reload the standby PRP without the ATM VC bundle and re-apply the ATM VC bundle after the standby PRP has booted.

- CSCee78208

  Symptoms: When IP TCP header compression is configured over a PPP link attached to a Cisco 7200 router which has an LLQ service policy attached to the PPP link, the LLQ rates that are being seen at the other end of the PPP link are much less than the configured rate.

  Workaround: There is no workaround.

- CSCee93228

  Symptoms: Under certain unknown circumstances, a traceroute may trigger a process watchdog.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S2. However, the problem is not specific to a Cisco 12000 series or to Cisco IOS Release 12.0S and may occur on other platforms and in Release 12.2T and Release 12.3.

  Workaround: There is no workaround.

- CSCef62324

  Symptoms: Router may crash upon removal of an ATM subinterface with PVCs.

  Workaround: There is no workaround.

- CSCef85231

  Symptoms: When SSO redundancy mode is configured and you enter the **no** form of the **mpls ldp neighbor targeted** command to deconfigure a previously configured command, the standby RP may reload. The symptom may also occur when you enter the **no** form of the **mpls ldp neighbor implicit-withdraw** command. For example, any of the following command sequences may cause the symptom to occur:

  ```
  Example 1:
  mpls ldp neighbor 10.0.0.1 targeted ldp
  ...
  no mpls ldp neighbor 10.0.0.1 targeted ldp

  Example 2:
  mpls ldp neighbor 10.0.0.1 targeted ldp
  ...
  no mpls ldp neighbor 10.0.0.1 implicit-withdraw
  ```

  Conditions: This symptom is observed when the **mpls ldp neighbor targeted** command is configured and when the Label Distribution Protocol (LDP) is globally disabled. (By default, LDP is globally enabled, but it can be disabled by entering the **no mpls ip** global configuration command.) The symptom does not occur when other commands are configured for the specific neighbor, for example, if an MD5 password is configured for the neighbor as illustrated in the command sequence below:

  ```
  no mpls ip
  mpls ldp neighbor 10.0.0.1 targeted ldp
  mpls ldp neighbor 10.0.0.1 password foo
  no mpls ldp neighbor 10.0.0.1 targeted ldp
  ```

  This symptom occurs in releases that integrate the fix for caveat CSCee12408. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee12408.

  Workaround: Configure a password for the neighbor as shown in the Conditions above before you enter the **no** form of the **mpls ldp neighbor targeted** command or the **no** form of the **mpls ldp neighbor implicit-withdraw** command.

- CSCeg27616

  Symptoms: CE to PE ping loss through VRF cloud when CEF is turned on PE.

  Conditions: The problem is seen on Cisco routers that are running Cisco IOS Release 12.2(27.1)S.

  Workaround: There is no workaround.

- CSCeh06200

  Symptoms: You may not be able to gain access to a router via HTTP when the idle time is set on a TACACS server. Telnet via TACACS works as expected.

  Conditions: This symptom is observed on a Cisco router that functions as an Access Point (AP) and that is configured for TACACS.

  Workaround: There is no workaround.

- CSCeh32706

  Symptoms: An inter-AS TE LSP fails to send a signal after a router is rebooted as an ASBR.

  Conditions: This symptom is observed when there are parallel links between ASBRs with a combination of point-to-point and broadcast interfaces that are configured with the MPLS Traffic Engineering--Inter-AS TE feature and (passive) link flooding.

  Workaround: Shut down the broadcast interface between the ASBRs.

- CSCeh52330

  Symptoms: When using SPA-CT3 in a SIP1 module the following error message might appear on the console screen.

  ```
  SLOT 7: 06:46:34: %INTR_MGR-3-INTR: SPA-4XCT3/DS0[7/0] EFC Parity Error
  06:46:34: %Fatal Error: Hardware error (EFC Parity Error) detected for SPA 7/0
  ```

  Conditions: This error message would appear if the T3 controller flaps continuously for a long time.

  Workaround: There is no workaround.

  Further Problem Description: Apart from the above error message appearing on the console, there are no apparent side effects because of it. The interfaces continue to function normally.

- CSCeh59149

  Symptoms: An “%ATM-3-FAILCREATEVC: ATM fails to create VC” error, and tracebacks are seen when trying to configure a new ATM PVC.

  Conditions: This problem is seen when trying to create new ATM PVCs following a redundancy force-switchover.

  Workaround: There is no workaround.

- CSCeh66159

  Symptoms: Pim interface counters on the incoming interface do not reflect the traffic stats correctly.

  Conditions: This is seen to happen with MDS (multicast distributed switching) is enabled on the router.

  Workaround: There is no workaround.

- CSCeh71960

  Symptoms: Alignment traceback will be shown on Standby RP after SSO.

  Conditions: This problem occurs when ATM interfaces are present in the configuration.

  Workaround: There is no workaround.

- CSCeh72672

  Symptoms: After a switchover two VRF aggr labels are seen.

  Conditions: This problem is observed if the BGP graceful restart is not configured and after a switchover.

  Workaround: Configure BGP graceful restart.

- CSCei39688

  Symptoms: When a CEF initialization failure occurs, an ATM PVC that is configured for OAM may not pass traffic even though the PVC link status is up:

```
Router#show ip interface brief | include ATM
ATM3/0/0                   unassigned      YES manual up      up
ATM3/0/0.100               unassigned      YES unset  up      up
ATM3/0/0.300               10.1.1.1        YES manual up      up
ATM3/0/0.999               unassigned      YES unset  up      up

Router#show cef interface brief | include ATM
ATM3/0/0                        unassigned      up      dCEF
ATM3/0/0.100                    unassigned      down    dCEF
ATM3/0/0.300                    10.1.1.1        down    dCEF
ATM3/0/0.999                    unassigned      down    dCEF

Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached             ATM3/0/0.300
```

  When CEF fails to initialize the ATM PVC, atm3/0/0.300, no /32 receive entries are created. Traffic that is destined for the IP address of the subinterface is dropped.

  Conditions: This symptom is observed on a Cisco router and occurs only when OAM is configured on the PVC.

  Workaround: To prevent the symptom from occurring, do not configure OAM on the PVC. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ATM subinterface. After the workaround has been applied, the output of the **show ip cef** command shows the following:

```
Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached             ATM3/0/0.300
10.1.1.0/32     receive
10.1.1.1/32     receive
10.1.1.3/32     receive
```

- CSCei58681

  Symptoms: Port does not come up in a Port channel

  Conditions: This symptom is observed when converting L2 port channel into L3 port channel then removing the minimum links command and do a Shut/NO Shut on the member port.

  Workaround: Reset the associated line card where the port channel member does not come up.

- CSCei59601

  Symptoms: A Cisco 7200 series router unexpectedly reloads.

  Conditions: This behavior is observed on Cisco IOS Release 12.2(28.05.06)SX.

  Workaround: There is no workaround.

- CSCei67410

  Symptoms: A router may crash when a rare race condition occurs between the Virtual Exec/Exec process and processes that contend with the resources that are used during the execution of the **show sss session all** command.

Conditions: This symptom is observed on a Cisco router that functions as an ISG when the router accesses memory that was overwritten by another process.

Workaround: Avoid entering the **show sss session all** command while the circuit state change. If this is not an option, there is no workaround.

- CSCei67700

  Symptoms: frde failed to match control packets on FR over AToM

  Conditions: The problem can be observed on a Cisco 7500 router.

  Workaround: There is no workaround.

- CSCei68902

  Symptoms: With around 15 MFR bundles, router reloads and sometimes spa_reload leads to some of the bundles staying in down state.

  Conditions: The router needs to have a SPA-CTE1 configured for Multilink Frame-relay and the LC or the SPA needs to be reloaded to hit.

  Workaround: One or two reloads of the SPA should recover the problem

  Further Problem Description: This problem has not yet been seen on SPA-CTE1. It has only been seen on a SPA-CT3. Since both share the design where the problem has been fixed, this DDTS is going to track the fix for SPA-CTE1

- CSCei83160

  Symptoms: PIM neighbors do not recognize each other via a VRF tunnel interface because multicast does not receive MDT updates from BGP. The output of the **show log** command shows the following debug message:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (3) received in update for prefix
  2:55:1111:192.168.31.1/32 from 192.168.31.1
  ```

  Conditions: This symptom is observed on a Cisco router and is not platform-dependent. The symptom occurs when a VRF instance is configured with BGP as the Exterior Gateway Protocol (EGP).

  Workaround: There is no workaround.

- CSCei92291

  Symptoms: A customer who is running Cisco Catalyst 6500 in native mode with Cisco IOS 12.2SXF software may encounter “Error in setting Reload Reason” error message at the time of write memory.

  Workaround: There is no workaround.

- CSCei93090

  Symptoms: EIGRP does not learn routes when the **ip pim sparse-dense-mode** command is configured on a Gigabit Ethernet interface.

  Conditions: This symptom is observed on a Cisco 7301 that runs Cisco IOS interim Release 12.4(4.3).

  Workaround: There is no workaround.

- CSCej21515

  Symptoms: ATM SPA SRAM parity or SDRAM ECC errors may occur if the SPA was brought up at one temperature and there is then a significant change in temperature. In the case of SRAM parity errors, the SPA will be reset. In the case of ECC errors, the corrupted packet will be dropped, and the SPA will continue operating normally.

Conditions: This problem would only be seen when there is a significant temperature change from the time when the SPA was initialized. Only a small percentage of ATM SPAs may see this problem and even those that are at risk will not come up in this state every time the card is initialized.

Workaround: There is no workaround.

- CSCej21520

  Symptoms: In HA environment, removing “aps protect 1” from ATM SPA interface, can cause console lock for a few minutes.

  Conditions: Router should be a 7600, with a secondary supervisor, and APS configured on an ATM SPA.

  Workarounds:

  1. User reloads the *secondary* supervisor (by using the **redundancy reload peer** command) and then issues a **no aps protect 1** command, while the secondary supervisor is still booting.
  2. User connects a console cable to the secondary supervisor and responds to the **no aps protect 1** command on the secondary console also.

- CSCej31343

  Symptoms: Active RP crash when unconfiguring ip vrf vpn after SSO.

  Conditions: Problem is found on HA-SSO capable routers with Cisco IOS Release 12.2(31.4)S image.

  Workaround: There is no workaround.

- CSCej83531

  Symptoms: The test failed at ping to dns-server in subtest change_hostname_ip of ipsec_realTimeDNs testing.

  Conditions: The above symptom happens on Cisco routers with Cisco IOS Release 12.4(4.7)PI3c.

  Workaround: There is no workaround.

- CSCek24782

  Symptoms: A Cisco platform that is configured for ISDN and AAA may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 5400XM that functions under stress. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCek26296

  Symptoms: Service policy configured with a single bandwidth+shape class it is not getting the guarantee.

  Conditions: Problem is seen on OSM-8OC3-POS interface with Cisco 7600 Sup3 router

  Workaround: There is no workaround.

- CSCek26742

  Symptoms: The line protocol remains down on SPA-8XCHT1E1 after rpr+ switchover. This issue is seen only on the Cisco 7600 router and not on Cisco 12000 series router.

  Conditions: A SPA-8XCHT1E1 needs to be present in the Cisco 7600 system.

  Workaround: There is no workaround.

- CSCek27892

  Symptoms: Disordered output of show policy-map.

Conditions: It can be observed on Cisco 7500 and Cisco 7200 platform.

Workaround: There is no workaround.

- CSCek30891

  Symptoms: Traffic loss may occur during reoptimization on a Cisco router that functions as a transit node for zero-bandwidth MPLS TE label switched paths (LSPs). The traffic loss stops when the TE tunnel headend switches traffic over to the new LSP.

  Conditions: This symptom is observed on a Cisco router when reoptimization is triggered on the headend either periodically, manually, or as a result of a topology change.

  Workaround: There is no workaround.

- CSCek34117

  Symptoms: The SIP200, installed with ATM SPA, would crash under scalability configuration + MQC QoS applied.

  Conditions: Interface flapping occurs under traffics.

  Workaround: There is no workaround.

- CSCek37085

  Symptoms: The **service-policy output** *policy-map-name* control-plane configuration command does not function.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCek39331

  Symptoms: In a FR MBP scenario, on the DTE side, a FR subinterface in shutdown state continues to receive and forward traffic.

  Conditions: This behavior is seen on SIP200, SIP400, FW2 and may impact other line cards on Cisco 7600.

  Workaround: There is no workaround.

- CSCek39946

  Symptoms: Ping failure or no connectivity with ATM Local switching after SSO Switchover

  Conditions: Configure ATM local switching with SIP-200 Linecard and ATM OC3 SPA on a redundant system that has been configured with Stateful Switchover (SSO). Perform a forced switchover and verify connectivity after the standby supervisor becomes active.

  Workaround: Do shut & no shut on the atm interfaces where connect has done. Show connect will show as up, then local switching will work. Ping will go pass after this.

- CSCek41338

  Symptoms: A router reloads when you enter the **peer default ipv6 address pool** *pool-name* command in template-configuration mode.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6.

  Workaround: A workaround is not applicable because the **peer default ipv6 address pool** *pool-name* command in template-configuration mode is not supported in an IPv6 configuration and should not be entered as such.

- CSCek42751

  Symptoms: The running configuration may not be accessible after you have copied a small file to the running configuration.

Conditions: This symptom is observed on a Cisco router that has an ATA file system after you have rebooted the router.

Workaround: Reboot the router once more.

- CSCek44532

  Symptoms: A standby RP may reload repeatedly when you enter the **issu loadversion** command during a period of high checkpointing activity. When you enter the **show checkpoint statistics** command on the active RP, the output shows that the checkpointing IPC flow control status remains set to zero indefinitely:

  ```
  CHKPT FLOW_ON status = 0
  ```

  Conditions: This symptom is observed on a Cisco router when the standby RP reloads as part of the In-Service Software Upgrade (ISSU) process while, for example, a large number of PPPoA sessions are being disconnected.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command to cancel the ISSU process, and then reload the router.

- CSCek44674

  Symptoms: Ping failed Across Network from Source CE1 to Dest CE3.

  Conditions: The symptom occurs on Cisco 7600 router that is running Cisco IOS Release 12.2(32.8.11)SR and Release 12.2(32.8.1)SRA.

  Workaround: There is no workaround.

- CSCek49107

  Symptoms: A router crashes when you unconfigure and then reconfigure MLPoFR.

  Conditions: This symptom is observed on a Cisco router that has a QoS service policy with traffic shaping.

  Workaround: There is no workaround.

- CSCek51851

  Symptoms: When more on slavenvram:startup-config is in progress and switchover is performed, the standby keeps constantly reloading and does not come up.

  Conditions: This problem is seen on Sup720 platforms.

  Workaround: There is no workaround.

- CSCek53704

  Symptoms: When you first configure and attach more than 255 class maps in a single policy to an interface and when you then remove the policy map, the router crashes.

  Conditions: This symptom is observed on a Cisco router and occurs because a maximum of 255 class maps (that is, 254 user-defined class maps and one default class map) are supported in a single policy map.

  Workaround: There is no workaround. Ensure that you do not configure more than 255 class maps, including the default class map, in a single policy map.

- CSCek57267

  Symptoms: CPUHOG and IPCOIR errors may occur on a Cisco router when you change the IP address of a loopback interface that is associated with a large number of active PPP sessions.

  Conditions: This symptom is observed on a Cisco 10000 series that runs slowly when interfaces flap. The symptom is platform-independent.

Workaround: There is no workaround.

- CSCek59453

  Symptoms: When you configure an ATM VC on which PPPoE sessions are established, a spurious memory access may be generated.

  Conditions: This symptom is observed on a Cisco router when the VC is torn down.

  Workaround: There is no workaround.

- CSCek60629

  Symptoms: A Cisco 10000 series may crash because of an address error (that is, a load or instruction fetch exception) when multiple combined command-line interface (CLI) changes are made.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for RPR+ when you attempt to make multiple policy map changes on a PVC that has a small number of active sessions with a moderate amount of downstream traffic. The symptom appears to be both platform- and release-independent.

  Workaround: There is no workaround.

- CSCek64188

  Symptoms: An error message indicating memory leak and pending transmission for IPC messages is displayed as follows:

  ```
  *Dec  3 01:31:31.792: %IPC-5-WATERMARK: 25642 messages pending in xmt for the
  port Primary RFS Server Port(10000.C) from source seat 2150000
  *Dec  3 01:32:01.489: %SYS-2-MALLOCFAIL: Memory allocation of 4268 bytes
  failed from 0x9F32944, alignment 32
  ```

  Conditions: This issue is triggered by CSCeb05456 and is applicable only if your Cisco IOS image has integrated the fix of CSCeb05456.

  Workaround: Periodically, reload the router so that the IPC buffer pool will be reinitialized.

- CSCek67698

  Symptoms: A session cannot be set up because you cannot apply a service policy to the session.

  Conditions: This symptom is observed on a Cisco router when a VRF is present in the service profile of an IP-routed subscriber and when the initiator is configured for DHCP.

  Workaround: Remove the VRF from the service profile.

- CSCek67782

  Symptoms: When you enable or disable the **fair-queue** or **random-detect** command, the router may unexpectedly reload because of a TLB exception.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek67845

  Symptoms: SSO and ISSU may not function for PPP- and MLP-related links.

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

  Workaround: There is no workaround.

- CSCek68014

  Symptoms: After a router is reloaded through a Telnet session via vty lines, the router may wait for an input character on the console instead of booting up.

Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G2 when you perform a remote upgrade.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **reload** command via the console.

- CSCek68047

  Symptoms: Authentication may be skipped during account logon.

  Conditions: This symptom is observed when an IP session is brought up with a default service before account logon.

  Workaround: Do not configure a default service before account logon.

- CSCek71346

  Symptoms: The MPLS forwarding table is not shown on a router, causing packet drops in end-to-end connectivity across the MPLS cloud.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router after a switchover has occurred.

  Workaround: There is no workaround.

- CSCek71514

  Symptoms: On a Cisco router that has the **mpls ldp igp sync delay** *delay-time* command enabled, the master timer may be accessed prior to being initialized, and the following error message is generated:

  ```
  %SYS-3-MGDTIMER: Uninitialized timer, init with uninitialized master, timer = 53E62C0.
  -Process= "Init", ipl= 0, pid= 3
  ```

  Because the master timer was not properly initialized, other symptoms may occur, including the following:

  – When the LDP session comes up, further error messages and a traceback regarding the master timer may be generated:

  ```
  LDP-SYNC: Et1/0: Delay notifying IGP of sync achieved for 60 seconds R1
  (config)#
  %SYS-3-MGDTIMER: Uninitialized timer, set_exptime_internal, timer = 198A980.
  -Process= "Tag Control", ipl= 0, pid= 61
  -Traceback= 2AEAE4 3642DC 364580 364ADC 364BAC 9BF154 9C22C0 9C24D8 9D4500
  9CD544 9D1C8C 34AD58 34AD54
  ```

  – When the “Delay notification” error message is generated (see above), the output of the **show mpls ldp igp sync** command may shows “0 seconds left” for the synchronization delay time, which contradicts the “Delay notification” error message:

  ```
  LDP-SYNC: Et1/0: Delay notifying IGP of sync achieved for 60 seconds R1
  (config)#
  %SYS-3-MGDTIMER: Uninitialized timer, set_exptime_internal, timer = 198A980.
  -Process= "Tag Control", ipl= 0, pid= 61
  -Traceback= 2AEAE4 3642DC 364580 364ADC 364BAC 9BF154 9C22C0 9C24D8 9D4500
  9CD544 9D1C8C 34AD58 34AD54
  ```

  – OSPF may remain in the “sending maximum metric” state, and the routing table may not be updated, as can be shown in the output of the **show ip ospf mpls ldp interface** command:

  ```
  R1#show ip ospf mpls ldp interface
  Ethernet1/0
  ```

```
Process ID 1, Area 0
LDP is not configured through LDP autoconfig
LDP-IGP Synchronization : Required
Holddown timer is not configured
Interface is up and sending maximum metric
```

Conditions: These symptoms are observed when an RPR+ switchover has occurred or when you configure the **mpls ldp igp sync delay** *delay-time* command while LDP is not enabled or while LDP is enabled but not fully active (for example, when all the interfaces are down).

Workaround: There is no workaround to prevent the initial error message and traceback from being generated. However, after the initial error message and traceback have been generated, you can prevent any further symptoms from occurring by reconfiguring the synchronization timer and re-enabling the **mpls ldp igp sync delay** *delay-time* command on the affected interface as in the following example:

```
R1(config-if) no mpls ldp igp sync delay
R1(config-if) mpls ldp igp sync delay 60
R1(config-if) no mpls ldp igp sync
R1(config-if) mpls ldp igp sync
```

- CSCek71805

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: A PA-8B-ST port adapter may be powered down when you boot the router.

  Condition 1: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G2 and a PA-8B-ST port adapter. The symptom does not occur with an NPE-G1.

  Workaround 1: Perform a software OIR to bring up the port adapter.

  Symptom 2: The ISDN layers may not come up.

  Condition 2: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G2 and a PA-8B-ST port adapter. The symptom does not occur with an NPE-G1.

  Workaround 2: Enter the **debug bri-interface** command to bring up the ISDN layers.

- CSCek71844

  Symptoms: When the **virtual-profile** command is configured, PPP sessions do not come up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek72621

  Symptoms: IPv6 neighbor discovery may stop caching sourced outgoing packets during resolution.

  Conditions: This symptom is observed on a Cisco router after IPv6 neighbor discovery has cached 16 messages for resolution when these messages are locally generated.

  Workaround: There is no workaround.

- CSCek73386

  Symptoms: A Cisco router with an ESCORT jacket card crashes.

  Conditions: This symptom is observed with a Cisco 7200 router that is loaded with Cisco IOS Release 12.4XD if an ESCORT jacket card is present.

  Workaround: There is no workaround.

- CSCek74474

  Symptoms: When you enter the **protocol ip** *protocol-address* **broadcast** command on an ISP termination point, the command may not be applied to a connected CPE, preventing the CPE from populating its ARP cache and from properly forwarding traffic.

  Conditions: This symptom is observed on a Cisco router that functions as an ISP termination point and that is configured for point-to-point ATM connections when a connected CPE is configured for multipoint-to-point ATM connections.

  Workaround: Configure the **protocol ip** *protocol-address* **broadcast** command as part of a PVC configuration on the CPE.

  Alternate Workaround: Configure the connection between the ISP termination point and the CPE as a multipoint-to-point ATM connection.

- CSCek74740

  Symptoms: Shaping and random detect may not be enabled when you attempt to do so.

  Conditions: This symptom is observed on the fourth native Gigabit Ethernet port on a Cisco 7201 that runs Cisco IOS Release 12.2SB but may not be platform- and release-specific.

  Workaround: There is no workaround.

- CSCek74858

  Symptoms: When the **glbp** *group* **weighting track** *track_number* command is configured on the active processor of an HA capable router, the equivalent command does not get synced to the standby processor configuration. After the processor switchover, the GLBP weighting track command will have no affect on the operation of the group.

  Conditions: This symptom has been observed on HA capable routers in RPR, RPR+ or SSO mode, and supporting GLBP.

  Workaround: There is no workaround. The configuration will have to be entered into the new active processor configuration after switchover.

- CSCek75732

  Symptoms: A router may crash when you attach a service policy to range of PVCs.

  Conditions: This symptom is observed when a policy map has a bandwidth configured and when the service policy is attached in the ingress direction.

  Workaround: There is no workaround.

- CSCek76933

  Symptoms: A router may crash when you configure an ATM PVC on an ATM point-to-point subinterface.

  Conditions: This symptom is observed on a Cisco router when the ATM point-to-point subinterface is already part of a bundle.

  Workaround: Configure the ATM PVC on an ATM multipoint subinterface.

- CSCek78330

  Symptoms: A router that is configured with ATM PVCs may generate the following type of error messages:

  ```
  %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual-
  Access2.1 linked to wrong idb Virtual-Access2.1
  ```

  Conditions: This symptom is observed on a Cisco router that has virtual-template subinterfaces.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **no virtual-template subinterface** command, save the configuration to the startup configuration, and reload the router.

- CSCin92033

  Symptoms: On bootup of Serial PAs, the following messages may be seen on the console:

  ```
  "Failed to assert Physical Port Admini State Down"
  ```

  Conditions: These messages seem harmless but may cause the router cards to reload a couple of times before stabilizing.

  Workaround: There is no workaround.

- CSCin97208

  Symptoms: When more on slavenvram:startup-config is in progress and switchover is performed, the standby keeps constantly reloading and does not come up.

  Conditions: This problem is seen on Sup720 platforms.

  Workaround: There is no workaround.

- CSCin97912

  Symptoms: After LC reset, Intf comes as up-up even if peer is down

  Conditions: This symptom occurs when two FE SPAs are connected back-to-back. Both the ports are configured up. During reloading one of the line cards and shutdown the port on the other End. When the line card on one END will come up online. The SPA on the line card has to detect that the peer is down and the port on that SPA should go down-down. Interface comes up.

  Workaround: Shut/No Shut.

- CSCir00786

  Symptoms: When you attempt to update the startup configuration from a file but the **boot** commands are incorrect or you are unauthorized to enter the **boot** commands, a boot configuration error message should be displayed, but this does not occur.

  Conditions: This symptom is observed on a Cisco router after the startup configuration has been updated by SNMP.

  Workaround: Perform the following tasks:

  1. Copy the startup configuration to the running configuration.
  2. Copy the running configuration to the startup configuration.
  3. Verify manually that the **boot** commands are indeed correct and use the CLI to update the startup configuration.

- CSCir02274

  Symptoms: Some issues are observed during unit testing on EVC PC, which needs the hw_index determination for EVC PC. For that, add two macros

  ```
  + #define SIP10G_PC_MLINK_ON_PXF0 0
  + #define SIP10G_PC_MLINK_ON_PXF1 1
  ```

  Conditions: This symptom is seen during unit testing for EVC PC.

  Workaround: There is no workaround.

- CSCsa49566

  Symptoms: An error message similar to the following may be logged on a router:

  ```
  %FIB-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface
  ```

```
for unknown if with illegal if_number: 0
```

This message is followed by a traceback.

Conditions: This symptom is observed on a Cisco router when a virtual interface or a virtual loopback interface is created.

Workaround: There is no workaround.

- CSCsa99158

  Symptoms: Unexpected START records seen in accounting.

  Conditions: Authentication done by RADIUS server. Authorization done by IOS AAA locally.

  Workaround: There is no workaround.

- CSCsa99983

  Symptoms: New AToM or L2TPv3 sessions may not come up.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink Frame Relay (MFR) over L2TPv3/AToM when there are services with incomplete MFR over L2TPv3/AToM configurations and when the router has run for a long period of time.

  Workaround: There is no workaround.

- CSCsb12329

  Symptoms: The ifAdminStatus shows that ATM layer and ATM AAL5 Layer of ATM sub-interface are down even though there is **no shutdown** command. This situation prevents from monitoring the proper administrative status of the ATM sub-interface via SNMP.

  Conditions: This symptom is observed when ATM main interface or sub-interface is operationally down, which could be caused by circuit line problem, facing equipment's down, etc.

  Workaround: There is no workaround on SNMP. Rather, use **show interface** CLI command.

- CSCsb12969

  Symptoms: All VIPs or FlexWAN modules reload unexpectedly on a platform that is configured for Modular QoS CLI (MQC).

  Conditions: This symptom is observed on a Cisco 7500 series (with VIPs) and a Cisco 7600 series and Cisco Catalyst 6500 series (both with FlexWANs) when the following steps occur while the physical interface is in the UP state:

  1. An input policy and output policy map are already attached to an ATM or Frame Relay PVC. When you attach the same policy map to the main interface, an error message is generated and the configuration is rejected.
  2. You remove the policy map from the PVC and attach the same policy map to the main interface.
  3. You remove the policy map from the main interface.

  At this point, all VIPS or FlexWAN modules reload, even though no traffic is being processed during the above-mentioned steps.

  Workaround: There is no workaround.

- CSCsb42241

  Symptoms: A Cisco 7500 series router configured for dMLPPP may experience an unexpected reload of the VIP when the members of the bundle flap.

  Conditions: This symptom is seen on a Cisco 7500 series router that is configured for dMLPPP.

  Workaround: There is no workaround.

- CSCsb47257

  Symptoms: A Cisco router may reload due to a bus error.

  Conditions: This symptom is observed on a Cisco router that is configured for IPSec. This crash may occur when the peer sends a certificate wrapped in an PKCS7 envelope and the validation fails. When the peer tries to resend the certificate the router may crash.

  Workaround: There is no workaround.

- CSCsb48739

  Symptoms: Cisco GTP server load balancer forwards the create request to an alternate GGSN even when there exists a sticky IMSI object when the create request comes after the session object idles out.

  Conditions: This problem is seen only when the second create request comes after the session idles out.

  Workaround: There is no workaround.

- CSCsb68178

  Symptoms: Traceback %MPLS_IPRM-3-DB_PATH is seen on 6VPE.

  Conditions: This symptom is observed on 6VPE with “address-family vpnv6” configured for bgp.

  Workaround: There is no workaround.

- CSCsb76401

  Symptoms: If you load Cisco IOS Release 12.2(29.X)SX and Release 12.2(18)SXF image in active and standby, configuration mode will be locked out indefinitely.

  Workaround: Load same image on both active and standby.

- CSCsb83521

  Symptoms: The following error message may be generated after an SSO switchover:

  ```
  %SCHED-3-STUCKMTMR: Sleep with expired managed timer 55BE2914 time 0x1CD561
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that is configured for High Availability (HA).

  Workaround: There is no workaround.

- CSCsc04015

  Symptoms: When querying the cbQosCMStatsTable of the CISCO-CLASS-BASED-QOS-MIB, byte and bitrate statistics are not available for Port Adapters (PAs). The value returned for byte and bitrate statistics are always zero. This information is available on the CLI. The customer is getting zero value when polling cbQosCMPostPolicyByte64 in Cisco IOS Release12.2(18)SXE2 (7600/SUP720).

  Conditions: This problem only occurs in the Cisco 7600/6500 FlexWAN and PAs interfaces.

  Workaround: There is no workaround.

- CSCsc08602

  Symptoms: Lack of code 50 support is no stickies built when a code 50 message is processed.

  Conditions: This symptom occurs when a code 50 message is sent to an RLB server.

  Workaround: There is no workaround.

- CSCsc14208

  Symptoms: When you change the IP address of a loopback interface that functions as the ID for a TE router, TE auto-mesh tunnels do not reestablish a connection with that router. Also, static TE tunnels for which the destination is modified to match the new loopback IP address cannot reestablish their connection and the tunnels remain down.

  Conditions: This symptom is observed when all of the following conditions occur:

  – OSPF is configured to flood TE advertisements in a given area via the **mpls traffic-eng area** *area-number* command.

  – OSPF is configured to use the loopback interface for which the IP address is modified as the ID for the TE router via the **mpls traffic-eng router-id** *loopback* command.

  – TE tunnels or auto-mesh tunnels are configured with the destination set as the IP address of the loopback interface that is mentioned above.

  – You change the IP address of the loopback interface that is used as the ID for the TE router.

  Workaround: If you need to change the loopback address that is used as the ID for the TE router, follow these steps:

  1. Shut down the loopback interface.
  2. Modify the IP address of the loopback interface.
  3. Bring up the loopback interface.

  When the loopback interface address was changed and the symptom has occurred, clear the OSPF routing process in order for the tunnels to be reestablished by entering the **clear ip ospf process** command.

- CSCsc27474

  Symptoms: The output of the **show ip mcache** command does not display the MAC header on a router that is configured for multicast and Multilink Frame Relay (MLFR).

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(5) but appears to be release-independent.

  Workaround: There is no workaround.

- CSCsc30268

  Symptoms: When you reload one line card, all other line cards in the chassis may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(32)S or an earlier release and on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SX.

  Workaround: There is no workaround.

- CSCsc30451

  Symptoms: On routers with a lot of IPSec tunnel interfaces (VTI) configured, after rebooting, many tunnel interfaces remain in state “line protocol down” even though IPSec SAs are correctly establish. As a consequence no traffic can be sent through the affected tunnels from that router.

  Conditions: This was observed on a router with approximately 200 tunnel interfaces, 90 of them remain down after rebooting.

  On the VPN peer for one of those tunnels, the interface was up.

  Workaround: Do a **shutdown**, followed by a **no shutdown** on one affected tunnel interface will bring it up correctly.

- CSCsc43862

  Symptoms: Ping failure on SPA interfaces

  Conditions: This can happen with SPA inserted in a C7600-SIP-200. The problem is caused by fabric channel sync failure during bootup of a C7600-SIP-200. To verify if a ping failure is caused by this problem, check the **show logging** command under the C7600-SIP-200 console for the following error message:

  ```
  00:00:43: Serial Primary Channel SYNC FAILED!
  ```

  To get the C7600-SIP-200 console, use the **attach** *slot #* command.

  Workaround: Reloading the affected C7600-SIP-200 can correct the sync failure problem.

- CSCsc46105

  Symptoms: The type of service (ToS) value from a Cisco SSL Module (SSLM) for back-end encryption is not carried over but is stripped off.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when the **tos carryover** command is enabled on the SSLM and when the **mls qos** command is enabled in Native IOS. The symptom does not occur when the **mls qos** command is not enabled, nor does it occur for encryption in the direction of the clients.

  Workaround: Disable the **mls qos** command in Native IOS.

- CSCsc46301

  Symptoms: A Cisco 7600 series router that is running GTPSLB crashes.

  Conditions: This symptom occurs when removing real server without taking the real out of service with gtp imsi configured.

  Workaround: Clear the GTP imsi sticky entries before removing the real:

  clear ip slb sticky gtp imsi

- CSCsc61309

  Symptoms: When DHCP for IPv6 is configured on an interface, memory may not be freed when a packet is dropped, causing memory allocation failures.

  Conditions: This symptom is observed, for example, when the interface is not configured for IPv6, when the interface is not in the up state, or when encryption is configured on the interface.

  Workaround: There is no workaround.

- CSCsc61784

  Symptoms: The **show interface** *interface* **stats** command output incorrectly shows fastswitched packets as process switched packets.

  Conditions: This symptom is observed on a Cisco 7200 platform on T1/E1 interfaces only.

  Workaround: There is no workaround. Do not rely on the counters displayed by the **show interface** *interface* **stats** command output.

- CSCsc68615

  Symptoms: The router crashes with IPv6 tunnel.

  Conditions: This symptom is observed after tunnel forwarding is complete and unconfguring the applied configs is done.

  Workaround: There is no workaround.

- CSCsc77704

  Symptoms: Cisco router may experience a hang in which access is not available via console or telnet. Router must be reloaded to recover.

  Conditions: The specific conditions and/or trigger are not known. This problem is being seen in Cisco IOS Release 12.3(14)T5.

  Workaround: There is no workaround.

- CSCsc78707

  Symptoms: The **mpls l2transport route** command may be rejected as an invalid input.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCsc84768

  Symptoms: BFD configuration under Ethernet type of interfaces will be lost.

  Conditions: This symptom has been observed when the Removal / Insertion of the Ethernet type of interface is done.

  Workaround: There is no workaround.

- CSCsc95559

  Symptoms: When a policy class is configured only with the **trust** command, the output CoS may be set to zero for incoming MPLS packets, instead of to the incoming MPLS EXP bit (that is, assuming that the **no mls qos mpls trust exp** command is not configured).

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when incoming MPLS packets are layer 2-switched.

  Workaround: Add a **police** command that does not perform actual policing, for example, with an exceed-action “transmit”.

- CSCsc98850

  Symptoms: On a Catalyst 6000 series switch, the following message may be logged:

  ```
  macedon_tunnel_set_pmtu: Could not send pmtu information vlan 65535 pmtu 0
  ```

  Conditions: This symptom is seen when tunnel path-mtu-discovery is configured under a Tunnel interface.

  Workaround: This is a cosmetic issue that does not impact functionality nor performance of the switch.

- CSCsd01885

  Symptoms: In FLEXWAN module, CAM entries are not flushed when the PVC goes DOWN.

  Conditions: This symptom is observed on a Cisco Catalyst 6000.

  Workaround: There is no workaround.

  Further Problem Description: Depending on customer network design, this can lead to backholing traffic.

- CSCsd05513

  Symptoms: When using service policy on an OSM-POS port some MIB objects have wrong values:

  1. The TX cbQosCMPrePolicyByte64 counter is always 0. It is not incremented with traffic.
  2. The TX cbQosCMDropByte64 counter is always 0 even when the policer is dropping traffic.

3. The class-default counters for RX and TX (cbQosCMPostPolicyByte), (cbQosCMPrePolicyByte), (cbQosCMDropByte) are not incrementing even when traffic is sent in this class.

Conditions: This symptom occurs when using service policy on an OSM-POS port.

Workaround: There is no workaround.

- CSCsd15625

  Symptoms: CEF adjacencies are not established with subinterfaces having ISL encapsulation

  Conditions: This issue is only seen when subinterfaces with ISL encapsulation are configured. It is not seen with dot1q encapsulation.

  Workaround: There is no workaround.

- CSCsd19880

  Symptoms: The new style atm pvc command does not work properly. The command is accepted but the pvc will not come up. The ATM legacy ping fails.

  Conditions: This symptom occurs when applying the new style atm pvc command. The command will be accepted, but the PVC will not come up.

  Workaround: Use the old style atm pvc command. It works fine.

- CSCsd22834

  Symptoms: The following errors may be seen while using a 7600-SIP-200 card:

```
SLOT 1: *Dec 13 06:46:12.642 CST: %SIP200_MP-4-PAUSE: Non-master CPU is
suspended for too long, from 0x4060E438(2) to 0x4060E764 for 369087 CPU cycles.
-Traceback= 4060EA2C 40615DE8 405B7A48 405B7CF8 405B8160 405B8628 40646F8C
40663798 4069FB9C 406AC76C 406A50F4 406A58AC
SLOT 2: *Dec 13 06:46:12.642 CST: %SIP200_MP-4-PAUSE: Non-master CPU is
suspended for too long, from 0x4060E438(2) to 0x4060E764 for 368286 CPU cycles.
-Traceback= 4060EA2C 40615DE8 405B7A48 405B7CF8 405B8160 405B8628 40646F8C
40663798 4069FB9C 406AC76C 406A50F4 406A58AC
```

  Conditions: This symptom can be seen on any system using SIP-200 cards.

  Workaround: There is no workaround.

- CSCsd27088

  Symptoms: ARP/CDP Packet loss is seen on a SIP400 interface on a system that is running Cisco IOS Release 12.2(18)SXF4.

  Conditions: This symptom is seen with input QoS service policy with the "set-mpls-exp-imposition-transmit" defined in the policy. Example:

```
policy-map QOS_POLICY_IN
   class class-default
   police cir 3072000 bc 576000 be 1152000 conform-action
set-mpls-exp-imposition-transmit 5 exceed-action drop
```

  Workaround: Remove input service policy.

- CSCsd30533

  Symptoms: Duplicate IPsec flows may be created on the responder side during IPsec Quick Mode (QM) negotiation, leaving one flow with IPsec SAs and the other flow empty. This situation may cause multiple IPsec SAs to be created.

Conditions: This symptom is observed during the creation of IPsec SAs when the IPsec module fails to find the existing flow.

Workaround: There is no workaround.

- CSCsd30932

  Symptoms: Issuing the **trust-point storage** command sometimes causes a crash.

  Conditions: This symptom only occurs when an error occurs on a previous execution of this command. The second execution of the command results in a crash.

  Workaround: If an error occurs when issuing this command, the trustpoint must be removed and re-created to avoid a crash.

- CSCsd34114

  Symptoms: A router that has the **ip local pool** command enabled in an IPv6 configuration may reload under rare circumstances.

  Conditions: This symptom is observed when the local pool must allocate prefixes to the same user name on multiple interfaces in a specific order, then releases one of the prefixes, and then attempts to allocate a new prefix.

  The interfaces that the prefixes are allocated on, and the ordering of the events, must follow a very specific pattern in order for the symptom to occur.

  Workaround: Use per-user prefixes from a RADIUS server, or in a DHCP-PD configuration, use the prefix allocation per DUID.

  Further Information: IP local pools in an IPv6 configuration are used by DHCP-PD and by IPv6 Control Protocol (IPv6CP) for IPv6 over PPP links. However, the symptom is unlikely to occur with IPv6CP.

- CSCsd55004

  Symptoms: A FRR backup tunnel undergoes reoptimization, resulting in the teardown of the old lsp that is carrying traffic for primary lsps that have cutover to the backup tunnel.

  Conditions:

  – TE tunnel protecting interfaces/links
  – Usual triggers for re-optimization (link up, timer expiry, etc.)

  Workaround: There is no workaround.

- CSCsd56696

  Symptoms: Traffic is not shaped to the expected rate.

  Conditions: This symptom is observed when adaptive shaping is configured in egress direction and around 60kpps BECNs are received on this interface.

  Workaround: There is no workaround.

- CSCsd70673

  Symptoms: Traceback from DCEF720 @ sw_vlan_read_configuration(0x20d42764)+0xf4.

  Conditions: The problem is seen on dCEF720 line card after booting up the test image.

  Workaround: There is no workaround.

- CSCsd74729

  Symptoms: A crypto map may become “incomplete” and IPsec negotiation may fail.

Conditions: This symptom is observed on a Cisco platform when the **ip vrf forwarding** *vrf-name* interface configuration command is removed from an interface or changed.

Workaround: Remove and re-apply the crypto map configuration to the interface.

- CSCsd81275

  Symptoms: When a standby supervisor engine or standby RP comes up, the following error message may be generated:

  ```
  %PFINIT-SP-1-CONFIG_SYNC_FAIL: Sync'ing the private configuration to the
  standby Router FAILED, the file may be already locked by a command like: show
  config.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for ISSU.

  Workaround: There is no workaround.

- CSCsd87915

  Symptoms: The bug happens when RSVP Graceful Restart is configured on a router, and a neighbor router is performing an SSO switchover.

  When the RSVP refresh interval is modified to 5000mSec, a TE LSP will not be recovered followed a switchover.

  Conditions: This symptom occurs on Cisco IOS 12.2S and 12.0S releases that are supporting RSVP Graceful Restart help-neighbor mode.

  Workaround: Configure the RSVP refresh interval to 30 seconds (default value) or longer.

- CSCse01124

  Symptoms: The Hot Standby Router Protocol (HSRP) may not come up and may remain in the “Init” state, which can be verified in the output of the **show standby brief** command.

  Conditions: This symptom is observed when dampening is configured on a native Gigabit Ethernet interface of a Cisco 7200 series or on a Fast Ethernet interface of a PA-FE-TX port adapter. Other types of interfaces are not affected.

  Workaround: When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the Gigabit Ethernet and Fast Ethernet interfaces of all routers of the standby group.

  To prevent the symptom from occurring, remove dampening from the Gigabit Ethernet and Fast Ethernet interfaces.

- CSCse09460

  Symptoms: Aggregate RAM is not programmed after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for QoS when the SSO switchover is initiated by a script.

  Workaround: There is no workaround.

- CSCse11678

  Symptoms: Removing a member link when there are 3 member links in the bundle causes ping failures.

  Conditions: This symptom is seen when the bundle must exists on a SIP1. The problem does not happen with a bundle on a FlexWan or Enhanced Flexwan.

  Workaround: Shut/No shut on the bundle.

- CSCse15728

  Symptoms: On a Cisco 7600 series router with a VPNSM (VPN Services Module), upon receiving IPSec packets with invalid SPI (Security Parameter Index), the router fails to send the peer device IKE DELETE NOTIFY messages, thus causing the encrypted traffic to be blackholed.

  Conditions: This symptom occurs on a Cisco 7600 series router with a VPN Services Module (VPNSM).

  Workaround: There is no workaround.

- CSCse21536

  Symptoms: It is possible for the tunnel path mtu discovery information to get out of sync between the route processor and VPN-SPA. This causes tunnel path-mtu discovery to stop working

  Conditions: This problem happens when tunnel path-mtu-discovery command is removed form the tunnel configuration when the tunnel interface is shut down. Once the tunnel is unshut, the GRE tunnel will not have the path mtu configuration, but VPN-SPA will have it and remember the last path mtu found. Path mtu discovery will not work after getting into this state, even if it is reenabled in the tunnel interface.

  Workaround: To get out of this state, the tunnel needs to be completely removed. It can later be added, and path mtu discovery will behave correctly.

- CSCse43316

  Symptoms: One cannot configure a Virtual Private Network Routing Forwarding Table with the Command Line Interface configuration command **ip vrf** *VPN_VRF_Instance_Name*. The error message

  ```
  %IP_VRF-3-VRF_CREATE_FAIL: VRF id alloc failure
  ```

  is returned in repsonse to the configuration command.

  Conditions: This symptom occurs whenever one attempts to define a Virtual Private Network Routing Forwarding Table instance in the configuration context.

  Workaround: There is no workaround.

- CSCse49846

  Symptoms: System takes more time to resume complete traffic flow after events like RPF change occurs. It looks to be a case of performance degradation in ION images.

  Conditions: The problem appears to be happening with 6708-10GE card in the path, but it is not exactly determined if 6708-10GE is the cause of this issue. Installation of entries in hardware appears to be taking more time than expected on RPF change events which causes more time for traffic to resume at expected rates.

  Workaround: There is no workaround.

- CSCse52755

  Symptoms: An ELMI link between a PE router and CE router may remain down.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions as a PE router when the following conditions are present:

  – The PE router is configured with a SIP-400 that has a SPA with a Gigabit Ethernet interface that connects to the CE router.

  – The Gigabit Ethernet interface has an Xconnect-based Ethernet Virtual Circuit (EVC) configuration.

  Workaround: On the PE router, enter the **ethernet cfm enable** global configuration command.

Further Problem Description: The symptom occurs because the ELMI packets that are sent by the CE router and are destined for the PE router are tunneled to a remote side instead of being punted to the RP of the CE router.

- CSCse53002

  Symptoms: A memory leak occurs in the IPSec key engine process, and the output of the **show memory summary** command shows that the memory block that is used as "KMI num ipsec" is leaking.

  Conditions: This symptom is observed on a Cisco router when traffic is being processed.

  Workaround: There is no workaround.

- CSCse55425

  Symptoms: When configuring a serial interface or issuing **show** commands related to that serial interface, a router may incorrectly configure a different serial interface or may show output from a different serial interface in the router.

  Conditions: The conditions under which the problem manifest itself are unknown, and appear to be random. The symptom exists only when using a channelized T3 card and configuring one of the T1s.

  Workaround: A router reload clears the issue.

- CSCse89861

  Symptoms: L2TP cannot be established via an authorization of the domain.

  Conditions: This symptom is observed when a domain is not authorized and when only the username@domain is sent, regardless of the configuration of the **vpdn authen-before-forward** router configuration command.

  Workaround: There is no workaround.

- CSCse95800

  Symptoms: WRED counters are not being updated.

  Conditions: This symptom is observed on a Cisco router when WRED is attached to the parent class and when the child class has a police statement.

  Workaround: There is no workaround.

- CSCsf24836

  Symptoms: A line card may crash, and the following error messages may be generated:

  ```
  %INTR_MGR-DFC4-3-INTR: Queueing Engine (Blackwater) [0]: IPM Invalid packet
  ID
  %ESM20-DFC4-3-UNEXPECTED_GLOBAL_INT: Unexpected Global Interrupt:
  Blackwater_0/Icewater_0 Error
  %DFCWLC-DFC4-2-UNRECOVERABLE_FAILURE: DFC WAN Line Card Unrecoverable Failure
  for Device: Queueing Engine (Blackwater)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions in a SPAN in configuration.

  Workaround: Remove the SPAN configuration.

- CSCsf28509

  Symptoms: When you enter the **clear ip dhcp binding** command to clear DHCP bindings, the corresponding DHCP-initiated subscriber sessions are not cleared.

Conditions: This symptoms is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

Workaround: Enter the **clear ip subscriber** command to clear the subscriber sessions.

- CSCsf96592

  This caveat consists of two symptoms, two conditions, and two workarounds.

  Symptoms 1: The input interface when switching the tunnel encapsulated packet remains set to the original input interface. When the encapsulated packet leaves the box through the same interface as the payload was originally received, ICMP Redirect messages might be generated in error.

  Conditions 1: This symptom exists when tunneled packets leave out of the interface the original payload was received on.

  Workaround 1: There is no workaround.

  Symptoms 2: TE tunnel adjacencies might miss the L2 encapsulation size in the byte counts.

  Conditions: This symptom applies to all MPLS/TE tunnels.

  Workaround 2: There is no workaround.

- CSCsg00673

  Symptoms: When you enter the **show memory statistics** command and query the same data via SNMP, the values do not match for transient memory.

  Conditions: This symptom is observed on a Cisco router that is queried via SNMP.

  Workaround: There is no workaround.

- CSCsg07870

  Symptoms: The new active supervisor engine may crash after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsg12385

  Symptoms: When the **ipv6 verify unicast reverse-path** command is enabled on an interface, the following error message may be generated:

  ```
  %COMMON_FIB-3-NOSWSBDECODE: No IPv6 uRPF subblock control decode function for
  GigabitEthernet2/0/10 (Pixar-2)
  ```

  Conditions: This symptom is observed in a configuration with a stack of two or more Cisco Catalyst switches or routers.

  Workaround: There is no workaround.

- CSCsg22981

  Symptoms: A router may crash because of a bus error when sending L2X data packets.

  Conditions: This symptom is observed on a Cisco 7301 that runs Cisco IOS Release 12.2(28)SB and that is configured for QoS. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg26096

  Symptoms: When you enter the **hw-module reset** command on a 1-port CHOC-3/CHSTM-1 SPA that is installed in a Cisco 7600 series at the local end, the network clock at the remote end may become out-of-range (OOR), that is, the network clock goes beyond the acceptable limits of pps, without an error message being generated.

Conditions: This symptom is observed when the Network Clocking feature is configured on the 1-port CHOC-3/CHSTM-1 SPA.

Workaround: There is no workaround.

- CSCsg36725

  Symptoms: A memory leak and memory exhaustion may occur when QoS policies are updated on 40,000 sessions.

  Conditions: This symptom is observed on a Cisco 10000 series but may also affect other platforms.

  Workaround: There is no workaround.

- CSCsg44331

  Symptoms: A router may crash when a policy map that is in use by sessions is modified while the sessions are disconnected.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may not be limited to this platform.

  Workaround: Clear all sessions before you modify the policy map.

- CSCsg44431

  Symptoms: A DHCP-initiated IP subscriber session may not respond to DHCP control packets.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the subscriber session has features enabled that affect the handling of the DHCP control packets.

  Workaround: Apply access control lists (ACLs) to the subscriber session to permit bidirectional DHCP control traffic between the ISG and the DHCP client. To do so, enter the **access-list** *access-list-number* **permit udp any any eq bootps** command.

- CSCsg44555

  Symptoms: An MPLS TE tunnel with a third-party vendor headend, a Cisco midpoint, and a Cisco tailend may occasionally transition to the up/down state on the midpoint while still appearing in the up/up state on the headend and tailend. When this situation occurs, traffic may continue to flow on the tunnel even though the tunnel is in the up/down state at the midpoint or it may come to a halt.

  Conditions: This symptom is observed when the Cisco router that is the tailend for the MPLS TE tunnel uses a bandwidth or burst size that is not a multiple of 1 Kbps or 1 Kbyte and that rounds up the Resv burst size to the next higher multiple of 1 Kbps or 1 Kbyte.

  Workaround: Specify a tunnel bandwidth that is a multiple of 8 Kbps.

- CSCsg53728

  Symptoms: A router may crash when an input service policy is attached to an interface.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for Control Plane Policing (CoPP) while traffic is flowing.

  Workaround: There is no workaround.

- CSCsg61922

  Symptoms: The **show l2tp session all vcid** command generates incorrect output.

  Conditions: This symptom is observed on a Cisco router that has an L2TPv3 tunnel.

  Workaround: There is no workaround.

- CSCsg70932

  Symptoms: A Cisco 7200 series that is configured for QoS may crash when traffic is sent.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 or NPE-G2 and that has a Port Adapter Jacket Card in which a 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) in installed that has an interface with a service policy.

  Workaround: There is no workaround.

- CSCsg76546

  Symptoms: An attempt to attach a policy map to an ATM PVC or ATM interface may fail and a "policy-map not configured" error messages may be generated even though the output of the **show policy-map** command shows that the policy map is configured.

  Conditions: This symptom is observed on a Cisco 7600 series and occurs only for an ATM PVC or ATM interface on a SPA.

  Workaround: There is no workaround.

- CSCsg78729

  Symptoms: PE routers may not report an alarm indication signal (AIS) after the interface on a connected CE router is shut down. Instead of reporting an AIS, the PE routers report a loopback timeout.

  Conditions: This symptom is observed on routers when the following conditions are present:

  – The PE routers are connected through an L2TPv3 tunnel.

  – The CE router that is connected to one of the PE routers is connected to another CE router through a PVC.

  – OAM is enabled on all the routers.

  Workaround: There is no workaround.

- CSCsg83772

  Symptoms: When a prepaid service is automatically applied on account logon to a PPPoE session via RADIUS, the service may remain in a locked state even after the session has been cleared.

  Conditions: This symptom is observed when many PPPoE sessions are set up and brought down. To verify that the symptom has occurred, look at the output of the **show subscriber session** and **show sss server output** commands. If the output of the latter command shows a number greater than 1 for "SVM-Feature-Info", the symptom has occurred:

```
Service "biznes_xxx":
    Version 1:
      SVM ID               : 6C0001E7
      Child ID             : B40001EA
      Locked by            : SVM-Feature-Info       [15]
      Locked by            : SVM-Printer            [1]
      Locked by            : TC-Child               [1]
```

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the router.

- CSCsg85441

  Conditions: When you configure a large number of individual PVCs (about 52,000) and enter the **show running-config** command, it may take about 50 seconds before the command output is displayed.

Symptoms: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may also affect other platforms.

Workaround: There is no workaround.

- CSCsg89189

  Symptoms: A router may reload when you enter the **show subscriber session detailed** command while sessions are being modified.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

  Workaround: Do not enter the **show subscriber session detailed** command while sessions are being modified.

- CSCsg90929

  Symptoms: When you configure MR-APS between a Cisco 7304 and another router such as a Cisco 7500 series or Cisco 7600 series with PA-MC-STM-1 port adapters, the following tracebacks are logged on the Cisco 7304:

  ```
  -Process= "APS process", ipl= 0, pid= 191
  -Traceback= 406DC2E0 40741174 400C24BC 400C2BF0 400C6D9C 400C79EC 400C8814
  400C8894 400C90B8
  ```

  Conditions: This symptom is observed on a Cisco 7304 when the working or protect PA-MC-STM-1 port adapter in the active state.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs with the following Cisco IOS software images:

  On the Cisco 7304:

  – Release 12.2(27)SBC5 (PGP ver.4)

  – Release 12.2(28)SB5 (PGP ver.4)

  Note that Release 12.2S could also be affected.

  On the Cisco 7600 series:

  – Release 12.2(18)SXD5 (PGP ver.3)

  – Release 12.2(33)SRA1 (PGP ver.4)

- CSCsg91545

  Symptoms: A warning message is seen on SP:

  ```
  %MLS_ACL_COMMON-SP-4-MLS_ACL_CONSIST: ACL TCAM inconsistency seen at index XXX
  ```

  Conditions: This symptom occurs with certain configurations after a switchover. Also when IPv6 ACLs are applied and removed from the interface.

  Workaround: This is a warning message and no workaround is required.

  Further Problem Description: This message indicates that the ACL TCAM consistency checker has detected and fixed a discrepancy between the software shadow copy of the TCAM and the hardware. This occurs because some fields in the TCAM entry may not be cleared in the hardware. (This will not cause any issue as entries will be corrected by consistency checker.)

- CSCsg95072

  Symptoms: The **show atm vc** command may be missing VCs.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB or a rebuild of Release 12.2(31)SB when at least one ATM line card is installed and VCs are configured.

Workaround: You can display the ATM VC information by using a more specific command: enter the **show atm vc interface atm** *card/subcard/port* command.

Further Problem Description: The missing VCs tend to be from select ATM subinterfaces.

- CSCsg96495

  Symptoms: An error message of type is seen: IDBINDEX_SYNC-3-IDBINDEX_ENTRY_SET for an interface. And the **show idb** command shows an if- index value of -1 for one or more IDBs on either the Standby or Active RP.

  If this happens on a Standby RP, there is no effect on traffic. However if the RP switches over to become Active, it will prevent traffic from flowing on the affected interfaces.

  Conditions: This symptom is most likely to happen if a platform has a bug such that OIR insertion notifications are synced to the Standby RP before the corresponding interface index values have been synced. The normal order is to always guarantee the index values arrive first.

  Workaround: If this happens on an HA protected Active RP (which affects traffic), check whether the Standby RP has good if-index values for all interfaces by running the **show idb** EXEC command on the Standby RP. If so, then do an RP switchover, so the RP with good interface indexes becomes the Active RP.

  If the Standby RP shows this symptom, reload the Standby RP and check that after it comes up, it has good interface index values, which should happen in most cases.

  Further Problem Description: This DDTS is to provide a platform-independent code workaround that allows the interface index values to self-recover after the correct if-index values are synced to the Standby RP.

  If the condition is seen on an Active RP, this DDTS fix will allow it to recover following an OIR deletion/insertion rather than remaining in the error condition.

  The root-cause of the incorrect syncing order will still need to be fixed by the platform that has this symptom. But this DDTS will lower the severity by allowing it to self-recover in most cases on its own without user intervention.

- CSCsg97717

  Symptoms: The PXF engine of an NSE-150 crashes when you enter the **ip pim bidir-enable** command.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for MVPN with a single VRF when multicast traffic is flowing through this VRF.

  Workaround: There is no workaround.

- CSCsg99331

  Symptoms: The **show host** command will not show full host name.

  Conditions: In case of hostname is used, only the first character on the host name is displayed or used in the query.

  Workaround: There is no workaround.

- CSCsh01626

  Symptoms: A “%SYS-2-MALLOCFAIL” error message may be generated, indicating that there is no free memory available in the router.

Conditions: This symptom is observed only on a Cisco 7200 series that is configured with an NPE-G2 and that runs a Cisco IOS software image that is based on Release 12.2S.

Workaround: There is no workaround. To clear the symptom, reboot the router.

- CSCsh04911

  Symptoms: On a Cisco 7304 that is configured for AToM, a software-forced reload may occur on an NSE-100.

  Conditions: This symptom is observed when egress NetFlow is configured on an AToM attachment circuit.

  Workaround: There is no workaround.

  Further Problem Description: The configuration that is stated in the Conditions is essentially a misconfiguration. NetFlow can collect information only about Layer 3 IP packets. However, the AToM attachment circuit is transmitting Layer 2 frames, so the egress NetFlow is not valid.

- CSCsh05677

  Symptoms: A Cisco device that is running Cisco IOS configured with MPLS and Netflow may show all traffic out an interface being process switched. This will cause high CPU under the IP Input process.

  Conditions: This issue is seen when **ip flow ingress** is configured on any interface on the device, and MPLS is also enabled. All traffic out of the MPLS enabled interface will be process switched as evident in the **show interface statistic** command.

  Workaround: Enable MPLS aware netflow via the **ip flow-cache mpls label-positions 1** command. This will prevent the process switching of traffic. However additional MPLS fields will be added to the netflow export records.

- CSCsh07031

  Symptoms: L2TP connectivity may not function across the native Gigabit Ethernet interface of an NPE-G2.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB2 when EIGRP is configured as the routing protocol.

  Workaround: There is no workaround.

- CSCsh12653

  Symptoms: When an ISG receives VSAs that cannot be parsed by the SIP parser, the ISG disconnects the established session and does not respond with a CoA Nak message.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG when an incorrect VSA is sent via a CoA message and when the SIP parser returns a DENY message to the ISG.

  Following are examples of incorrect VSAs:

  – a vc-weight that is larger than the maximum that is allowed: cisco-avpair = “atm:vc-weight=3000”

  – a non-existent service-policy name: cisco-avpair = “atm:vc-qos-policy-out=non_exist_policy” cisco-avpair = “atm:vc-watermark-max=1”

  Workaround: There is no workaround.

- CSCsh13739

  Symptoms: The usage of the PXF engine increases to 100 percent. This situation may cause interface flapping, error messages that state that OSPF neighbors are unreachable, and a failure of the standby processor.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with either an NSE-100 or an NSE-150, that has a POS interface that is configured for Frame Relay and that has an output shaping service policy, and that receives traffic that matches the output shaping service policy. In addition, the router is configured with a cross-connect, more specifically, an interface that is configured for Xconnect service and that is connected to a remote peer.

  Workaround: There is no workaround.

- CSCsh15456

  Symptoms: A router may crash when you remove a QoS policy from an interface or modify the policy map.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when you configure a QoS policy, attach it to the interface, run traffic, and then, after a long time, remove the QoS policy or modify the policy map.

  Workaround: There is no workaround.

- CSCsh15817

  Symptoms: IP SLA operations on a router that has a response time reporter (RTR) enabled may fail at the source. The UDP socket events are not received by the RTR responder process, and the UDP socket events are missing when a UDP packet is routed through a VRF.

  Conditions: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.2SB. You can verify that the symptoms are occurring through any of the following commands:

  – debug rtr trace
  – debug ip udp
  – debug socket

  Workaround: Use IP SLA operations without VRFs.

- CSCsh27931

  Symptoms: A platform may crash when an arithmetic exception crash occurs. Before this situation occurs, the following error message is generated:

  ```
  %COMMON_FIB-SP-4-UNEQUAL: Ratio of unequal path weightings (1 1 40 ) prevents
  oce IP adj out of GigabitEthernet3/2, <ip addr> from being used.
  ```

  Conditions: This symptom is observed on a Cisco platform that functions in an IS-IS configuration when TE tunnels are shut down.

  Workaround: There is no workaround.

- CSCsh28556

  Symptoms: When configuring frame relay queueing, bandwidth is taking 28kbps, and more than 28 kbps cannot be configured.

  Conditions: This symptom happens only when service policy is applied under map- class frame-relay and then binding it under the DLCI with frame-relay traffic shaping enabled under the interface.

  Workaround: There is no workaround.

- CSCsh28899

  Symptoms: IS-IS routes are not learned at remote sides.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G2 when the router connects to the remote sides through a native Gigabit Ethernet (GE) interface.

  Workaround: Do not use a native GE interface. Rather, use a GE port adapter such as the PA-GE.

- CSCsh34529

  Symptoms: An ATM interface configuration may become lost on the standby RP.

  Conditions: This symptom is observed on a Cisco 7600 series when you perform the following steps:

  1. You configure an ATM main interface on a SPA.
  2. You configure PVCs on the ATM main interface.
  3. You shut down the SPA.
  4. You reload the standby supervisor engine and wait until it comes up.
  5. You bring up the SPA from the active RP.

  At this point, the ATM interface configuration is lost on the standby RP.

  This symptom is observed with both 8-port OC-3c/STM-1 ATM SPAs and Circuit Emulation over Packet (CEoP) SPAs.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the standby supervisor engine once more.

- CSCsh37008

  Symptoms: If the chassis is WS-C6509-NEB-A or CISCO7609 with one fan, the system cooling capacity is 76cfm. WS-X6708-10GE module requires 84cfm cooling capacity. It would be powered down by default.

  Conditions: This symptom is observed on WS-C6509-NEB-A or CISCO7609 chassis with one fan, and system has WS-X6708-10GE inserted.

  Workaround: User can add the following configuration if running image without this fix:

  Router(config)#environment temperature-controlled

- CSCsh45466

  Symptoms: A memory leak may occur on a router that is configured with IP ACLs.

  Conditions: This symptom is observed when you enter the **show access-list** command to see a list of ACLs that contains dynamic elements.

  Workaround: There is no workaround.

- CSCsh51778

  Symptoms: An ISG that receives incorrect VSAs for a policy map may no longer accept any VSAs even if the VSAs are correct.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and that runs Cisco IOS Release 12.2(28)SB, Release 12.2(31)SB, or Release 12.2(31)SB1.

  Workaround: There is no workaround.

- CSCsh54999

  Symptoms: A router may crash when the dynamic ACL timer expires.

Conditions: This symptom is observed on a Cisco router only when the **show access-list** command is entered before the timer expires.

Workaround: There is no workaround.

- CSCsh55768

  Symptoms: All packets received by a Cisco Catalyst 3550 Switched Virtual Interface (SVI) are dropped. In the output of the **show interfaces** command for the SVI, the number of packets in the SVI input queue reaches the maximum number and the input queue drop counter increments.

  Conditions: All of the following conditions must be true for the problem to occur:

  – The switch is a Cisco Catalyst 3550 switch.

  – The Cisco IOS software feature set is IP Base or IP Base Crypto.

  – The Cisco IOS software version is Release 12.2(35)SE, Release 12.2(35)SE3, or Release 12.2(35)SE5.

  – IP routing is enabled.

  – The switch SVI interface receives certain IP multicast packets. Examples of applicable packets are EIGRP or RIPv2 packets.

  Workaround: Any of the following items are a workaround:

  – Upgrade the switch software to Cisco IOS Release 12.2(37)SE.

  – With affected Cisco IOS versions, do not use the IP Base or IP Base Crypto feature set. The IP Services and IP Services Crypto feature sets are not affected.

  – Downgrade the switch software to a Cisco IOS release prior to Release 12.2(35)SE.

  – Configure an access list to block the offending IP multicast packets.

  – Configure a passive interface on the router adjacent to the switch to prevent the receipt of EIGRP or RIPv2 packets by the switch SVI.

- CSCsh57509

  Symptoms: A Cisco router that is configured for RIPv2 may not delete a path from the routing table when it should do so.

  Conditions: This symptom is observed after the router has learned multiple paths for a prefix with different next hops from one neighboring router and after the neighboring router stops advertising one of the paths.

  Workaround: Enter the **clear ip route *** command.

- CSCsh57611

  Symptoms: Frame Relay end-to-end keepalives may unexpectedly time out.

  Conditions: This symptom is observed on a Cisco 7206VXR that has an NPE-G1 and that runs Cisco IOS Release 12.2(31)SB2.

  Workaround: There is no workaround.

- CSCsh59375

  Symptoms: A DHCP interface may not be switched when you enter the **ip dhcp smart-relay** command.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(12.15a) and that is configured for MPLS VPN.

  Workaround: There is no workaround.

- CSCsh66935

  Symptoms: A router crashes in avl_get_next_threaded.

  Conditions: This symptom happens in extremely rare cases when deleting many tunnels with tunnel protection enabled.

  Workaround: There is no workaround.

- CSCsh68976

  Symptoms: A small memory leak is observed when any of the following commands is issued:

  – **show hw-module** *slot* **transceiver 0 idprom brief**
  – **show hw-module** *slot* **transceiver 0 idprom detail**
  – **show hw-module** *slot* **transceiver 0 idprom dump**

  Conditions: This symptom occurs when the above commands are issued.

  Workaround: Do not issue these commands:

  – **show hw-module** *slot* **transceiver 0 idprom brief**
  – **show hw-module** *slot* **transceiver 0 idprom detail**
  – **show hw-module** *slot* **transceiver 0 idprom dump**

- CSCsh69341

  Symptoms: In a Server Load Balancing (SLB) configuration, input features (except for Policy Based Routing [PBR]) that should not be processed are unexpectedly executed in a special switching path.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch that runs Cisco IOS Release 12.2SXH and on a Cisco 7600 series that runs Release 12.2SXH or Release 12.2(33)SRB and that are configured with a Supervisor Engine 720.

  Workaround: There is no workaround.

  Further Problem Description: The symptom may cause SLB to behave in an unexpected way. For example, when an input access control list (ACL) is applied on an interface, SLB is supposed to bypass the ACL, which is considered an input feature, so SLB packets can reach their destination without a problem. However, because of the symptom, the ACL is active and may stop SLB packets from reaching their destination.

- CSCsh74270

  Symptoms: A router may crash when you attach a map class to a Frame Relay data-link connection identifier (DLCI) interface.

  Conditions: This symptom is observed on a Cisco router that is configured with an output service policy with a priority kbps/percentage value.

  Workaround: There is no workaround.

- CSCsh76558

  Symptoms: The **show stacks** command on any router platform that uses IPC may show a process whose name appears to be corrupted, including a very large number of blank lines before the next line of the **show stacks** output is printed.

  Conditions: The problem is seen when a **show stacks** command is issued or when any other command that causes this command to be executed (for example, **show tech-support**) is issued. This is seen in router platforms that have IPC processes.

  Workaround: There is no workaround.

- CSCsh85531

  Symptoms: Some E1 channels may remain down after you have reloaded a router.

  Conditions: This symptom is observed on a Cisco 7200 series that function as a PE router and that connects to a CE router. Both routers are connected through 1-port multichannel STM-1 (PA-MC-STM-1) port adapters, and the **framing no-crc4** command is enabled on all interfaces of both routers.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the SONET controller of the PA-MC-STM-1 at the PE side to enable all interfaces to come up.

- CSCsh92854

  Symptoms: When the **ip cef** command is enabled, output bytes of a virtual-access interface do not increment correctly.

  Conditions: This symptom is observed on a Cisco router that has a PPPoVPDN virtual-access interface when the VPDN traffic is sent over an ATM interface. The symptom does not occur when the VPDN traffic is sent over a Gigabit Ethernet interface.

  Workaround: If this is an option, disable CEF on the interface from which the VPDN traffic is switched. However, doing so may affect the performance of the platform. If this is not an option, there is no workaround.

- CSCsh93436

  Symptoms: Layer 2 Tunnel Protocol version 3 (L2TPv3) will have transport problems, which may include an inability to receive packets from the transport layer.

  Conditions: When this symptom is present, L2TPv3 tunnels will not come up.

  Workaround: There is no workaround.

- CSCsh93517

  Symptoms: SCTP may have transport problems, which may include an inability to receive packets from the transport layer.

  Conditions: This symptom occurs when SCTP has transport problems.

  Workaround: There is no workaround.

- CSCsh93653

  Symptoms: A router crashes when you configure a local ISG service policy with any routing protocol such as BGP or ISS.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB3 when you enter the following commands:

  ```
  Router(config)# router bgp 1
  Router(config-router)# service
  Router(config-router)# policy-map type service <policy-map-name>
  Router(config-service-policymap)# service local
  ```

  Workaround: Configure and download service profiles via a RADIUS server.

- CSCsh94637

  Symptoms: An NPE-G1 may crash because of a bus error and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address TLB (store) exception, CPU signal 10,
  PC = 0x61F1D0D0
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB2 and that is configured for L2TP. The symptom may not be platform specific.

Workaround: There is no workaround.

- CSCsh95788

  Symptoms: A router that is running Cisco IOS software may unexpectedly restart.

  Conditions: This symptom can occur when the following interface mode command is removed:

  ipv6 nd prefix framed-ipv6-prefix

  Workaround: There is no workaround.

- CSCsh96662

  Symptoms: There are no label forwarding entries for VPNv6 prefix on Inter-AS option B boundary.

  Conditions: This symptom occurs when the VPNv6 prefix is learned from an IPv4 neighbor (not IPv6 enabled).

  Workaround: Switch the neighbor to peer through IPv6.

- CSCsh98088

  Symptoms: PDSN is reloaded when the **no vpdn-group CDMA** command is configured.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(15)T PDSN software when **source-ip** is configured in the **vpdn-group** subcommand.

  Workaround: Use the global **vpdn source-ip** command instead of the **source-ip** command that is configured within the individual VPDN groups.

- CSCsi00136

  Symptoms: Cisco IOS software fails to properly detect the presence of NAT with some implementation, leading to unsuccessful phase 1 or phase 2 establishment.

  Conditions: This symptom occurs when the remote peer sends more than 2 NAT-D (NAT DISCOVERY) payload in the phase 1 establishment.

  Workaround: There is no workaround.

- CSCsi03714

  Symptoms: A router may crash when a DLCI configuration is removed from an MFR subinterface.

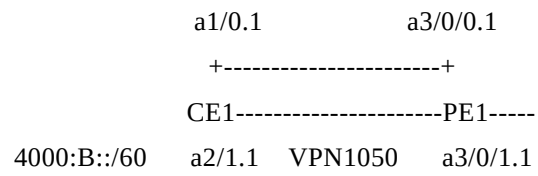
  Conditions: This symptom is observed on a Cisco 7200 series when the MFR interface has a map class with a service policy attached.

  Workaround: There is no workaround.

- CSCsi07822

  Symptoms: When using the IPv6 VPN over MPLS (6VPE) capability and EBGP multihop where loadsharing is being done on the VRF. If one of the loadsharing paths on the PE is flapped, loadsharing across the appropriate paths may no longer occur. This is because the RIB is unable to resolve the route to the next hop via the flapped interface.

  Conditions: Assuming we have the topology below and eBGP multihop loadsharing is being done by PE1:



332:332:332::332/128 444:444:444::444/128

EBGP multihop session between PE1 and CE1 via loopback addresses 444:444:444::444/128 and 332:332:332.332/128 respectively.

################################
Loadsharing before the interface flap
################################

```
PE1# show bgp vpnv6 unicast vrf VPN1050 4000:B:0:270::/60

BGP routing table entry for [1050:1]4000:B:0:270::/60, version 3760 Paths: (1
available, best #1, table VPN1050) Advertised to update-groups: 1 3510 102
332:332:332::332 (FE80::217:95FF:FEE4:1A90) from 332:332:332::332 (10.1.1.32) Origin
IGP, localpref 100, valid, external, best Extended Community: RT:1050:1 mpls labels
in/out 13509/nolabel

PE1#
PE1# show ipv6 route vrf VPN1050 4000:B:0:270::/60

Routing entry for 4000:B:0:270::/60 Known via "bgp 6777", distance 20, metric 0, type
external Route count is 1/1, share count 0 Routing paths: 332:332:332::332 Last
updated 02:17:03 ago
PE1#
```

###
Let's look at the RIB for the next hop; we should see both paths.
###

```
PE1# show ipv6 route vrf VPN1050 332:332:332::332

Routing entry for 332:332:332::332/128 Known via "static", distance 1, metric 0
Redistributing via bgp 6777 Route count is 2/2, share count 0 Routing paths:
2004:1000:9250:A910::2 Last updated 00:48:21 ago 2006:106:106:2006::2 Last updated
00:00:20 ago
```

################################
CEF looks good as shown below
################################

```
PE1# show ipv6 cef vrf VPN1050 4000:B:0:270::/60 detail

4000:B:0:270::/60, epoch 24 local label info: other/13509 recursive via
332:332:332::332 recursive via 2004:1000:9250:A910::2 recursive via
2004:1000:9250:A910::/64 attached to ATM3/0/0.1 recursive via 2006:106:106:2006::2
recursive via 2006:106:106:2006::/64 attached to ATM3/0/1.1
PE1#
```

Now shut down one of the interfaces on PE1

```
PE1(config)# int a3/0/1
PE1(config-if)# sh
PE1(config-if)# end
PE1#
```

###
CEF now only has one recursive output chain to the destination after the interface is shut down - Good
###

```
PE1# show ipv6 cef vrf VPN1050 4000:B:0:270::/60 detail

4000:B:0:270::/60, epoch 24 local label info: other/13509 recursive via
332:332:332::332 recursive via 2004:1000:9250:A910::2 recursive via
2004:1000:9250:A910::/64 attached to ATM3/0/0.1
```

```
PE1#

##############################################
Now bring back up the a3/0/1 interface and observe CEF
##############################################

PE1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
PE2(config)# int a3/0/1
PE2(config-if)# no sh
PE2(config-if)# end
PE1#

#################################################################################
Let's see if RIB and CEF have resolved the next hop via this interface - It does not as demonstrated
below
#################################################################################

PE1# show ipv6 route vrf VPN1050 332:332:332::332

Routing entry for 332:332:332::332/128 Known via "static", distance 1, metric 0
Redistributing via bgp 6777 Route count is 1/1, share count 0 Routing paths:
2004:1000:9250:A910::2 Last updated 00:56:35 ago

PE1# show ipv6 cef vrf VPN1050 332:332:332::332/128 detail

332:332:332::332/128, epoch 24 local label info: other/3305 1 IPL source [no flags]
Dependent covered prefix type inherit cover NULL recursive via 2004:1000:9250:A910::2
recursive via 2004:1000:9250:A910::/64 attached to ATM3/0/0.1
PE1#
```

Workaround: Toggle the associated CE interface a few times.

- CSCsi12104

  Symptoms: When you repeatedly change active routers by enabling preemption and then change the priorities on the router interface, the router may crash.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.5)T after you have shut down the interface of the active router.

  Workaround: There is no workaround.

- CSCsi14211

  Symptoms: A CPUHOG condition may occur when an LDP session goes down.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS LDP, that has more than 30 LDP sessions with peers, and that exchanges more than 5000 label bindings for each LDP session. The symptom occurs when the LDP session goes down shortly after it comes up.

  Workaround: There is no workaround.

- CSCsi15221

  Symptoms: A Cisco 7200 series with an NPE-G2 may hang during the boot process.

  Conditions: This symptom is observed when several native Gigabit Ethernet ports with "MV64460" hardware come up simultaneously, for example, while the router boots. To verify if the Gigabit Ethernet ports of your router have "MV64460" hardware, look in the output of the **show interfaces** command.

  Workaround: There is no workaround.

- CSCsi17158

  Symptoms: Catalyst Series 4xxx and 35xx switches that run Cisco IOS software may crash with the error message “System returned to ROM by abort at PC 0x0” when processing SSHv2 sessions.

  Conditions: This symptom occurs when an SSH server is enabled.

  Workaround: This vulnerability can be mitigated. For Cisco IOS software, the SSH server can be disabled by applying the **crypto key zeroize rsa** command while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

  Access to the SSH server on Cisco IOS software may also be disabled by removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with **ssh** removed from the list of permitted transports on VTY lines while in configuration mode. For example:

  line vty 0 4

  transport input telnet

  end

  If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely through the use of access control lists (ACLs) on the VTY lines as shown at the following URL:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html#xtocid14

  More information on configuring ACLs can be found on Cisco’s public website:

  http://www.cisco.com/warp/public/707/confaccesslists.html

  An example of a VTY access list can be found below:

  access-list 2 permit 10.1.1.0 0.0.0.255

  access-list 2 deny any

  line vty 0 4 access-class 2 in

  end

- CSCsi19924

  Symptoms: Ping failures with MLPPP are seen on an SPA-8XCHT1/E1.

  Conditions: This symptom occurs when MFR with xconnect/ATOM and MLPPP are configured on the same SPA on a Cisco 12000 series platform.

  Workaround: Reload the SPA.

- CSCsi21733

  Symptoms: An SPA-2XOC48POS/RPR goes to Out Of Service after encountering an SPA BUS ERROR. TRANSCEIVER-6-REMOVED messages are followed by an SCC failure, resulting in the SPA going to Out Of Service.

  Conditions: This symptom occurs when there are many L1 errors (B2-BER) found on the link and when the interfaces flap many times before the BUS ERROR.

  Workaround: Reload the LC.

- CSCsi22585

  Symptoms: DNS requests from a PC client may time out.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG, that is located between a PC and a DNS server, and that redirects DNS requests to a local DNS server.

Workaround: There is no workaround.

- CSCsi23968

  Symptoms: When IKE phase 1 is cleared and IPSec requests a rekey, IKE fails to rekey.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.5)T. IKE rekeys phase 1 after two attempts instead of five attempts. IKE does rekey successfully within the time frame of two attempts. However, when the network connection to the peer is down and not restored within the time frame of two attempts, the rekey fails. In this situation, IKE should make five attempts. Note that the symptom is not release specific.

  Workaround: There is no workaround.

- CSCsi25578

  Symptoms: When a Cisco IOS LNS router receives a L2TP Incoming Call Request (ICRQ) message with same assigned session ID as an existing session of another tunnel from the same LAC, it disconnects the session because of unknown Attribute-Value Pair (AVP).

  Conditions: This symptom occurs under the following conditions:

  – When L2TPv2 is used.

  – When the LAC is not a Cisco router that reuses the same session immediately for different tunnels. (A Cisco LAC will always advance the session even it is for a different tunnel. It is rare to run across this condition.)

  Workaround: There is no workaround.

- CSCsi28462

  Symptoms: A router may reload when using SASL.

  Conditions: This symptom occurs when SASL is being used. Some of the affected commands include:

  bingd device *port* **sasl profile** *sasl-profile*

  bingng device *host port* **sasl user** *user* **password** *password*

  netconf beep listener *port* **sasl** *sasl-profile*

  netoconf beep initiator *host port* **user** *user* **password** *password*

  Workaround: There is no workaround.

- CSCsi30780

  Symptoms: ATM Stateful Switchover (SSO) takes more than 5 seconds.

  Conditions: This symptom occurs when ATM traffic is sent and an SSO is done.

  Workaround: There is no functionality breakage.

- CSCsi30993

  Symptoms: The output of the **show vtemplate** command shows an inaccurate number of active interfaces and subinterfaces.

  Conditions: This symptom is observed on all platforms that are running Cisco IOS Release 12.2SB software and using any feature that requires the use of Virtual-Access interfaces.

  Workaround: There is no workaround.

- CSCsi31041

  Symptoms: When the **service local** command is configured under a policy map, service is denied.

Conditions: This symptom is observed on a Cisco router that functions as an ISG and that is configured for AAA.

Workaround: There is no workaround.

- CSCsi32790

  Symptoms: When both sides of a CE are configured with “pvc-oam manage” and an interface on the PE is shut down, the CE side does not detect that the interface went down.

  Conditions: This symptom occurs when both sides of a CE are configured with “pvc-oam manage” and an interface on the PE is shut down.

  Workaround: The ATM OAM TIMER process had got deleted because of a return inside the while loop. The return statement is changed to continue, and the function micro_block_get_or_alloc() is used instead of micro_block_get().

- CSCsi40658

  Symptoms: With a Cisco 7600 configured for xconnect with interface vlan, a crash may happen when the interface vlan is unconfigured, with a **no interface vlan** *num* command.

  Conditions: This symptom occurs only when there are a large number of pseudowires configured.

  Workaround: There is no workaround.

- CSCsi42061

  Symptoms: When I try to do the bundle configuration on an ATM interface, I see that the random-detect attach red-test command is not accepted.

  Conditions: Configure ATM bundle, attach PVC, and then we see that the random detect command is not recognized.

  Workaround: There is no workaround.

- CSCsi43776

  Symptoms: Some CLI commands on any router platform that supports ISSU and uses IPC may show a process whose name appears to be corrupted, including a very large number of blank lines before the next line of the place where the process name would be printed.

  Conditions: This symptom is seen in router platforms that have ISSU related IPC processes. The bug ID CSCsh76558 fixed this issue for the **show stacks** command. This bug tracks a more generic fix.

  Workaround: There is no workaround.

- CSCsi45831

  Symptoms: There may be a delay in the creation of IP sessions over an interface that is configured for QinQ support.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the **initiator dhcp class-aware** command is enabled to place the clients in a specific VRF.

  Workaround: There is no workaround.

- CSCsi46028

  Symptoms: On routers that are configured for WCCP, interfaces that are connected to the content engine can become wedged.

  Conditions: This issue was introduced by CSCuk61396; only the images that have the fix for CSCuk61396 are affected by this issue.

  Workaround: There is no workaround. If an interface gets wedged, the only way to recover the system is to do a reload.

- CSCsi46897

  Symptoms: PPP may crash when an **snmpwalk** command is executed on the cbQosSetStatsTable object.

  Conditions: This symptom is observed when a service policy with a child policy that contains marking (“set”) actions is applied to an interface before the **snmpwalk** command is executed on the cbQosSetStatsTable object of the CISCO-CLASS-BASED-QOS-MIB.

  Workaround: There is no workaround.

- CSCsi48273

  Symptoms: L2VPN Local switching configs are not synced to the standby on reload on both active and standby PRE-2.

  Conditions: This symptom occurs only on reload of both the active and the standby.

  Workaround: There is no workaround.

- CSCsi49907

  Symptoms: A memory leak may cause a slow response and timeouts during the setup of new IP sessions, and the connection speed for established sessions may be very slow. To verify that there is a memory leak, enter the **show memory debug leak summary** command, and look for “Alloc PC” in the output.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB3 and that has the following configuration commands under a BVI or on an IP interface:

  service-policy type control XXXX

  ip subscriber routed

  initiator dhcp class-aware

  Workaround: There is no workaround.

- CSCsi51014

  Symptoms: Disk access freezes a router.

  Conditions: This symptom occurs after some fsck execution.

  Workaround: Format the disk, but all the content in disk is lost.

- CSCsi52268

  Symptoms: A router may run out of memory when you scale sessions with QoS and distribute them among a large number of subinterfaces.

  Conditions: This symptom is observed on a Cisco router such as a Cisco 10000 series with a PRE3 that is configured for Hierarchal Queuing Framework (HQF). The symptom is not platform-specific. The symptom occurs when the following conditions are present:

  – Sessions are being scaled.

  – Per-session shaping and/or queuing is configured.

  – The number of sessions per subinterface is small.

  – Hierarchical queuing policy maps on sessions with aggregate shaping are configured, meaning that the subinterfaces are shaped as well. The subinterfaces are either shaped VLAN-QinQ subinterfaces or shaped ATM VC subinterfaces.

  Workaround: There is no workaround.

- CSCsi53232

  Symptoms: The active IMA link flaps when the IMA interface is down because of insufficient active links.

  Conditions: This symptom is observed on an IMA interface configured on a CEM SPA on a Cisco 7600 platform connected to a 7200 T1-IMA PA at the other end.

  Workaround: There is no workaround.

- CSCsi53353

  Symptoms: IPv6 EBGP sessions fail with the following message in “debug bgp events”:

  ```
  %BGP-4-INCORRECT_TTL: Discarded message with TTL 32 from <ip>
  ```

  Conditions: This symptom occurs when BTSH is configured between the peers.

  Workaround: Disable BTSH between the IPv6 peers.

- CSCsi53469

  Symptoms: A router may hang for approximately 7 minutes.

  Conditions: This symptom is observed when you attempt to configure the **range pvc** command in a manner that exceeds the interface limit.

  Workaround: There is no workaround.

- CSCsi57207

  Symptoms: A bus error crash is seen on a Cisco router that is running Cisco IOS Release 12.2(31)SB3.

  Conditions: This symptom is seen when PPPoE/PPPoA is configured with PPP idle timeout and PPP keepalive.

  Workaround: There is no workaround.

- CSCsi60103

  Symptoms: When you perform an online insertion and removal (OIR) to replace a port adapter, you may not be able to configure IPv6 on an interface of the newly inserted port adapter.

  Conditions: This symptom is observed when the newly inserted port adapter has an overlapping namespace with the port adapter that was replaced, for example, when a 1-port Fast Ethernet (FE) port adaptor is replaced by a 2-port FE port adaptor.

  Workaround: First unconfigure IPv6 on the interface of the port adapter that is to be replaced before you perform an OIR.

  Further Problem Description: The symptom is not observed when you perform an OIR to replace a port adapter with the exact same type of port adapter.

- CSCsi60125

  Symptoms: For TCP flows (typically short lived) being NATed at connection rates of about and over 100 connections per second, incorrect NetFlow translations are seen. One would see TCP RSTs generated by the TCP endpoints (e.g. server). We have noticed two NetFlow shortcuts pointing to the same adjacency.

  Conditions: Static NAT on PFC3A or PFC3B or PFC3BXL or PFC3C based systems (e.g. SUP32 or Sup720).

  Workaround: Keep the connection rate to below 100 connections per second, and if more performance is required, consider using Firewall Service Module (FWSM) to do NAT.

- CSCsi76569

  Symptoms: A Cisco router may crash during bootup or while writing or erasing the configuration during the “flow_def_master_list_lookup” process.

  Conditions: The symptom occurs during bootup or when a configuration is written to or erased from memory. The symptom may also occur when you enter the **show running-config** command.

  Workaround: There is no workaround.

- CSCsi76936

  Symptoms: A router may crash when the **debug glbp** command is enabled.

  Conditions: This symptom occurs only when GLBP receives a packet from a group that is not configured locally.

  Workaround: Do not enable GLBP debug.

- CSCsi78785

  Symptoms: A router may crash when a policy map is unconfigured.

  Conditions: This symptom is observed on a Cisco router that is configured with an output policy with Frame Relay Traffic Shaping.

  Workaround: There is no workaround.

- CSCsi82166

  Symptoms: A router may reload during SASL authentication.

  Conditions: This symptom is observed when SASL authentication is performed while the **sasl** command is changed. For example, the symptom may occur when a BEEP session that uses SASL is performing authentication while the **sasl** command is being unconfigured.

  Workaround: Do not configure or unconfigure SASL when SASL authentication is being performed.

- CSCsi82427

  Symptoms: A ping may fail when a native Gigabit Ethernet interface functions in “speedauto,” duplex auto,” and “no neg auto” mode and when the peer interface functions in “fixed speed” and “duplex” mode.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G2 when the interfaces are connected back-to-back via an RJ-45 cable.

  Workaround: Configure the same speed and duplex mode on both interfaces.

- CSCsi85384

  Symptoms: A flexwan may fail to boot the modules, and error messages similar to the following might be observed:

  ```
  SLOT 3/1: 00:00:19: %XDR-3-XDROOS: Received an out of sequence IPC message. Expected
  0 but got 26
  ```

  Conditions: The Cisco 7600 is running a 12.2(32)SRB2 image; this is occurring on an Enhanced flexwan with PA-MC-E3 port adapters.

  Workaround: There is no workaround.

- CSCsi85532

  Symptoms: A Cisco 851 that is running the c850-advsecurityk9-mz.124-11.T1 image is crashing with an Unexpected exception to CPU: vector 300.

  Conditions: The router crashes if not specifying pw-class in the pseudowire on interface Virtual-PPP1.

Workaround: Specify pw-class in the pseudowire.

- CSCsi90461

  Symptoms: If many L2TP sessions are brought up and down again continuously, the following error messages will be displayed on the console:

  ```
  %L2TP-3-ILLEGAL: _____:_____: ERROR: [l2tp_session_get_l2x_cfg::241], -Traceback=
  0x121FE88 0x25394E8 0x2539730 0x25558CC 0x2555FA0 0x254C0C4 0x254BB88 0x254BCD8
  0x254BDD8 0x2554040 0x2548250 0x2541E50 0x2541F6C 0x7D6510 %L2TP-3-ILLEGAL:
  _____:_____: No session config, -Traceback= 0x121FE88 0x25394E8 0x2539748 0x25558CC
  0x2555FA0 0x254C0C4 0x254BB88 0x254BCD8 0x254BDD8 0x2554040 0x2548250 0x2541E50
  0x2541F6C 0x7D6510
  ```

  Conditions: This symptom happens in both VPDN and Xconnect applications.

  Workaround: Reload the router.

- CSCsi92079

  Symptoms: If an access control list (ACL) is used for a destination-only prefix, a fatal error is declared and optimized edge routing (OER) is shut down. For destination-only traffic classes, a prefix list should be used, not an ACL or access control entry (ACE).

  Conditions: This symptom is observed in Cisco IOS Release 12.4(11)T and later releases at this time.

  Workaround: Use a prefix list instead of an ACL/ACE for destination-only traffic classes. For example:

  – Use a prefix list for traffic class 100.1.1.0/24

  – Use an ACE for traffic class 100.1.1.0/24 DSCP af11

- CSCsi93020

  Symptoms: A router may crash when it functions as a LAC with a single PPPoE session that is locally terminated and when a service policy contains CoS marking or any other non-supported configuration.

  Conditions: This symptom is observed under the following conditions:

  1) Attach the policy to both the outbound and inbound interfaces of the virtual template.

  2) Unconfigure the policy from the outbound and inbound interfaces of the virtual template.

  3) Re-attach the policy to the outbound interface of the virtual template.

  Workaround: There is no workaround.

- CSCsj00571

  Symptoms: A buffer memory leak may cause a SPA-IPSEC-2G to crash. When this situation occurs, the following error messages are generated in the logs:

  ```
  SPA_IPSEC-3-PWRCYCLE: SPA (<slot/subslot>) is being power-cycled (Module not
  responding to keep-alive polling) SPA_OIR-3-RECOVERY_RELOAD: subslot <slot/subslot>:
  Attempting recovery by reloading SPA ACE-6-INFO: SPA-IPSEC-2G[<slot/subslot>]: Crypto
  Engine X going DOWN
  ```

  Conditions: The conditions are as follows:

  – Large outbound packets (approx > 3500 bytes) undergo fragmentation first.

  – Followed by smaller outbound packets (approx > 1900 bytes) undergo fragmentation next.

  Workaround: Restrict the large packets going the VPNSPA by setting smaller MTUs.

- CSCsj01310

  Symptoms: With VRF configured, TCP probes turn FAILED and never become OPERATIONAL.

Conditions: Server farms & VServers are configured with access CLIs, and VRF forwarding is enabled in the client/server interfaces.

Workaround: There is no workaround.

- CSCsj05251

  Symptoms: An IOU image crashes during bootup.

  Conditions: The IOU image crashes after CSCsi64025 fix.

  Workaround: There is no workaround.

- CSCsj07189

  Symptoms: Entering the **snmpget** of an object identifier (OID) using the interface index (ifIndex) value of an interface for its index will result in an error:

  snmpget -c <community> -v1 <device> IF-MIB::ifDescr.92

  Error in packet Reason: (noSuchName) There is no such variable name in this MIB. Failed object: IF-MIB::ifDescr.92

  Conditions: This can occur after port adapters (PAs) have been swapped, such as replacing a 4-port PA with an 8-port PA.

  Workaround: Use the **snmpwalk** to retrieve the IF-MIB values.

- CSCsj07297

  Symptoms: Config sync is seen with Cisco 7600 HA routers.

  Conditions: This symptom is observed when the **no vrrp 1 preempt** interface configuration command is configured and when a switchover is done from primary to secondary.

  Workaround: There is no workaround.

- CSCsj07446

  Symptoms: When L4 Redirect is configured for a traffic class with an inbound ACL only, downstream traffic may not be translated.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG.

  Workaround: Configure both an inbound and outbound ACL for the traffic class.

- CSCsj14847

  Symptoms: The **crypto connect** command on a channelized T3 WAN card (serial interface in the non-channelized mode) is lost after a chassis reload or a WAN card reload.

  Conditions: Chassis reload with the **crypto connect** command in the startup configuration for a serial interface. WAN card reload with the **crypro connect** command configured on the serial interface.

  Workaround: Reconfigure the **crypto connect** command.

- CSCsj18688

  Symptoms: In the display of the **show l2 sess all vcid** command, the block containing “FS flash header information” is moved before the display of the counters, resulting in regression.

  Conditions: All.

  Workaround: There is no workaround.

- CSCsj19308

  Symptoms: MLPPP/MLFR ping failure on SPA-2/4CT3 or SPA-CH-STM.

Conditions: MLPPP/MLFR configured on SPA-2/4CT3 or SPA-CH-STM.

Workaround: Reload the SPA using hw-module subslot <slot>/<subslot> reload,

- CSCsj21066

  Symptoms: IPv4 eBGP or IPv6 eBGP session flaps when its configuration is unchanged.

  Conditions: This symptom occurs when route-target configuration is changed on another eBGP session on the same link.

  Workaround: There is no workaround.

- CSCsj21099

  Symptoms: IPv4 eBGP session flaps when IPv6 address family is removed from VRF configuration; IPv6 eBGP session flaps when IPv4 address family is removed from VRF configuration.

  Conditions: The symptom occurs only with images that support “vrf definition” configuration.

  Workaround: There is no workaround.

- CSCsj25562

  Symptoms: A router that functions in a BBA QoS configuration may crash when a shaper policy map is removed from a PPPoEoVLAN subinterface while QoS sessions are being established.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may not be limited to a PRE-3.

  The issue is not present in any released images; it is present only in a few interim images leading up to the final 12.2(31)SB6 image.

  Workaround: There is no workaround.

- CSCsj29687

  Symptoms: An ATM VC may remain down until you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the ATM VC is configured.

  Conditions: This symptom is observed after a service policy has been added to or deleted from the ATM VC.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the ATM VC after the service policy has been added or deleted.

- CSCsj30138

  Symptoms: The standby PRE-2 may fail to boot. It may reach the standby hot state but may then reload after a “Bulk-sync failure” error is displayed on the console:

  ```
  Config Sync: Bulk-sync failure due to BEM mismatch
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB5 when SSH Version 1 (SSHv1) or SSH Version 2 (SSHv2) is configured. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsj43962

  Symptoms: ISG may send the physical MAC address in ARP reply packets when Gateway Load Balancing Protocol (GLBP) may require the virtual MAC address (VMAC) for proper operation.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, that functions as an ISG, and that connects to another ISG via an interface that is configured for GLBP.

  Workaround: There is no workaround.

- CSCsj50333

  Symptoms: An ISSU on a Cisco 7600 series may fail.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when, after you have entered the **runversion** command, the ifIndex bulk synchronization client sends infinite messages to the peer because it has entered into an endless loop.

  Workaround: There is no workaround.

- CSCsj54395

  Symptoms: A crash occurs when the IPHC **ip tcp header compression** command is configured.

  Conditions: This symptom occurs when the IPHC **ip tcp header compression** command is configured with SLIP encapsulation.

  Workaround: Use ppp/hdlc/x25/fr encapsulation.

  Further Problem Description: The crash occurs with 12.2S/12.2SR/12.2SX images, but not with 12.4/12.4T/12.0S images.

- CSCsj66522

  Symptoms: A line card crashes when running a script that adds or deletes interfaces bundles, changes encapsulation, or changes CRC.

  Conditions: Include the following:

  ```
  top# show context slot 5

  CRASH INFO: Slot 5, Index 1, Crash at 13:44:02 UTC Sun Jul 15 2007
  VERSION:
  GS Software (GLC1-LC-M), Version 12.0(071407A2.2007-07-14) UBUILDIT Image, CISCO
  DEVELOPMENT
  TEST VERSION
  Compiled Sat 14-Jul-07 15:28 by xxxxxxxx
  Card Type: ISE 2.5G SPA Interface Card, S/N SAD10250A6D
  ```

  Workaround: There is no workaround.

- CSCsj67820

  Symptoms: A virtual cem interface does not get deleted when there are no VCs configured under the interface.

  Workaround: There is no workaround.

- CSCsj93643

  Symptoms: In rare cases, a Cisco 12000 router with a SIP400 and one or more SPA-CT3/DS0 and SPA-T3E3 installed may display the following message:

  ```
  SLOT 14:Jul 22 06:18:31.790 EDT: %SPA_PLIM-3-HEARTBEAT: Subslot 2 has experienced an
  heart beat failure Current Sequence 1980 received Sequence 1970 Time since last keep
  2952ms.
  ```

  The SPA-CT3/DS0 and SPA-T3E3 may stay in the state, and the SPA may not recover in some cases.

  Workaround: The following command may be used to disable SPA heartbeat to avoid the SPA failure.

  execute-on <slot#> test hw-module subslot <subslot#> ipc keepalive disable

  It is not recommended to use this command, and it may cause the SPA to become stuck in the bad state. The test command shall be used under Cisco Support supervision.

- CSCsj94561

  Symptoms: A router may crash because of a bus error when you perform an OIR of a PA-MC-8TE1+ port adapter or when you enter the **hw-module slot** *slot-number* **stop** command for the slot in which the PA-MC-8TE1+ port adapter is installed.

  Conditions: This symptom is observed on a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCsj94583

  Symptoms: When a service policy with “priority + Police cir percent x” is applied on a subinterface, it is not being accepted for all the percent values.

  Conditions: When police cir percent conversion to cir value increases a certain range, the policy is not being accepted.

  Workaround: There is no workaround.

  Further Problem Description: Here, the cause was seen in the function af_policer_percent_to_bps. The percent value is converted to the rate, and it is compared to temp_visible_bandwidth (which is the max allowed rate). The var temp_visible_bandwidth was of type ulong, so it was not holding the right max allowable value. So the calculated rate from percent was always greater than temp_visible_bandwidth.

- CSCsj99980

  Symptoms: User is not able to configure AToM xconnects on interfaces that use PA-POS-1OC3 cards. The following error message is displayed:

  ```
  MPLS encap is not supported on this circuit
  ```

  Conditions: xconnects cannot be configured when PA-POS-1OC3 cards are used.

  Workaround: There is no workaround.

- CSCsk00054

  Symptoms: Packets requiring fragmentation going into an mGRE tunnel are dropped.

  Conditions: Symptoms are observed consistently when using mGRE.

  Workaround: It is possible to specify a large MTU on the GRE tunnel in order to avoid fragmenting going into the tunnel.

- CSCsk06279

  Symptoms: Port no calculation for pc evc egress port is missing in a few places.

  Conditions: Found during code walk-through.

  Workaround: There is no workaround.

  Further Problem Description: During the code walk-through, I found a few places where the egress port number calculation for pc evc was needed but it was not present.

- CSCsl17798

  Symptoms: Etherchannel membership on standby supervisor is inconsistent with the state on active supervisor. Reported in ESM-20G line card.

  Conditions: This defect may be seen with Etherchannel mode “on” and on a standby reload. Reported in Cisco 7600 series router. Could impact other platform as well.

  Etherchannel configuration and performing SSO.

  Impact: This may impact traffic forwarding. Etherchannel state inconsistent between active and standby.

Frequency: Every time when Line card reloads.

Workaround: Once standby supervisor has reached hot, remove etherchannel configuration and repapply. No other workaround exists.

- CSCsl33632

  Symptoms: Router crashes when VRF is unconfigured.

  Conditions: Crash is observed on Cisco 7200 router while VRF is unconfigured.

  Workaround: There is no workaround.

- CSCsl49124

  Symptoms: Observing the issue while booting the router.

  Conditions: On booting the router the issue was seen

  Workaround: There is no workaround.

- CSCsl51945

  Symptoms: The HSRP IPv6 configuration on the standby RP may lose its address. The configuration on the standby RP appears as:

  standby 1 ipv6 ::

  The standby resets as well.

  Conditions: This will occur if group is in init state while doing the configuration or changes its state to init after applying the configuration. If you re-apply the command on the active RP without first removing it then a config sync error will occur and the standby RP will reload.

  Trigger: Standby RP on switchover stucks in standby-cold state.

  Impact: Secondary RP resets, configuration sync failure.

  Workaround: There is no workaround.

- CSCsl60107

  Symptoms: VPLS/EoMPLS traffic may be dropped at imposition when a WRED policy applied to any port on the same HW datapath on SIP600 or ES20.

  Additionally, QoS may be incorrectly applied and traffic may stop on an FRR cutover of a VPLS/EoMPLS VC under similar conditions to above.

  Conditions:

  1. If a VPLS/EoMPLS VC egresses a port with no QoS applied and any other port on the LC has a WRED policy applied, the VC's traffic may be dropped in the imposition direction, or misqueued.
  2. If a VC is FRR protected and BOTH the primary and backup paths egress ports on the second datapath on ES20 (ports 10-19), VC traffic may be dropped on tunnel switchover to the backup path.

  Workaround:

  1. Configure QoS on the egress interface carrying the VPLS/EoMPLS VC.
  2. Configure primary and backup tunnel paths to egress interfaces on the first 10 ports of ES20.

- CSCsl70667

  Symptoms: A line card crash is observed after the following error messages:

  ```
  FIBXDRINV: Invalid XDR format. FIB entry XDR has bogus routecount
  ```

  Conditions: This error message and crash are seen very rarely after OIR of the line card.

Workaround: There is no workaround.

- CSCuk44154

  Symptoms: RPR+ mode does not work properly from a CEF perspective because the forwarding dBase is synced across from the active to redundant RP (RRP). Syncing of the forwarding dBase should happen only for SSO mode, and, consequently, Non-Stop Forwarding (NSF) should not occur in RPR+ mode.

  Conditions: Upon switchover to the RRP in RPR+ mode. The CEF forwarding dBase is already present, but should be re-created from the config.

  Workaround: There is no workaround.

- CSCuk54570

  Symptoms: IPv6 communication does not function.

  Conditions: This symptom is observed between two 6PE routers that are connected by a TE tunnel when CEFv6 does not resolve properly for these routers. The symptom does not occur for IPv4.

  Workaround: Enable an LDP session through the tunnel by entering the **interface tunnel** *te number* command followed by the **mpls ip** command.

- CSCuk61910

  Symptoms: A PE router crashes.

  Conditions: This symptom occurs while configuring MVPN.

  Workaround. There is no workaround. The bug is 100-percent reproducible.

TCP/IP Host-Mode Services

- CSCeb54456

  Symptoms: A data-link switching plus (DLSw+) circuit may not function when a TCP connection gets stuck. After about 90 seconds, the TCP connection is closed by DLSw+, and a new TCP connection is built for DLSw+. Once the new TCP connection is up, the DLSw+ circuit starts functioning again.

  Conditions: This symptom is observed on a Cisco router that is configured with both a DLSw+ interface and an ATM interface.

  Workaround: If this is an option, remove the ATM interface from the router. When you configure the DLSw+ interface and the ATM interface on different routers, the symptom does not occur.

- CSCec79570

  Symptoms: User Datagram Protocol (UDP) port 1985 (on which Hot Standby Router Protocol [HSRP] runs) may be opened by a port scan. This is improper behavior.

  According to the router log, the router does not generate a message that indicates that UDP port 1985 cannot be reached, as it should do.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(2)T1 but may also occur in other releases.

  Workaround: There is no workaround.

- CSCsb51019

  Symptoms: A TCP session does not time out but is stuck in the FINWAIT1 state, and the following error message is generated:

  ```
  %TCP-6-BADAUTH: No MD5 digest from x.x.x.x to y.y.y.y(179) (RST)
  ```

Conditions: This symptom is observed on a Cisco router that is configured for BGP and that is connected to a third-party vendor router after the BGP authentication password is changed on the Cisco router.

Workaround: Identify the BGP connection that is stale by entering the **show tcp brief** command, and then clear the TCP control block.

- CSCsc39357

  Symptoms: A Cisco router may drop a TCP connection to a remote router.

  Conditions: This symptom is observed when an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than what the remote router can handle, causing the remote router to advertise a zero window. Subsequently, when the remote router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be sent to the remote router, the Cisco router may drop the TCP connection.

  Workaround: Increase the window size on both ends to alleviate the symptom to a certain extent. On the Cisco router, enter the **ip tcp window-size** *bytes* command. When you use a Telnet connection, reduce the *screen-length* argument in the **terminal length** *screen-length* command to 20 or 30 lines.

- CSCsh92986

  Symptoms: The latency for the RSH command could increase when they are flowing through an FWSM module.

  Conditions: The following issue was observed on an FWSM that is running 2.2 (1) software. The long delay was triggered by using either Cisco IOS Release 12.3(13a)BC1 or Release 12.3(17a)BC1 on routers toward which those RSH commands were sent.

  Workaround: Either bypass the FWSM module or downgrade to Cisco IOS Release 12.3(9a)BC3, which is not affected by this extra delay issue.

- CSCsi40766

  Symptoms: H.323 calls on a Cisco IOS VoIP gateway may fail after the gateway has processed about 54,500 calls.

  Conditions: This symptom is observed when H.323 uses TCP to transport signaling messages. When the Cisco IOS gateway must generate a unique port for the local TCP session, this port is selected from a range of open ports. When the number of times that an unique TCP session is created for the same IP address on the gateway exceeds 54,500, further attempts to create a local TCP port fail and calls are not completed.

  The symptom occurs for H.323 calls only when a separate TCP session is established for the H.245 session. When H.245 tunneling is enabled or no H.245 session is established, the symptom does not occur for H.323 calls.

  When the **debug ip tcp transaction** command is enabled on the gateway, the “TCP: Ran out of ports for network 0” debug output is generated when the symptom occurs.

  Enabling debugs on a Cisco IOS gateway should always be done with caution to minimize impact to the performance of the router. At a minimum, ensure that logging to the console is changed from the default behavior of the debug level to, for example, an informational level.

  Workaround: After the symptom has occurred, reload the Cisco IOS VoIP gateway. To prevent the symptom from occurring, ensure that for H.323 call processing all H.323 devices have H.245 tunneling enabled. This may not always be possible: for example, H.245 tunneling on Cisco CallManager is not supported.

- CSCsi43868

  Symptoms: TCP listening ports cease to respond to incoming SYN packets.

  Conditions: This condition occurs if a system receives the initial SYN packets but does not receive the final ACK to complete the 3-way handshake.

  Workaround: There is no workaround.

  Further Problem Description: This issue affects only images that have the fix for CSCef74037.

- CSCsi92978

  Symptoms: The “Show udp/Show ip socket” local address field may show “--any--” for port 161 and 162 because of the output of the snmp walk command showing an IP address as 0.0.0.0.

  Conditions: This problem is observed on a Cisco 7200 router with a Cisco IOS image.

  Workaround: There is no workaround.

- CSCsj62846

  Symptoms: A MIB walk of the udpTable will have extra bad entries when a UDP IPv6 connection to the box is made.

  Conditions: IPv6 must be configured, and an IPv6 UDP socket must be present.

  Workaround: There is no workaround. The symptom should not interfere with normal box operation.

Wide-Area Networking

- CSCdw04802

  Symptoms: The virtual-access counters and the RADIUS accounting data exceed the real value.

  Conditions: This symptom is observed on a Cisco 7200 PA-A3 port adapter and a Cisco 6400 NRP2-SV when a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) uses an ATM permanent virtual connection (PVC) as an ingress interface for L2TP tunnels.

  Workaround: Configure an Ethernet port as the ingress interface.

- CSCec27942

  Symptoms: A virtual-access interface is not freed when a client session is torn down.

  Conditions: This symptom is observed on a Cisco router that is configured for VPDN when the client session is momentarily disconnected and then reconnected.

  Workaround: There is no workaround.

- CSCee56988

  Symptoms: High CPU usage occurs on a Cisco 7301, and the following error message and traceback are generated:

  ```
  %TCP-2-INVALIDTCPENCAPS: Invalid TCB encaps pointer: 0x0 -Process= "L2X SSS manager",
  ipl= 0, pid= 69 -Traceback= 0x606E43DC 0x60B9FAC8 0x60BA11C4 0x619F502C 0x619F4A2C
  0x619F4D34 0x619F35C4 0x619F4FF4 0x619F6820 0x619F5ED8 0x619F6350 0x619CA1F4
  0x619CA6C4 0x619D2524 0x619CABB4 0x619CAFA0
  ```

  Conditions: This symptom is observed on a Cisco 7301 that runs Cisco IOS Release 12.4(5b) with PPTP/VPDN connections after, on a connected platform, rate limiting is changed to MQC policy-based limiting of the bandwidth. Note that the symptom may be release-independent.

  Workaround: There is no workaround.

- CSCef67942

  Symptoms: The amount of free processor memory slowly decreases because the “IP input” process holds increasingly more memory. This situation finally leads to MALLOC failures and a crash.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(6) or a later release, that is configured with dialer interfaces, and that is configured for large-scale dial-out (LSDO).The symptom may be release-independent.

  Workaround: When the amount of free processor memory becomes too low, reload the router when it least affects the service.

- CSCef71011

  Symptoms: Pings fail when translational bridging and ATM DXI encapsulation are configured.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, Release 12.2S, or a release that is based on Release 12.2S.

  Workaround: Do not configure ATM DXI encapsulation. Rather, configure HDLC, PPP, or Frame Relay encapsulation.

- CSCeh25440

  Symptoms: InvARP packets on multiple MFR bundle interfaces may be dropped, causing traffic to fail after you have reloaded microcode onto a line card that processes a high load of traffic over many PVCs on MFR interfaces.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S when 42 MFR bundles are configured over 336 full T1s and when egress MQC is configured on the 42 MFR bundle interfaces. However, the symptom is not platform- and release-specific.

  Workaround: There is no workaround.

- CSCeh32353

  Symptoms: An LNS intermittently routes packets to an incorrect interface in the process-switching path, preventing some applications from working properly. These applications, such as ARP, CBAC, and NAT, depend on the first packet to go to process-switching for their initialization operation. Consequently, this situation may affect user connectivity to the Internet.

  Conditions: This symptom is observed when the next-hop ISP router is connected via static routes and when there is no ARP entry on the LNS.

  Workaround: There is no workaround.

- CSCeh35068

  Symptoms: CEF adjacency is not established with a serial interface with Frame Relay and FR-IETF encapsulation.

  Conditions: The symptom has been observed on a Cisco 7200 router with a CE1 potent interface.

  Workaround: Enter the **shutdown** command and then the **no shutdown** command on that interface.

- CSCek54185

  Symptoms: When you add Variable Bit Rate (VBR) traffic shaping parameters to active PPPoA sessions, a Cisco 10000 series may crash and generate the following error message:

  ```
  %ERR-1-GT64120 (PCI-1)
  ```

  Conditions: This symptom is observed when PPPoA sessions without VBR are in the process of coming up while you add VBR traffic shaping parameters.

Workaround: Wait until the sessions are completely up and then add VBR traffic shaping parameters.

- CSCek56693

  Symptoms: When you deactivate an ATM PVC, an “ALIGN-3-SPURIOUS” error message may be generated on the console.

  Conditions: This symptom is observed when the ATM PVC is carrying PPPoA sessions.

  Workaround: Deactivate the PPPoA sessions before you deactivate the ATM PVC.

- CSCek76406

  This caveat consist of two symptoms, two conditions, and two workarounds:

  Symptom 1: A Cisco 7200 series may crash when payload compression is added to or removed from an MFR interface that has interface fragmentation configured.

  Condition 1: This symptom is observed when traffic is sent through an MFR interface that has or had interface fragmentation and payload compression configured. The symptom may not be platform-specific.

  Workaround 1: There is no workaround. Do not configure both interface fragmentation and payload compression on an MFR interface.

  Symptom 2: A Cisco 7200 series may crash when you remove interface fragmentation from an interface that is configured for Frame Relay encapsulation while traffic is running.

  Condition 2: This symptom is observed with both serial Frame Relay and MFR interfaces. The symptom may not be platform-specific.

  Workaround 2: Shut down the interface before you remove interface fragmentation.

- CSCek77555

  Symptoms: PPP may not start on a serial interface that is physically up. When this situation occurs, inspection of the interface via the **show interface** command shows that the physical layer is up, but that the line protocol is down, and that LCP is closed.

  Conditions: This symptom is observed only on regular serial interfaces that use PPP encapsulation. The symptom does not occur with tunneling mechanisms such as PPP over ATM (PPPoATM) or VPDN sessions. The symptom may occur when the physical layer undergoes multiple state transitions, starting from an up state and ending in an up state, with the entire sequence occurring over a short period of time. In such a situation, event filtering mechanisms in Cisco IOS software may prevent a notification from being sent to PPP when the link returns to an up state and, in turn, PPP from (re-)starting on the interface. The most likely time for such a situation to occur is when PPP itself resets the interface, which occurs when an existing PPP session is terminated because of a keepalive failure or LCP negotiation failure.

  Workaround: Any sequence that resets the physical layer and that is slow enough that the filtering mechanisms do not once again intrude is sufficient to restart PPP. For example, you can restart PPP on the interface by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCek78126

  Symptoms: A compilation error occurs.

  Conditions: This symptom occurs because vpdn ever enable variable is missing in autobahn76.

  Workaround: There is no workaround.

- CSCin86951

  Symptoms: An LNS router crashes on establishing a large number of PPPoA L2TP sessions.

Conditions: This symptom is observed only when you establish sessions at a high rate. When you attempt to establish 8000 sessions, the router crashes shortly after 5000 sessions are established.

Workaround: Establish sessions at a low rate.

- CSCsb11520

  Symptoms: A Cisco 7204 series will display "%SYS-2-LINKED: Bad enqueue of 6318AECC in queue 6313B39C" when attempting to dial out over ISDN.

  Conditions: This symptom is observed on a Cisco 7204VXR that runs Cisco IOS Release 12.2(29) and that is configured with an NPE-400 processor. The dial out attempt fails to connect to the remote end. Connections dialing in to the same interface will establish okay.

  Workaround: There is no workaround.

- CSCse81327

  Symptoms: When a main interface has subinterfaces and is configured for Frame Relay encapsulation and when a subinterface is deleted and then re-added, the DLCI information is not re-added to the running configuration, and no error message is generated to indicate an error.

  Conditions: This symptom is observed on a Cisco router only when the main interface is shut down. If the main interface is administratively up, the symptom does not occur.

  Workaround: Do not provision and rollback subinterfaces on main interfaces that are shut down.

- CSCsf30411

  Symptoms: In an L2TP dialout configuration, when a failover occurs and when limit and priority options are specified, the output of the **show vpdn** command may be incorrect. This situation causes the limit option to be unusable.

  Conditions: This symptom is observed when limit and priority options are enabled on the LNS and when a ping is made from the LNS to two LACs to check if the limit option functions. The session should be the same as that of the limit, but is more than the specified limit.

  Workaround: There is no workaround.

- CSCsg56725

  Symptoms: When you enter the **terminate-from hostname** *hostname* command to terminate L2TP tunnels, some L2TP tunnels are terminated in the wrong VPDN group while other L2TP tunnels on the same host are terminated in the correct VPDN group.

  Conditions: This symptom is observed on a Cisco 7206VXR that has an NPE-G1 and that runs Cisco IOS Release 12.2SB and occurs only during the first two or three minutes after the router has booted. After that period, the symptom no longer occurs. Note that the symptom is both platform- and release-independent.

  Workaround: To prevent the symptom from occurring, enter the **no aaa accounting system guarantee-first** command on the router before you reload the router. Doing so enables the tunnels to be terminated in the correct VPDN groups.

  After the symptom has occurred, clear each of the affected tunnels by entering the **clear vpdn tunnel id** *local-id* command. Then, after the tunnels have been re-established, you should be able to terminate them in the correct VPDN groups.

- CSCsg89222

  Symptoms: A PPP session that is initiated from a client may not be forwarded to an LNS.

  Conditions: This symptom is observed on a Cisco router after the PPP session has been established.

  Workaround: Enter the **vpdn source-ip** global configuration command.

- CSCsh02500

  Symptoms: L2TP sessions fail when the L2TP peer (that is, the LAC if Cisco IOS software is acting as an LNS) is sending L2TP AVPs that are hidden. “Debug vpdn error” will show the following error message:

  ```
  Error unhiding AVP <x>, no shared secret configured
  ```

  Conditions: This symptom occurs when the L2TPv2 tunnel protocol is used and when the L2TP peer is sending L2TP AVPs hidden according to RFC 1661, section 4.3.

  Workaround: There is no workaround.

- CSCsh06841

  Symptoms: A router may crash while establishing a PPP session.

  Conditions: This symptom is observed when the **ppp reliable-link** interface configuration command is enabled on an interface that is bound to a dialer profile.

  Workaround: Disable the **ppp reliable-link** interface configuration command, save the configuration, and reload the router. Disabling the command without reloading the router is not sufficient.

- CSCsh27457

  Symptoms: On an HA BBA, the standby RP disconnects PPPoE sessions when the **ppp lcp echo mru verify** command is configured under the Virtual-Template.

  Conditions: This symptom occurs when the **ppp lcp echo mru verify** command is configured under the Virtual-Template.

  Workaround: Do not configure the **ppp lcp echo mru verify** command.

- CSCsh49699

  Symptoms: A router may crash when you configure Frame Relay fragmentation on a Frame Relay main interface after the following error message has been generated:

  ```
  Leased-line fragmentation works with main interface service-policy only, please
  remove policy under subinterface/PVC and re-enter the command.
  ```

  Conditions: This symptom is observed on a Cisco router after you first attempt to configure Frame Relay fragmentation on a Frame Relay main interface that has a service policy on a subinterface, when you then remove the service policy from the subinterface, and when you then again attempt to configure Frame Relay fragmentation.

  Workaround: After the error message has been generated, immediately remove the Frame Relay fragmentation before you remove the service policy.

- CSCsh62833

  Symptoms: The **sessions per-mac throttle** command functions as expected, but when you enter the **show pppoe throttled mac** command, no output is displayed, and a warning message and traceback are generated:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 70A48450
  chunkmagic 0 chunk_freema0 -Process= "Exec", ipl= 0, pid= 234 -Traceback= 6053AADC
  606167A8 6158DB78 61578A28 61578B4C 604E4BF4 601C01E8 604FE6F8 60617B54 60617B40
  604FE6F8 60617B54 60617B40
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has an PRE-2, that runs Cisco IOS Release 12.2(28)SB4, and that is configured for PPPoE connection throttling. Note, however, that the symptom is not platform-specific.

  Workaround: There is no workaround.

- CSCsh72559

  Symptoms: The **show pppoe throttled mac** command may display no or invalid output.

  Conditions: The problem may be seen when the **show pppoe throttled mac** command is issued.

  Workaround: There is now workaround.

- CSCsi00004

  Symptoms: The following errors are displayed:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=657A5740, count=0
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61A716DC reading 0x22
  ```

  The line protocol may also go down.

  Conditions: These errors may be seen when removing frame-relay payload-compression configuration when frame-relay interface fragmentation is configured.

  Workaround: Remove the frame-relay interface fragmentation configuration before removing frame-relay payload-compression.

- CSCsi02669

  Symptoms: A router may reload while displaying the output of the **show ppp multilink** command.

  Conditions: This symptom is observed when the multilink bundle goes down while the output is being displayed.

  Workaround: There is no workaround.

- CSCsi51530

  Symptoms: If a non-Cisco PPPoA client is dialing in to a Cisco router, the call may fail at the PPP authentication phase. When this situation occurs, the following error message is generated:

  ```
  Failed to send an authentication request x
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB5.

  Workaround: There is no workaround.

- CSCsi57143

  Symptoms: After an SSO switchover has occurred, some serial interfaces may remain down on the newly active RP.

  Conditions: This symptom is observed on a Cisco router that has several serial interfaces with PPP encapsulation up and running on the active RP before the SSO switchover occurs.

  Workaround: There is no workaround.

- CSCsi60136

  Symptoms: The standby processor on a router that is configured for PPP may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router when the **debug ppp redundancy** command is enabled on the standby processor.

  Workaround: Do not enable the **debug ppp redundancy** command on the standby processor.

- CSCsi69009

  Symptoms: High CPU usage may occur when IPCP is being renegotiated. Eventually, the high CPU usage may cause buffers to be backed up, may cause error message to be generated, and may cause L2TP tunnels to be dropped.

Conditions: This symptom is observed on a Cisco router when clients renegotiate IPCP unnecessarily. You can verify this situation by enabling the **debug ppp negotiation** command or by configuring RADIUS authorization and then checking the virtual-access interface for the phrase “cloned from: AAA, AAA, ...” (that is, multiple instances of AAA) as identification.

Workaround: There is no workaround.

Further Problem Description: You can alleviate the situation somewhat by configuring the NCP timeout to 15 seconds to disconnect clients that take a long time to renegotiate IPCP. You can also do the following:

- Increase the hello timers for L2TP and for the receive windows.
- Configure the timers under the virtual template.
- Do not configure the **redistribution connected** command under a routing protocol such as (but not limited to) EIGRP, RIP, or OSPF.
- Ensure that the IP local pools are concise. For example, create one statement for multiple /24s instead of splitting all /24s on single lines, because with single lines, the look-up becomes long and contributes to the high CPU usage.

- CSCsi72045

  Symptoms: A bus error crash occurs on a Cisco router that is running Cisco IOS Release 12.2(31)SB3.

  Conditions: This symptom is seen with AAA and PPPoE configured.

  Workaround: There is no workaround.

- CSCsi78968

  Symptoms: When a multilink bundle comes up, the following error message may be generated:

  ```
  SYS-2-INTSCHED: ’idle’ at level 2 -Process= "PPP Events"
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3.

  Workaround: There is no workaround.

- CSCsi82832

  Symptoms: FastStart does not function on PPP interfaces. (FastStart is enabled by default for regular serial interfaces.)

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

  Further Problem Description: FastStart acts as a partial solution for the condition that is described in caveat CSCek77555, because FastStart enables an inbound packet from a peer to trigger the startup of PPP (that is, FastStart brings PPP out of the inert state that is documented in caveat CSCek77555).

- CSCsi94498

  Symptoms: Alternate packets may be dropped during a ping test.

  Conditions: This symptom is observed when you initiate a ping over a Frame Relay PVC bundle.

  Workaround: There is no workaround.

- CSCsj05288

  Symptoms: When you delete a Frame Relay subinterface, the following error message and a traceback may be generated continuously:

  ```
  SYS-2-BADSHARE: Bad refcount in retparticle
  ```

Conditions: This symptom is observed on a Cisco router when a Frame Relay subinterface with a service policy is applied inside a VRF.

Workaround: Recreate and then delete the interface. When you do so, the error message and a traceback are no longer generated.

- CSCsj10933

  Symptoms: Under extremely unusual conditions, a multilink-group interface may not start PPP after two or more serial links have negotiated PPP and joined that bundle interface, creating a bundle. Inspection of the output from the **show ppp multilink** command will show that the bundle exists and has active member links; however, inspection of output from the **show interface** and **show ppp interface** commands will reveal that the bundle interface is in a Line-Protocol Down state and will further indicate that the bundle interface is in the "LCP Negotiating" phase.

  Conditions: This symptom can occur if two or more PPP serial links are assigned to a common multilink-group interface, and the links come up and negotiate PPP in near perfect simultaneity, but the links do not receive the exact same remote endpoint identification credentials (these being the PPP Multilink Endpoint Discriminator and/or PPP Authenticated username) on all the links. Note that this situation should never normally arise, at it could not itself occur except as a result of some other error (for example a cabling error, a misconfiguration at one end or the other, or an operational error with the remote system). It is implicit in being assigned to a single group interface that all links in the set will be providing identical identification information.

  Workaround: Any sequence that resets the bundle interface will generally clear the condition. For example, using the **clear interface Multilink10** command.

  Further Problem Description: This situation occurs if a link comes up and starts the formation of a bundle, and then a second link comes up—with conflicting identification information—in the window of time between when the first link starts the formation of the bundle and when that formation can be completed. Also note that this is specific to the use of static bundle interfaces (multilink group interfaces), and not an issue when dynamic (virtual-access) interfaces are used for the bundles.

- CSCsj12579

  Symptoms: The router can reload if using the vpdn-group command **lt2p ignore tx-speed** on a router acting as a LAC. This command is expected to be used on an LNS, but if it is used on the LAC, a reload can occur.

  Conditions: This symptom occurs on a router acting as a LAC. This command is expected to be used on an LNS, but if it is used on the LAC, a reload can occur.

  Workaround: There is no workaround.

- CSCsj36201

  Symptoms: The traffic flow stops and tracebacks are generated when the fragmentation size is changed by using an MQC shaped policy on a PVC. When the fragmentation size is set to a value equal to or larger than 700, the router hangs.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.2(31)SB4.

  Workaround: When the symptom occurs, you must power-cycle the router. To prevent the symptom from occurring, first remove fragmentation, change the size, and then reapply the map class. To prevent the router from hanging, use FRTS.

- CSCsj51280

  Symptoms: No debugs are displayed on the console. VPDN debugs are not displayed when conditional debugging like the **debug condition domain cisco.com** command or any other conditional debugging commands are enabled.

  Conditions: This symptom occurs only when conditional debugging is enabled (for example, the command above).

  Workaround: Do not enable the above conditional debugging to display the messages.

- CSCsj60578

  Symptoms: When the minimum number of links has joined a multilink bundle, Network Control Protocols (NCPs) such as IPCP fail to come up.

  Conditions: This symptom can occur if both peers are configured with the **ppp multilink links minimum mandatory** command.

  Workaround: Remove the **ppp multilink links minimum mandatory** command from the configuration.

- CSCsj75575

  Symptoms: A router may crash when Dynamic Bandwidth Selection (DBS) parameters are applied to a PPPoE session.

  Conditions: This issue arises only when DBS is configured.

  Workaround: Disable DBS.

- CSCsj75811

  Symptoms: MIB: cvpdnSessionAttrUserName is limited to 31 CHAR.

  Conditions: This symptom occurs on a Cisco IOS router acting as VPDN LNS and running Cisco IOS Release 12.4(15)T.

  Workaround: There is no workaround.

- CSCsj76378

  Symptoms: A router crashes when a vc-group is configured using an MFR bundle link interface.

  Conditions: This symptom occurs when an invalid FRF.5 configuration is attempted.

  Workaround: This is an invalid configuration. Use the MFR bundle interface instead of the bundle link.

Resolved Caveats—Cisco IOS Release 12.2(33)SRB2

Cisco IOS Release 12.2(33)SRB2 is a rebuild release for Cisco IOS Release 12.2(33)SRB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRB2 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCef77265

  Symptoms: A router may crash upon receiving certain TACACS+ packets.

  Conditions: This symptom is observed when the TACACS+ packets have the length of their headers set to zero.

Workaround: There is no workaround.

- CSCeh12411

  Symptoms: A router may hang when you enter the **show running-config** command.

  Conditions: This symptom is observed on a Cisco 7200 series but appears to be platform-independent.

  Workaround: Do not enter the **show running-config** command.

- CSCei62358

  Symptoms: A router may crash when a privilege-level 15 user logs on with the callback or callback-dialstring attribute.

  Conditions: This symptom is observed on a Cisco 805 that runs Cisco IOS Release 12.3(15) and on a Cisco 7600 series that has an RSP720 and that runs Release 12.2 (33)SRB1 when the following conditions are present:

  – The router is configured with AAA authentication and authorization.

  – The AAA server runs CiscoSecure ACS 2.4.

  – The callback or callback-dialstring attribute is configured on the AAA server for the user.

  Workaround: Do not configure the callback or callback-dialstring attribute for the user.

  Alternate Workaround: If the callback-dialstring attribute is used in the TACACS+ profile, ensure that the NULL value is not configured for the callback-dialstring attribute.

- CSCek68473

  Symptoms: A router may reload unexpectedly when you reconfigure the **login block-for** command.

  Conditions: This symptom is observed happens after a couple of invalid login attempts have occurred and then you reconfigure the **login block-for** command.

  Workaround: There is no workaround.

- CSCek73197

  Symptoms: The SNMP server engine ID is not removed after you have entered the **no snmp-server engineID** command. This situation can be verified in the output of the **show running-config | inc snmp-server** command.

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

  Workaround: There is no workaround.

- CSCse98807

  Symptoms: A “%SCHED-3-STUCKMTMR” error message and traceback may be generated during the “SNMP Timers” process.

  Conditions: This symptom is observed when there are too many RMON collection events and alarms. The error message and traceback may also be generated when many entries/rows are created in certain MIBs and occur because of simultaneous row creation timeouts.

  Workaround: Ensure that there are not too many RMON collection events and alarms or simultaneous row creation timeouts. However, note that the error message and traceback do not have an impact on the functionality of the platform. The messages are just warning messages from the Cisco IOS process scheduler, indicating that the process (in this case the “SNMP Timers” process) is not able to process all the events before the process suspends.

- CSCsg03830

  Symptoms: The **tacacs-server directed-request** command appears in the running configuration when is should be disabled. When you disable the command by entering **no tacacs-server directed-request** and reload the router, the command appears to be enabled once more.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for CSCsa45148, which disables the **tacacs-server directed-request** command by default.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa45148. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Temporary Workaround: Each time after you have reloaded the router, disable the command by entering **no tacacs-server directed-request**.

- CSCsg21398

  Symptoms: The Cisco IOS software image may unexpectedly restart when a crafted "msg-auth-response-get-user" TACACS+ packet is received.

  Conditions: This symptom is observed after the Cisco platform had send an initial "recv-auth-start" TACACS+ packet.

  Workaround: There is no workaround.

- CSCsh36727

  Symptoms: IP SLA MPLS path discovery may not properly discover the number of equal-cost MPLS paths between the router on which the IP SLA MPLS path discovery originates and the router that is the target of the path discovery request.

  Conditions: This symptom is observed when an IP SLA MPLS path discovery request is issued on a router for a target IP address and when some of the equal-cost paths between this router (that is, the originating router) and the target router traverse another router on which a single interface provides a connection to multiple downstream neighbors.

  Workaround: Do not use a single interface to connect to multiple downstream neighbors. Rather, use separate interfaces to connect to each of the downstream neighbors.

- CSCsh41142

  Symptoms: A router may crash when you unconfigure and reconfigure a RADIUS server.

  Conditions: This symptom is observed on a Cisco router when you first create 5000 PPPoE sessions in a load-balancing environment, clear the sessions, unconfigure a RADIUS server, and then reconfigure a RADIUS server.

  The following example shows the unconfiguring and reconfiguring of the RADIUS server:

  ```
  no radius-server host <ip-address 1> auth-port 1645 acct-port 1646 key <string>
  no radius-server host <ip-address 2> auth-port 1645 acct-port 1646 key <string>
  radius-server host <ip-address 3> auth-port 1814 acct-port 1815 key <string>
  ```

  Workaround: There is no workaround.

- CSCsj02971

  Symptoms: The **show ip cache aggregation as** command may not function properly.

Conditions: This symptom is observed on a Cisco 7600 series. When a flow to or from a Cisco ASN Gateway is equal to or larger than 2^16, the output of the **show ip cache aggregation as** command may show the flow as a negative number because a signed 16-bit integer is not properly used or displayed.

Workaround: There is no workaround.

- CSCsi48975

  Symptoms: A router may crash during the allocation of memory for subflows at the interrupt level.

  Conditions: This symptom is observed on a Cisco router that is configured for NetFlow.

  Workaround: Do not collect subflows such as BGP or IPM.

- CSCsi77983

  Symptoms: When NetFlow attempts to access a FIB source that is not present in the FIB, the router may crash.

  Conditions: This symptom is observed on a Cisco router that is configured with VLAN interfaces and virtual templates when a FIB source that is related to a virtual interface is not present in the FIB because of severe interface flaps.

  Workaround: There is no workaround.

- CSCsj44081

  Cisco IOS software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message whenever it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

  ```
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however provide an early indicator of other conditions that can eventually lead to poor system performance or a Cisco IOS software image restart.

  Recommended Action: Collect "show tech-support" command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORR UPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

- CSCsj72320

  Symptoms: A Cisco 7613 may crash during an SNMP dump, causing a memory allocation failure.

  Symptoms: This symptom is observed when you perform an SNMP dump by using an SNMP monitoring tool. The application queries the IP Tunnel MIB and CISCO-SWITCH-ENGINE-MIB on the router, causing a memory allocation failure, preventing the router from completing a SSO and creating a crashfile on the RP.

  Workaround: Remove the IP Tunnel MIB by entering the **remove tunnel mib** command.

Interfaces and Bridging

- CSCsf20714

  Symptoms: A DHCP relay may crash at the “print_unaligned_summary” function while requesting an IP address from a DHCP client.

  Conditions: This symptom is observed on a Cisco router after the bridge group has changed from one group to another.

  Workaround: There is no workaround.

- CSCsj57084

  Symptoms: Voice packets that are processed through a priority queue may be subjected to jitter.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with an Enhanced FlexWAN Module (WS-X6582-2PA) and a PA-A3-T3 port adapter.

  Workaround: There is no workaround.

- CSCsk28821

  Symptoms: A router may reload unexpectedly when you configure 34 or more double-tagged dot1q QinQ subinterfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB or Release 12.2(33)SRB1.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCei93768

  Symptoms: A Cisco router that is configured for BGP may crash and generate the following error messages:

  (Note that the hex values of tracebacks and other parameters that are part of the error messages will vary with different occurrences of the symptom).

```
%SYS-2-NOTQ: unqueue didn't find 4552953C in queue 454BE738
-Process= "BGP Router", ipl= 0, pid= 195
-Traceback= 4063BE54 4099DC2C 40C60FDC 40C6188C 40C627C8 4191C694 40C628BC 40C3BA10
40C3CCE0
%SYS-2-NOTQ: unqueue didn't find 455294EC in queue 454BE690
-Process= "BGP Router", ipl= 0, pid= 195
-Traceback= 4063BE54 4099DC2C 40C60FDC 40C6188C 40C627C8 4191C694 40C628BC 40C3BA10
40C3CCE0CMD: 'end'

%SYS-5-CONFIG_I: Configured from console by console
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header,
chunk 45519C14  data 4552953C  chunkmagic 15A3C78B  chunk_freemagic 0
-Process= "Check heaps", ipl= 0, pid= 6
-Traceback= 4063C5FC 4063C788 4065A9D0

chunk_diagnose, code = 2
chunk name is IP RDB Chunk

current chunk header = 0x0x4552952C
data check, ptr = 0x0x4552953C

next chunk header = 0x0x4552957C
data check, ptr = 0x0x4552958C
```

```
previous chunk header = 0x0x455294DC
data check, ptr = 0x0x455294EC
```

Conditions: This symptom is observed mostly with configuration changes that involve the **bgp dmzlink-bw** command for a BGP IPv4 address family, but in very rare cases, the symptom may also occur on other situations.

Workaround: There is no workaround.

- CSCek71050

  Symptoms: Compared to other Cisco IOS software releases, unusually high CPU usage may occur in the BGP router process on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Conditions: This symptom is observed when BGP is learning routes from the RIB, even if redistribution is not directly configured under BGP. (Redistribution from other routing protocols to BGP can exacerbate the CPU usage.)

  Workaround: There is no workaround.

- CSCek76776

  Symptoms: The configuration of a deleted subinterface may show up on a new subinterface and may cause a traffic outage.

  Conditions: This symptom is observed on a Cisco router that has IP interface commands enabled when a script adds and deletes ATM subinterfaces on a regular basis.

  Workaround: Verify the subinterface configuration. When the configuration of a subinterface cannot be deleted, delete the subinterface, and then create a dummy subinterface that will pull the configuration that could not be deleted. Then recreate the first subinterface with a new configuration.

- CSCek77898

  Symptoms: A router that runs BGP may crash when paths are imported from the global table into a VRF via the **import** *address-family* **map** *route-map* command under a VRF.

  Conditions: This symptom is observed when the import is denied for a path that was previously allowed to be imported into the VRF and may occur, for example, after a configuration change for the import route map.

  Workaround: There is no workaround.

- CSCek78043

  Symptoms: A high CPU usage may occur in the BGP scanner process when an IP prefix is imported from the global table into a VRF table or when a topology is imported.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR when either the **import** *address-family* command is entered under a VRF or when the **import topology** *topology-name* command is entered under a BGP configuration.

  Workaround: There is no workaround.

- CSCsd16043

  Symptoms: A Cisco IOS platform that is configured for Auto-RP in a multicast environment may periodically lose the RP to group mappings.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(17) when the RP drops the Auto-RP announce messages, which is shown in the output of the **debug ip pim auto-rp** command. This situation may cause a loss of multicast connectivity while the RP mappings are purged from the cache. See the following output example:

  ```
  Auto-RP(0): Received RP-announce, from ourselves (X.X.X.x), ignored
  ```

  Note that the symptom may also affect other releases.

Workaround: Create a dummy loopback interface (do not use the configured IP address in the whole network) and use the **ip mtu** to configure the size of the MTU for the RP interface to 1500 and the size of the MTU for the dummy loopback interface to 570, as in the following examples:

```
interface Loopback1
 ip address 10.10.10.10 255.255.255.255
 ip mtu 570
 ip pim sparse-mode
end
```

(This example assumes that the Auto-RP interface is loopback 0.)

```
interface Loopback0
 ip address 10.255.1.1 255.255.255.255
 ip mtu 1500
 ip pim sparse-dense-mode
end
```

- CSCse99493

  Symptoms: A router that is configured for NAT Overload may crash while performing dynamic translation from many ports to one port.

  Conditions: This symptom is observed after more than 5000 translations have been performed.

  Workaround: There is no workaround.

- CSCsf27220

  Symptoms: A router in which an ATM port adapter is installed may crash.

  Conditions: This symptom is observed on a Cisco router that is configured for Next Hop Resolution Protocol (NHRP) when traffic is sent.

  Workaround: There is no workaround.

- CSCsg16778

  Symptoms: A router may reload when Border Gateway Protocol (BGP) neighbor statements are removed from the configuration.

  Conditions: This symptom is observed in rare circumstances on a Cisco router when BGP neighbors are removed very quickly by a script at a much faster rate than manually possible and when a large BGP table is already present on the router before the script adds and removes the BGP neighbors.

  Workaround: There is no workaround.

  Further Problem Description: If you manually remove the BGP neighbors, it is less likely that the symptom occurs.

- CSCsg55591

  Symptoms: When there are link flaps in the network, various PE routers receive the following error message:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (1) received in update for prefix
  155:14344:10.150.3.22/32 from 10.2.2.1
  ```

  Or, a local label is not programmed into the forwarding table for a sourced BGP VPNv4 network.

  Conditions: These symptoms are observed when an iBGP path for a VPNv4 BGP network is present, and then a sourced path for the same route distinguisher (RD) and prefix is brought up.

  Workaround: Remove the iBGP path. Note that when the sourced path comes up first, the symptoms do not occur.

Alternate Workaround: Use different RDs with the different PE routers. When the RD and prefix do not match exactly between the iBGP path and the sourced path, the symptoms do not occur.

- CSCsg90755

  Symptoms: When a Cisco router that has redundant RPs that function in RPR+ or SSO mode is reloaded, the standby RP may not boot correctly and may continuously reload.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that has an IPv4 MDT address family. The symptom occurs because of configuration synchronization issues that are related to the IPv4 MDT address family.

  Workaround: There is no workaround.

- CSCsg97662

  Symptoms: When you enter the **no ip nat service skinny tcp port 2000** command, NAT is not disabled on port 2000. This situation causes NAT to be applied to SCCP packets, and causes the CPU usage to be very high.

  Conditions: This symptom is observed when an application is running on the port 2000.

  Workaround: There is no workaround.

  Further Problem Description: SCCP and NAT for voice are not supported in Cisco IOS Release 12.2 or a release that is based on Release 12.2. The **no ip nat service skinny tcp port 2000** command is not supported in these releases.

- CSCsh24687

  Symptoms: After you have changed the default local preference, the bestpath recalculation does not occur for the BGP VPNv4 table.

  Conditions: This symptom is observed on a Cisco router when you enter the **clear ip bgp * vpnv4 unicast soft** command after you have changed the default local preference.

  Workaround: There is no workaround.

- CSCsh53926

  Symptoms: A router may crash because of a bus error in the OSPF process.

  Conditions: This symptom is observed on a Cisco router that is configured for incremental SPF (ISPF) and that functions in a network with MPLS TE tunnels.

  Workaround: Remove the ISPF configuration.

- CSCsh66406

  Symptoms: When you enter the **maximum route** VRF configuration command or reduce the *limit* argument of the **maximum route** VRF configuration command, stale routes may occur in the BGP VPNv4 table.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the connection with a CE router is configured for another protocol than BGP such as OSPF and when the routes are redistributed into BGP.

  Workaround: If OSPF is the other protocol, enter the **redistribute ospf** address family configuration command.

- CSCsh78277

  Symptoms: An “Mwheel” CPU hog condition may occur, and the platform may crash.

  Conditions: This symptom is observed in a multicast configuration when an RPF link changes.

  Workaround: There is no workaround.

- CSCsh79933

  Symptoms: A BFD session works correctly for an EIGRP neighbor but only until the first BFD failure event occurs. After the first failure event has occurred, BFD sessions are not re-established for any EIGRP neighbors over the interface on which the BFD failure event occurred. EIGRP neighbors are re-established and function correctly, however without the benefits of BFD. The symptom occurs on a per-interface basis. BFD sessions can be verified by entering the **show bfd neighbor** command.

  Symptoms: This symptom is observed in a basic configuration involving at least two routers that are connected through a link that is configured for EIGRP and BFD.

  Workaround: Restart EIGRP.

- CSCsh82953

  Symptoms: On a PE router in an EIGRP network, EIGRP prefixes are redistributed into BGP but are missing their EIGRP-derived extended community values.

  Conditions: This symptom is observed only when a **network** command is manually entered in "router EIGRP" mode while the **redistribute eigrp** command already exists in the BGP configuration. The symptom does not occur if all final configuration statements are present at router bootup time.

  Workaround: Re-enter the **redistribute eigrp** command in the BGP configuration. There is no need to first remove the command because entering the command triggers a new redistribution event.

- CSCsh86124

  Symptoms: A BGP neighbor that uses an IPv6 peer address may not be established, and the neighbor state may be idle.

  Conditions: This symptom is observed when the interface that connects to the peer flaps.

  Workaround: Enter the **neighbor** *ip-address* **shutdown** router configuration command followed by the **no neighbor** *ip-address* **shutdown** router configuration command.

- CSCsh96955

  Symptoms: The next hop for a BGP route is marked as "inaccessible," preventing the route from being advertised to peers or installed in the routing table.

  Conditions: This symptom is observed on a Cisco router when all of the following conditions are present:

  – The route is an IPv6 route with an IPv6 next hop.

  – The route is learned from an IPv6 eBGP router that is one hop away.

  – Peering occurs between loopback addresses.

  – The **disable-connected-check** command is configured for the peer from which the route is learned.

  Workaround: Disable the **disable-connected-check** command on the peer from which the route is learned. Rather, configure eBGP multihop.

- CSCsi03359

  Symptoms: A PIM hello message may not reach the neighbor.

  Conditions: This symptom is observed on a Cisco router when an interface comes up and a PIM hello message is triggered.

  Workaround: Decrease the hello timer for PIM hello messages.

Further Problem Description: The symptom occurs because the PIM hello message is sent before the port can actually forward IP packets. IGP manages to get its neighborship up but PIM does not, causing RPF to change to the new neighbor and causing blackholing to occur for up to 30 seconds.

- CSCsi06948

  Symptoms: A switch or router may crash because of a bus error after a BGP dampening-related command is entered.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that has a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF7 but may also affect other platforms and releases.

  Workaround: There is no workaround.

- CSCsi42566

  Symptoms: A router may crash when the you enter the **show bgp l2vpn vpls rd** *vpn-rd* command.

  Conditions: This symptom is observed on a Cisco router when BGP is configured but an L2 VPN address family is not configured.

  Workaround: When the router does not have an L2 VPN address family, do not enter the **show bgp l2vpn vpls rd** *vpn-rd* command.

- CSCsi49948

  Symptoms: The local BGP MDT prefix may be missing.

  Conditions: This symptom is observed on a Cisco router that has the **mdt default** *group-address* command enabled under a VRF configuration and occurs after you have entered the **clear ip bgp *** command.

  Workaround: Disable and re-enable the **mdt default** *group-address* command.

- CSCsi82425

  Symptoms: When a secondary IP address is removed from an interface, the entire ARP table may be flushed.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2((33)SRB.

  Workaround: There is no workaround.

- CSCsi84089

  Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

  Workaround: Add area 0 in the OSPF VRF processes.

  Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

- CSCsi86386

  Symptoms: The **clear ip bgp * soft in** command does not function for an inbound route map.

  Conditions: This symptom is observed on a Cisco router that has the **neighbor send-label** command enabled when the prefix that is being filtered is an IPv4 unicast prefix.

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

  Further Problem Description: The **clear ip bgp * soft in** command does function fine for other address families such as VRF and VPNv4.

- CSCsi97315

  Symptoms: When you remove the **neighbor** *peer-group-name* **fall-over bfd** command for a peer group, the configuration is not removed from the members of the peer group, and the members may still register with through Bidirectional Forwarding Detection (BFD).

  Conditions: This symptom is observed on a Cisco router that has the following configuration:

  ```
  router bgp <as-number>
  neighbor <peer-group-name> peer-group
  neighbor <peer-group-name> remote-as <as-number>
  neighbor <peer-group-name> fall-over bfd
  neighbor <ip-address> peer-group <peer-group-name>
  ```

  When you enter the **neighbor** *peer-group-name* **fall-over bfd** command, the IP address that is associated with this command is not removed.

  Workaround: Remove and reconfigure the neighbor.

- CSCsj17820

  Symptoms: A router may crash when an MGRE tunnel interface that is configured for NHRP is removed.

  Conditions: This symptom is observed on a Cisco router that functions in a DMVPN network and occur only when the tunnel interface is removed through an automated script. The symptom does not occur during manual removal of the tunnel interface.

  Workaround: There is no workaround.

- CSCsj25841

  Symptoms: A BGP router may not send the default route to its neighbor.

  Conditions: This symptom is observed when the **neighbor default-originate** command is conditionally configured with a route map and when the matching route is installed into the RIB by BGP itself.

  Workaround: There is no workaround.

- CSCsj25940

  Symptoms: A router that is configured for EIGRP and BFD may generate the following error message and traceback:

  ```
  %SYS-2-NOTQ: unqueue didn’t find 667BD8F4 in queue 644087B4
  -Process= "Exec", ipl= 0, pid= 3,
  -Traceback= 0x608452B4 0x609CBCDC 0x612D8128
  ```

  Conditions: This symptom is observed on a Cisco router after you have entered the following commands:

  ```
  Router(config)#router eigrp <as-number>
  Router(config-router)#bfd interface <type number>
  Router(config-router)#no bfd interface <type number>
  ```

  Workaround: There is no workaround.

- CSCsj61743

  Symptoms: A BGP neighbor may not be able to establish a session, causing the session to become stuck in the passive connect state on one side and in the idle state on the other side. When this situation occurs, the output of the **show ip bgp vpnv4 all neighbor** *neighbor-address* command shows the following:

```
BGP neighbor is <ADDRESS>,  vrf <VRF-name>,  remote AS <AS>, external link
...
  BGP state = Idle
...
  Neighbor sessions:
    0 active, is multisession capable
  Message statistics, flags passive, state Connect:
...
```

  Conditions: This symptom is observed on a Cisco router that functions in a large BGP configuration with many VRFs after an interface has flapped.

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

- CSCsj71306

  Symptoms: After an RP switchover has occurred, BGP does not send a new BGP MDT update. Because of this situation, the MDT tunnel interface does not come up, and all multicast data traffic between VRFs is dropped after another RP switchover has occurred.

  Conditions: This symptom is observed after an RP switchover has occurred on a Cisco router that is configured for MVPN and that functions in SSO mode.

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

- CSCsj89029

  Symptoms: A router may crash after you have removed the route distinguisher (RD) for a VRF.

  Conditions: This symptom is observed when the VRF from which the RD was removed includes prefixes that were learned via BGP and that were imported from the global table.

  Workaround: There is no workaround.

- CSCsk19583

  Symptoms: A Multicast Virtual Private Networks (MVPN) may not function.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1, that uses extended communities to communicate the MDT information, and that interoperates with a Cisco IOS release that is earlier than Release 12.0(29)S or Release 12.2(31)SB.

  Workaround: There is no workaround.

- CSCsk39804

  Symptoms: The multicast Connection Admission Control (CAC) state may be incorrect after multicast routes have been cleared.

  Conditions: This symptom is observed on a Cisco router that has Source Specific Multicast (SSM)-mapped channels that are locally joined on the router.

  Workaround: There is no workaround.

- CSCsk43926

  Symptoms: High CPU usage may occur interrupt context on an RP, and spurious memory accesses may be generated when a route-map update is checked. You can verify this situation in the output of the **show align** command.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for BGP.

  Workaround: There is no workaround.

ISO CLNS

- CSCek76093

  Symptoms: A CLNS neighbor may still be formed after the IS-IS protocol has been shut down.

  Conditions: This symptom is observed only on serial interfaces.

  Workaround: There is no workaround.

- CSCsg40507

  Symptoms: BFD may not come up when an IP address on an interface is changed and when IS-IS is configured as the routing protocol.

  Conditions: This symptom is observed only when you first enter the **router isis** command and then enter the **bfd all-interfaces** command.

  Workaround: Unconfigure BFD, change the IP address, and then reconfigure BFD.

- CSCsh63785

  Symptoms: A MPLS tunnel may not come up after a stateful switchover (SSO) has occurred.

  Conditions: This symptom is observed on a Cisco router when Cisco IS-IS NSF is enabled and when IS-IS is used as the IGP for MPLS TE tunnels.

  Workaround: Do not configure Cisco IS-IS NSF. Rather, configure IETF NSF.

  First Alternate Workaround: Enter the **clear isis *** command.

  Second Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that is used for the MPLS TE tunnels after the SSO has occurred.

- CSCsi41944

  Symptoms: After redistribution-related configuration changes have been made, a CPUHOG condition may occur in the Virtual Exec process, causing loss of IS-IS adjacencies.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that runs Cisco IOS Release 12.2(18)SXF when the **redistribute maximum-prefix** command is configured under the **router isis** command and when BGP is configured to be redistributed into IS-IS. The symptom could also affect a Cisco 7600 series router that runs Release 12.2SR.

  Workaround: There is no workaround.

- CSCsi57971

  Symptoms: IS-IS may not advertise the prefix of a passive interface to the IS-IS database on a local router.

Conditions: This symptom is observed on a Cisco router when you shut down an interface (for example, G9/1/1) of a 5-port GE SPA (SPA-5X1GE) that is installed in a SIP-600, replace the SPA-5X1GE with another card, and then enter the **no shutdown** interface configuration command on the interface at the same location (G9/1/1) on the new card. In this situation, the prefix for the interface (G9/1/1) is not advertised.

Possible Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCsj53361

  Symptoms: IS-IS adjacencies may flap after a stateful switchover (SSO) has occurred.

  Conditions: This symptom is observed when there are large number of adjacencies (for example, 16) and when the IS-IS database is large (for example, one LSP containing 5000 routes).

  Workaround: Increase the hold time that is advertised in the IS-IS Hello (IIH) packet by entering the **router isis nsf advertise holdtime 90** command on the router on which the SSO occurs.

- CSCsj72039

  Symptoms: The prefix of a serial interface that is configured for PPP or HDLC and that functions as a passive interface for IS-IS may not be installed in the local IS-IS database.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)SXF6 but is not release-specific.

  Workaround: Remove and reconfigure the **passive-interface** command.

  First Alternate Workaround: Enter the **clear isis *** command.

  Second Alternate Workaround: Enter any command that triggers the generation of the local IS-IS database.

- CSCsj83306

  Symptoms: IS-IS prefixes may be missing from the IP routing table and LDP peers may not come up after you have entered the **issu runversion** command.

  Conditions: This symptom is observed on a Cisco 7600 series that has the **nsf cisco** command configured for IS-IS.

  Workaround: Do not configure NSF for IS-IS.

- CSCsk47890

  Symptoms: A router may crash when you enter the **show isis database detail** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB on powerPC based platform such as an RSP720.

  Workaround: There is no workaround.

Miscellaneous

- CSCdz55178

  Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

  Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

  ```
  cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
  0000000001111111111222222222333^ 12345678901234567890123456789012| | PROBLEM
  (Variable Overflowed).
  ```

Workaround: Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- CSCeb21064

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)
  – Media Gateway Control Protocol (MGCP)
  – Signaling protocols H.323, H.254
  – Real-time Transport Protocol (RTP)
  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCec24846

  Symptoms: System accounting is not sent as the first record when sessions are establishing while the system is coming up.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Workaround: There is no workaround.

- CSCek66092

  Symptoms: An IPv6 demultiplexer configuration is rejected over an Ethernet interface when there is an IP address configured on the same interface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(33)SRB or a release later than Release 12.2(31)SB and that is configured for Xconnect.

  Workaround: There is no workaround.

  Further Problem Description: The following example shows a configuration in which the symptom occurs:

  ```
  router(config)#interface FastEthernet5/0
  router(config-if)#ip address 10.10.10.10 255.255.255.0
  router(config-if)#xconnect 192.168.200.200 100 pw-class ipv6_demux
  Incompatible with ip address command on Fa5/0 - command rejected.
  ```

- CSCek66164

  Symptoms: A router may hang briefly and then may crash when you enter any command of the following form:

  show ... | **redirect rcp**:....

  Conditions: This symptom is observed when Remote Copy Protocol (RCP) is used as the transfer protocol.

  Workaround: Use a transfer protocol other than RCP such as TFTP or FTP.

Further Problem Description: RCP requires delivery of the total file size to the remote host before it delivers the file itself. The output of a **show** command is not an actual file on the file system nor is it completely accumulated before the transmission occurs, so the total file size is simply not available in a manner that is compatible with RCP requirements.

- CSCek68890

  Symptoms: Multicast traffic stops on one blade after both blades in a Blade-to-Blade stateful failover configuration are reloaded simultaneously.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when some interfaces are assigned to one IPSec VPN SPA and other interfaces to a second IPSec VPN SPA. The symptom occurs in the following scenario:

  – You reload the first blade.

  – You remove the second blade before the first blade comes back up so that both crypto engines are inactive for some time and all tunnels go down.

  After both crypto engines come back up and all SAs are re-established, multicast traffic only passes through the tunnels that are assigned to the first blade.

  The symptom does not occur when you reload one blade after the other, that is, when you wait until one blade comes back up before you reload the second blade.

  Workaround: To restore proper operation, enter the **hw-module subslot** *slot/subslot* **reload** command.

  Alternate Workaround: To restore proper operation, remove and re-add the tunnel configuration.

- CSCek69576

  Symptoms: The standby Route Switch Processor 720 (RSP720) may become stuck when it reloads after a switchover has occurred. Eventually, the RSP720 resets and boots fine thereafter. When the symptom occurs, the following error messages are generated:

  ```
  %ONLINE-SP-6-TIMER: Module 8, Proc. 0. Failed to bring online because of timer event
  %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded, changing to Simplex
  mode)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCek71534

  Symptoms: A SIP-600 crashes when sending H-VPLS traffic.

  Conditions: This symptom is observed on a Cisco 7600 series when the DA MAC address is in the range from 00.00.00.00.00.00 to 00.00.00.00.00.0F, when a 64-byte packet is sent encapsulated under VPLS, and when CFM continuity check is not configured on the interface of the SIP-600.

  The symptom occurs because CFM is zero but the DA MAC addresses in the range from 00.00.00.00.00.00 to 00.00.00.00.00.0F match the (unconfigured) CFM continuity check.

  Workaround: Enable CFM on the interface of the SIP-600 by entering the **ethernet cfm enable** global configuration command.

- CSCek71816

  Symptoms: An end-to-end ping fails when an ASBR restores a VRF in a multipath configuration with different autonomous systems.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB that functions in an EBGP VPNv4 multipath configuration.

Workaround: There is no workaround.

- CSCek74024

  Symptoms: A router that is configured for AAA may crash because of a bus error and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB or Release 12.2SRB and that has AAA authentication enabled.

  Workaround: There is no workaround.

- CSCek74480

  Symptoms: A router may not receive LDP traps that use SNMP VRF-aware context.

  Conditions: This symptom is observed when SNMP context is associated with a particular VRF and when LDP traps are enabled to use the SNMP context.

  Workaround: Check the syslog messages on the router and not rely on LDP traps.

- CSCek75082

  Symptoms: A router may crash when you unconfigure a T3 controller.

  Conditions: This symptom is observed in the following topology on a Cisco router (router B) when you unconfigure a channel group on another router (router A) while traffic is being processed:

  ```
  Traffic generator<------->router A<-------->router B<------->Traffic generator
  ```

  In this situation, router B crashes. The following sequence of commands on the routers causes router B to crash:

  ```
  router A#conf t
  Enter configuration commands, one per line.  End with CNTL/Z.
  router A(config)#controller T3 7/0
  router A(config-controller)#no t1 1 channel-group 0 timeslots 1-24
  ```

  ```
  router B#conf t
  Enter configuration commands, one per line.  End with CNTL/Z.
  router B(config)#controller T3 7/0
  router B(config-controller)#no t1 1 channel-group 0 timeslots 1-24
  ```

  Workaround: There is no workaround.

- CSCek76105

  Symptoms: When IPv6 multicast traffic is forwarded, the following type of alignment tracebacks may be generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at [memory address] reading 0x34
  %ALIGN-3-TRACE: -Traceback= [stack trace]
  ```

  Conditions: This symptom is observed when a tunnel that carries IPv6 multicast traffic is deleted.

  Workaround: There is no workaround.

- CSCek76878

  Symptoms: In a VRF that is configured for CsC and that uses LDP as the label distribution protocol between a PE and CE router, end-to-end MPLS connectivity breaks after an SSO switchover occurs for the Route Processors. After the switchover has occurred, the PE router fails to reallocate the local MPLS labels for the remote prefixes, preventing LDP from re-advertising the local MPLS labels to the CE routers.

  Conditions: This symptom is observed on a PE router that runs a Cisco IOS software image that integrates the fix for caveat CSCse67910 when all PE routers in the MPLS VPN network are configured with the same Route Distinguisher (RD) for the VRF. A list of the affected releases can

be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse67910. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

For the Cisco 7600 series, the symptom may occur in Release 12.2(33)SRB and Release 12.2(33)SRB1.

Workaround: Do not use LDP label distribution between the PE and CE routers. Rather, use BGP.

First Alternate Workaround: For the VRF, use different RDs on the PE routers in the MPLS VPN network.

Second Alternate Workaround: Enter the **clear ip route vrf** *vrf-name* ***** command for the VRF.

- CSCek78653

  Symptoms: A Point-to-Point Tunneling Protocol (PPTP) session may not be established, and the following error message may be generated:

  ```
  SSS MGR [uid:4]: ERROR - Failed to initialize FM Segment. Could not start Local service
  ```

  Conditions: This symptom is observed on a Cisco router that functions as an LNS and that terminates PPTP sessions that have ISG features applied to them.

  Workaround: Disable the ISG features. If this is not an option, there is no workaround.

- CSCek79390

  Symptoms: Egress traffic may not be forwarded when Traffic Engineering/Fast Reroute (TE-FRR) is configured on the same grouping of 10x1GE ports on an Ethernet Services (ES20) line card or on a SIP-600.

  Conditions: This symptom is observed on a Cisco 7600 series when the protected tunnel and backup tunnel reside on the same data path on the ES20 line card or on the same SIP-600.

  Workaround: There is no workaround.

- CSCsa96972

  Symptoms: A Dbus header error interrupt may occur during a recovery procedure on a DFC3, and the following error message is generated:

  ```
  %EARL_L3_ASIC-DFC5-3-INTR_WARN: EARL L3 ASIC: Non-fatal interrupt Packet Parser block interrupt
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when a recovery procedure occurs because of a transient problem in hardware forwarding.

  Workaround: There is no workaround. However, the error message indicates a harmless (non-fatal) error and does not have any impact on the traffic and proper functioning of the platform.

- CSCsb21941

  Symptoms: A supervisor engine may reset unexpectedly, and the following error messages may be generated:

  ```
  %PFREDUN-SP-7-KPA_WARN: RF KPA messages have not been heard for XXX seconds
  %OIR-SP-3-PWRCYCLE: Card in module 1, is being power-cycled (RF request)
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when "super jumbo" frames (greater than 10,000 bytes) are being used.

  Workaround: There is no workaround. The symptom can be mitigated by ensuring that all NICs on the domain are configured with a frame size that is smaller than 10,000 bytes.

- CSCsb57042

  Symptoms: While running a health monitoring diagnostics test, the supervisor engine may crash because of an illegal memory access and generate a “%SYS-SP-3-OVERRUN” error message.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that run Cisco IOS Release 12.2(18)SXF4 and on a Cisco 7600 series router that runs Cisco IOS Release 12.2(33)SRA3. The symptom may also affect other releases. The symptom occurs when the firmware of the module that is being tested reports more errors than an SCP message can carry, causing the health monitoring test to access unauthorized memory outside the SCP message.

  Workaround Enter the **no diagnostic monitor module** *module-num* **test** *test-id* command for the affected module.

- CSCsb74409

  Symptoms: A router may keep the vty lines busy after finishing a Telnet/Secure Shell (SSH) session from a client. When all vty lines are busy, no more Telnet/SSH sessions to the router are possible.

  Conditions: This symptom is observed on a Cisco router that is configured to allow SSH sessions to other devices.

  Workaround: Clear the SSH sessions that were initiated from the router to other devices.

- CSCsb79306

  Symptoms: Setting the cbeDot1dTpVlanAgingFromGlobal from “false” to “true” may cause the standby supervisor engine to reload unexpectedly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have redundant Supervisor Engine 720 modules that function in SSO mode when the following sequence of events occurs:

  1. Use the CLI to configure a VLAN, for example, VLAN 50:
  2. SNMP creates an entry cbeDot1dTpVlanAgingFromGlobal.50 with the value set to “true”.
  3. Manually set the value for cbeDot1dTpVlanAgingFromGlobal.50 from “true” to “false”.
  4. Use the CLI to delete VLAN 50.
  5. When you initiate a mibwalk for cbeDot1dTpVlanAgingFromGlobal, the entry for VLAN 50 is still present.
  6. Manually set the value for cbeDot1dTpVlanAgingFromGlobal.50 from “false” to “true”.

  This last event causes the standby supervisor engine to reload unexpectedly.

  Workaround: Do not use or limit the use of cbeDot1dTpVlanAgingFromGlobal.

- CSCsb85030

  Symptoms: Packets such as DHCP packets may be dropped, and MAC addresses may not be learned on interfaces even though the interfaces are in the up/up state.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when you first configure and then remove port security.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, manually configure the MAC addresses in the MAC-address table.

  Alternate Workaround: Re-enable and then disable port security once more on the affected ports.

- CSCsc32189

  Symptoms: ISAKMP does not check multiple transform payloads in one proposal, preventing a particular third-party vendor L2TP/IPSec client from using the ESP-3DES-SHA transform set.

Conditions: This symptom is observed when the particular third-party vendor L2TP/IPSec client sends the following proposal and when the Cisco IOS software checks only the first transform set and not the second one.

```
Proposal payload # 1
   Next payload: Proposal (2)
   Length: 92
   Proposal number: 1
   Protocol ID: IPSEC_ESP (3)
   SPI size: 4
   Number of transforms: 2
   SPI: 58CB6150
   Transform payload # 1
      Next payload: Transform (3)
      Length: 40
      Transform number: 1
      Transform ID: 3DES (3)
      SA-Life-Type (1): Seconds (1)
      SA-Life-Duration (2): Duration-Value (3600)
      SA-Life-Type (1): Kilobytes (2)
      SA-Life-Duration (2): Duration-Value (250000)
      Encapsulation-Mode (4): Transport (2)
      Authentication-Algorithm (5): HMAC-MD5 (1)
   Transform payload # 2
      Next payload: NONE (0)
      Length: 40
      Transform number: 2
      Transform ID: 3DES (3)
      SA-Life-Type (1): Seconds (1)
      SA-Life-Duration (2): Duration-Value (3600)
      SA-Life-Type (1): Kilobytes (2)
      SA-Life-Duration (2): Duration-Value (250000)
      Encapsulation-Mode (4): Transport (2)
      Authentication-Algorithm (5): HMAC-SHA (2)
```

Workaround: Do not use the ESP-3DES-SHA transform set. Rather, use the ESP-3DES-MD5 transform set.

- CSCsc59025

  Symptoms: The **udld port disable** command may be missing for an interface after several HA switchovers have occurred, causing UniDirectional Link Detection (UDLD) to be enabled on the interface.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when UDLD is globally enabled but disabled on the interface for which you entered the **udld port disable** command.

  Workaround: There is no workaround. Note that UDLD is disabled by default. When you enter the **udld port disable** command for an interface, you configure “no configuration of UD.”

Further Problem Description: When you configure the **udld port aggressive** command globally, then enter the **udld port disable** command for an individual port, and then the symptom occurs, the **udld port aggressive** command remains enabled on the individual port. A workaround for this situation is to enter the **no udld port aggressive** command on the individual port.

- CSCsc89932

  Symptoms: A switch or router may crash when you enter the **show diagnostic sanity** command.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsd31503

  Symptoms: Some protocol packets such as OSPF, EIGRP, MPLS LDP, BGP, and IS-IS may be dropped at the Route Processor (RP) because SPD classifies them as lower-priority packets.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when there are a number of routing protocols running with a very large topology and when rapid topology changes or changes in link states occur, causing more traffic to be processed by the RP.

  Workaround: Increase the priority of the protocol packets by entering the configuration stated below, in which 0 indicates a lower priority and 7 indicates a higher priority and in which the following levels are used for packet classification:

  – 0-1, indicating that the packet is to be dropped
  – 2-4, indicating that as a last resort the packet is to be dropped
  – 5-7, indicating that the packet should be the last one to be dropped.

  Priority level 5-7 is best suitable for protocol packets.

```
Router(config)#mls qos protocol ospf precedence 6
Marking will work on the packet which comes from untrusted port
Router(config)#mls qos protocol ?
isis
eigrp
ldp
ospf
rip
bgp
ospfv3
bgpv2
ripng
neigh-discover
wlccp
arp
```

```
Router(config)#mls qos protocol eig
Router(config)#mls qos protocol eigrp ?
pass-through  pass-through keyword
police        police keyword
precedence    change ip-precedence (used to map the dscp to cos value)
```

```
Router(config)#mls qos protocol eigrp pr
Router(config)#mls qos protocol eigrp precedence 6
Marking will work on the packet which comes from untrusted port
```

- CSCsd65434

  Symptoms: After a router has received an IGMP leave message for a group on a switchport and a user is still connected to this group while an IGMP general query is sent on the same interface, the group is cleared either immediately or after 10 seconds, and then added again when a join message is received.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when IGMP snooping is enabled.

  Workaround: Configure the DSLAM ports as IGMP snooping ports in a static multicast router configuration by entering the **ip igmp snooping mrouter interface** *type slot/port* command.

  Alternate Workaround: Add the multicast MAC address statically by entering the **mac-address-table static** *mac-addr* **vlan** *vlan-id* **interface** *type slot/port* command.

- CSCsd81407

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)

  – Media Gateway Control Protocol (MGCP)

  – Signaling protocols H.323, H.254

  – Real-time Transport Protocol (RTP)

  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  – Cisco IOS, documented as Cisco bug ID CSCsd85587

  – Cisco IOS XR, documented as Cisco bug ID CSCsg41084

  – Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999

  – Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348

  – Cisco Firewall Service Module (FWSM)

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

- CSCse68138

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)
  – Media Gateway Control Protocol (MGCP)
  – Signaling protocols H.323, H.254
  – Real-time Transport Protocol (RTP)
  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCse95996

  Symptoms: A configlet that is presented to a router via CNS configuration agents or via a NETCONF session may fail.

  Conditions: This symptom is observed with both syntax check turned on and syntax check turned off.

  Workaround: Use the action-on-fail=”continue” attribute when using CNS configuration agents or a NETCONF session.

- CSCsf18752

  Symptoms: GTP SLB does not function. GPRS PDP context create requests are forwarded to the GGSN, but they all go to a singe GGSN instead of being load-balanced over several GGSNs, and GTP IMSI sticky delete notifications are not created. In addition, when GTP SLB-related debugs are enabled, no debug messages are printed.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA5 when both the following conditions are met:

- The **mls ip slb search wildcard rp** is configured on the supervisor engine that functions as an SLB.
- More than one pair of GTP SLB server farms and vservers are configured.

Workaround: Remove **mls ip slb search wildcard rp** command from the supervisor engine.

- CSCsf23115

  Symptoms: After the fan tray has failed, the system can not determine if the fan tray is an original fan (FAN1) or high-speed fan (FAN2).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that hare configured with a Supervisor Engine 720.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur on a Cisco Catalyst 6504-E or Cisco Catalyst 6509 NEB that are configured with an E-FAN.

- CSCsg07525

  Symptoms: Packet loss may occur every 30 seconds over a distributed port channel on a Distributed Forwarding Card (DFC) card because the “TestScratchRegister” that runs every 30 seconds disrupts the normal RAN Backhaul (RBH) calculation.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: Disable the “TestScratchRegister” on the affected DFC by entering the following diagnostic command:

  Router(config)# no diagnostic monitor module <mod#> test TestScratchRegister

- CSCsg09423

  Symptoms: When IPsec SAs flap, traffic loss may occur during the IPsec and IKE rekey.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when there is a large number of IKE and IPsec SAs (that is, more than 2000 IKE SAs and 4000 IPsec SAs) and when RSA signature authentication is configured.

  Workaround: Reduce the number of IKE and IPsec SAs.

- CSCsg16272

  Symptoms: When you perform an OIR for a WS-6748-GE-TX or WS-6724-SFP, the module does not generate a linkDown SNMP trap for a physical wire that is connected to the port.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router. Note that the symptom does not occur for a WS-6704-10GE.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, look into the syslog to find the “%LINK-3UPDOWN” message for the port.

- CSCsg40567

  Symptoms: Malformed SSL packets may cause a router to leak multiple memory blocks.

  Conditions: This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

  Workaround: Disable the **ip http secure server** command.

- CSCsg55315

  Symptoms: Packets may be duplicated or triplicated on interface “gig1/1” of a Supervisor Engine 2, Supervisor Engine 32, or Supervisor Engine 720.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with WAN line cards such as an Enhanced FlexWAN, SIP-200, SIP-400, or SIP-600 when SPAN is enabled and when interface “gig1/1” is used to connect to another platform.

  Workaround: Do not use interface “gig1/1” to connect to another platform. Rather, use another interface.

- CSCsg70474

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)
  – Media Gateway Control Protocol (MGCP)
  – Signaling protocols H.323, H.254
  – Real-time Transport Protocol (RTP)
  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsg79129

  Symptoms: Multicast traffic may not be forwarded on a routed VPLS (R-VPLS) interface that is configured for PIM Sparse Mode (SM).

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-600 on which an RPF interface is configured and occur when egress replication mode is enabled.

  Workaround: Change the multicast replication mode from egress mode to ingress mode by entering the **mls ip multicast replication-mode ingress** command.

- CSCsg92950

  Symptoms: A software-forced reload may occur on a Cisco 7301.

  Conditions: This symptom is observed on a Cisco 7301 that terminates several thousand broadband subscribers. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg98728

  Symptoms: A ping from one CE router to another CE router through an AToM tunnel does not go through properly.

  Conditions: This symptom is observed on a Cisco router when the AToM tunnel runs over two different autonomous systems.

  Workaround: There is no workaround.

- CSCsh22171

  Symptoms: After an MPLS-TE path is rerouted, the Virtual Private LAN Services (VPLS) feature stops decapsulating Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames that are received from a remote PE router. This situation may result in an STP loop.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a PE router in an MPLS network, that has many MPLS-TE tunnels configured, and that has the **l2protocol-tunnel stp** command enabled.

  Workaround: Enter the **no l2protocol-tunnel stp** command.

- CSCsh23176

  Symptoms: A router crashes when you unconfigure RIP.

  Conditions: This symptom is observed on a Cisco router and is more likely to occur when there are many RIP routes configured.

  Workaround: Remove all network statements that are defined under the **router rip** command, wait for all RIP routes to age-out, then remove the **router rip** command.

- CSCsh24450

  Symptoms: A memory leak may occur when tunnels or sessions are created and deleted in quick succession.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SRB, or Release 12.2SXH and that is configured for SNMP.

  Workaround: If a virtual template is used, enter the **no virtual-template snmp** command to prevent the symptom from occurring. If no virtual template is used, there is no workaround.

- CSCsh25976

  Symptoms: There are two symptoms:

  1. The threshold of the fan-fail sensor of the power supply may not be updated correctly, and the following error message may be generated:

     ```
     power-supply incompatible with fan: N/A
     ```

     The value should not be “N/A” but “OK”.

  2. The threshold of the fan-fail sensor of the power supply may get be added when power supply is detected. For example, information about the fan-fail sensor of the power supply may not be shown in the output of the **show environment alarm thresholds power-supply** command.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Initiate a Stateful Switchover (SSO). After the SSO, the symptom no longer occurs.

- CSCsh27931

  Symptoms: A platform may crash when an arithmetic exception crash occurs. Before this situation occurs, the following error message is generated:

  ```
  %COMMON_FIB-SP-4-UNEQUAL: Ratio of unequal path weightings (1 1 40) prevents oce IP
  adj out of GigabitEthernet3/2, <ip addr> from being used.
  ```

  Conditions: This symptom is observed on a Cisco platform that functions in an IS-IS configuration when TE tunnels are shut down.

  Workaround: There is no workaround.

- CSCsh29863

  Symptoms: On an RPR switchover, the new active crashes during bootup diagnostics.

Conditions: This symptom occurs when bad SFPs are plugged into the SFP- capable ports. A bad SFP means an incompatible/unsupported/faulty SFP.

Workaround: Remove the incompatible/unsupported/faulty SFPs from the SFP port(s) and plug in a good one if needed.

- CSCsh30617

  Symptoms: A Cisco router may unexpectedly reload when the Embedded Event Manager (EEM) applet is removed from the configuration or shortly after the EEM applet has been removed.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(10.8)T or a later release and occurs most often when the applet was registered when the router booted. The symptom is not release-specific.

  Workaround: There is no workaround.

- CSCsh33128

  Symptoms: A VRF may not be created correctly. When this situation occurs, associated internal VLANs are not allocated. As a result, when a partial shortcut is installed, the internal partial VLAN is not included in the outgoing interface list (olist).

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router only when VRFs are added in a clean configuration and when hardware switching is enabled.

  Workaround: Disable and re-enable hardware switching.

- CSCsh41459

  Symptoms: A router crashes when you remove and then add back VRFs.

  Conditions: This symptom is observed on a Cisco router that functions as a PE Router in an MPLS VPN network.

  Workaround: There is no workaround.

- CSCsh46565

  Symptoms: When the configuration of the shape average is changed, the rate is not applied, which can be shown in the output of the **show policy interface** command and detected by a traffic analyzer.

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and GE-WAN subinterfaces that are configured with an HQoS (LLQ) output policy when the shape average is changed on all GE-WAN subinterfaces at the same time.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, delete the output policy and then reconfigure it on the GE-WAN subinterfaces.

- CSCsh54380

  Symptoms: On SIP600/ESM20G line cards that are running VPLS/EoMPLS in a highly scaled configuration, stats may be inaccurate when traffic engineering tunnels are configured with Fast Reroute and a failover scenario is encountered.

  Conditions: When a large number of VPLS VCs are configured and if all of these VCs are protected by FRR and traffic is failed over between protected and backup interfaces, the line card may experience a stats problem where the VCs may not be able to account the stats accurately.

  This problem is seen in the following configuration scenarios:

  When one of the traffic engineering tunnel's primary or backup interface is configured on:

  ```
  A port on a SIP-600 or
  A port from 0..19 on  a ESM20G(20x1GE) or
  First port (port 0) of a ESM20G (2x10GE)
  ```

and the other tunnel's interface is configured on:

```
Any port from 10-19 of ESM20G 20x1GE or
Second Port (port 1) of ESM20G 2x10GE
```

Workaround: There is no workaround.

- CSCsh61002

  Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a port-based EoMPLS interface (when Xconnect is configured on the main interface), forwarding stops on another L3 interface.

  Conditions: This symptom is observed on a Cisco 7600 series only when there is a short interval (about 30 seconds) between the **shutdown** and **no shutdown** commands.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the router.

  Further Problem Description: When you enter the **shutdown** command quickly followed by the **no shutdown** command on the port-based EoMPLS interface, a new internal VLAN is used. However, because of a software issue, an EoMPLS flag is set on the old VLAN, causing the router to process all packets that are received on the old VLAN as L2 packets. When a new L3 interface comes up and uses the old VLAN, the datapath fails because the router attempts to process these packets as L2 packets instead of L3 packet.

- CSCsh64335

  Symptoms: A router may crash when you enter the **mkdir** command to create a directory with a length of more than 127 characters and when you query this directory via SNMP.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

  Workaround: There is no workaround.

- CSCsh69420

  Symptoms: Connected routes that are redistributed via IPv6 VPN over MPLS (6VPE) into a VRF in an IPv6 address family for BGP may not be subsequently imported into another VRF.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsh70638

  Symptoms: When a router boots and when bursty traffic occurs, the following error messages may be generated:

  ```
  %ALIGN-SP-STDBY-3-SPURIOUS: Spurious memory access made at 0x72AB2370 reading 0xB8
  %ALIGN-SP-STDBY-3-TRACE_SO:
  -Traceback= (s72033-adventerprisek9_wan_dbg-0-dso-bn.so+0x1AE370) ([42:0]+0x1AE47C)
  ([31:-3]3-dso-b+0x220994) ([41:0]+0x220FB8) ([41:0]+0x221A90) ([41:0]+0x22214C)
  ([41:0] +0x222D6C) ([41:0]+0x2233CC)
  ```

  Conditions: This symptom is observed when bursty IPC traffic occurs while the router boots or during a switchover, typically with heavy configuration data exchanges.

  Workaround: There is no workaround.

- CSCsh72267

  Symptoms: A PVC that is configured on an ATM interface that is configured for cell packing may not receive the MNCP and MCPT parameters from the ATM interface. (MNCP = Maximum cells packed in one MPLS packet; MCPT = Maximum time to wait to pack the cells in one MPLS packet.)

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB but is platform-independent.

Workaround: Do not configure cell packing on the ATM interface. Rather, configure cell packing directly on the PVC.

- CSCsh79194

  Symptoms: Unexpected HSRP debug messages such as the following one may be generated when only a partial debug has been enabled:

  ```
  HSRP: Et0/0 Grp 1 Active: l/Hello rcvd from lower pri Standby router (110/10.0.0.102)
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for HSRP when the **debug** *standby terse* command is enabled.

  Workaround: There is no workaround.

- CSCsh83559

  Symptoms: A Cisco Catalyst 6000 series switch may leak memory in the IP Input task in the Cisco IOS-BASE process. The memory is leaked in a small amount per packet that is process switched over a VRF on the switch. Non-VRF traffic is not affected.

  Conditions: This symptom is seen on a Cisco Catalyst 6000 series switch that is running Cisco IOS Modularity. This can only happen if there are VRFs configured on the switch.

  Workaround: Do not use VRFs.

- CSCsh89826

  Symptoms: When a QoS service policy is applied to a serial interface, the rate that is provided to the default queue may drop to unexpectedly low values.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(31)SRA1 with a SPA-4XCT3/DS0 that in installed in a SIP-200. The following is an example of a configuration in which the symptom occurs:

  ```
  class-map match-all MGCP
    match ip precedence 4
  class-map match-all RTP
    match ip precedence 5

  policy-map TEST1
    class RTP
      priority percent 88
    class MGCP
      bandwidth percent 10

       interface Serial2/0/0/17:0
        ip address 10.1.0.13 255.255.255.252
        encapsulation ppp
        load-interval 30
        service-policy output TEST1
  ```

  In this configuration, when there are eight G.711 calls and an FTP file is sent, the throughput is around 30 Kbps of application data for the FTP file. Considering the output service policy and the fact that the priority class does not consume the bandwidth, this throughput rate is very low. Moreover, after a few minutes of operation, the throughput rate drops to about 2 Kbps even though

the rate that is provided in the priority queue has not changed. When the traffic is removed from the priority queue, the default queue continues to serve traffic at the reduced rate of only a few Kbps even though the full T1 line is now available.

Workaround: Remove the service policy from the interface to enable the data traffic to resume flowing at a normal rate.

- CSCsh97826

  Symptoms: VPNv6 forwarding entries may not be properly installed on an VPNv6 ASBR, and the following error message may be generated:

  ```
  %BGP_MPLS-3-VPN_REWRITE: installing rewrite for [100:2]CC:5::/32 failed: Illegal
  parameter
  ```

  Conditions: This symptom is observed on a Cisco router that functions as an ASBR that has IPv6 enabled on the interface that connects to a remote ASBR when this remote ASBR does not have IPv6 enabled on the peering interface.

  Workaround: Configure the peering interfaces consistently on both ASBRs. Either both ASBRs should have IPv6 enabled, or both ASBRs should have IPv6 disabled on the peering interfaces.

- CSCsh98208

  Symptoms: PIM Snooping causes duplicate multicast packets to be delivered in the network.

  Conditions: This symptom is observed when the shared tree and SPT diverge in a VLAN on a Cisco Catalyst 6500 series switch or Cisco 7600 series router that have PIM Snooping configured. PIM Snooping may suppress the (S,G) RPT-bit prune message that is sent by the receiver from reaching the upstream router in the shared tree, causing a situation in which more than one upstream router forward the multicast traffic by using their respective (S,G)-join state, and, in turn, causing duplicate multicast packet to be delivered to the receivers. This situation lasts only for a brief moment because the PIM-ASSERT mechanism kicks in and stop the extraneous flow. However, this cycle repeats again when the next (*,G) join (S,G) RPT bit prune message is sent by one of the receivers.

  Workaround: Disable PIM Snooping in the VLAN-interface configuration.

  Alternate Workaround: If the command is available in the release that you are running, enter the **no ip pim snooping suppress sgr-prune** command to disable SGR-prune message suppression.

- CSCsh98953

  Symptoms: When a PE router that is configured for L2TPv3 receives a Start-Control-Connection-Request (SCCRQ) message from a peer PE router and is unable to locate authorization information for this peer PE router, the PE router may respond with a S top-Control-Connection-Notification (StopCCN) message, and a memory leak may occur.

  Conditions: This symptom is observed when there is a misconfiguration or when the peer PE router sends the SCCRQ message before you have finished entering the Xconnect configuration on the PE router.

  Workaround: There is no workaround.

- CSCsi11257

  Symptoms: After an SSO switchover has occurred, the following error message is generated on the newly active supervisor engine:

  ```
  %SFF8472-3-READ_ERROR: Gi3/24: Error reading DOM data from transceiver
  ```

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

  Workaround: There is no workaround. However, note that the error message is false and can be ignored.

- CSCsi29423

  Symptoms: A ping may not go through an Ethernet Services (ES20) line card when packet verification is enabled.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when packets are corrupted at the tail part.

  Workaround: There is no workaround.

- CSCsi32655

  Symptoms: The running configuration of a Content Switching Module may be unexpectedly cleared. The CSM still appears to work fine, but the configuration cannot be accessed, edited, or updated.

  Conditions: This symptom is observed on a Cisco 6500 series switch and Cisco 7600 series router when you enter the **module csg** *slot-number* command in which the *slot-number* argument represents the module number of a configured CSM.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reboot the platform without saving the configuration to restore the running configuration.

- CSCsi40628

  Symptoms: A Cisco Group Management Protocol (CGMP) packet that is caught by Remote SPAN (RSPAN) may end up in a Layer 2 loop, being sent back and forth continuously between two platforms. When this situation occurs, the CPU usage on the supervisor engine may become very high, and a spanning tree loop may occur.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when the following conditions are present:

  – There are at least two RSPAN VLANS configured (for example, VLAN x and VLAN y).

  – The RSPAN source for one RSPAN VLAN (VLAN x) is on a different platform than the RSPAN source for the other RPSAN VLAN (VLAN y).

  – One of the platforms on which an RSPAN VLAN source is configured receives a CGMP packet.

  Workaround: Configure a monitor filter to enable all VLANs except RSPAN VLANs. For example, if the RSPAN VLANs are VLAN 600 and VLAN 601, configure the following:

  ```
  monitor session 1 filter vlan 1 - 599 , 602 - 4094
  ```

  First Alternate Workaround: Remove the SPAN source from one of the two platforms.

  Second Alternate Workaround: Remove the CGMP configuration.

- CSCsi41791

  Symptoms: A buffer memory leak may cause a SPA-IPSEC-2G to crash. When this situation occurs, the following error messages are generated in the logs:

  ```
  SPA_IPSEC-3-PWRCYCLE: SPA (<slot/subslot>) is being power-cycled (Module not
  responding to keep-alive polling)
  SPA_OIR-3-RECOVERY_RELOAD: subslot <slot/subslot>: Attempting recovery by reloading
  SPA
  ACE-6-INFO: SPA-IPSEC-2G[<slot/subslot>]: Crypto Engine X going DOWN
  ```

  Conditions: This symptom is observed rarely on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when GRE fragments are reassembled by the SPA-IPSEC-2G and when the length of the IP packet after GRE decapsulation is more than 9126 bytes.

  Workaround: To prevent the symptom from occurring, proactively reload the SPA-IPSEC-2G outside of business hours by entering the **hw-module subslot** *slot*/*subslot* **reload** command.

- CSCsi42517

  Symptoms: A Cisco 7600 series may crash when Cisco IOS-SLB receives a GSN backup update packet.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an HSRP configuration and that has virtual servers configured when none of the virtual servers has the **service gtp-inspect** command enabled.

  Workaround: There is no workaround because the situation that is described in the Conditions is a misconfiguration.

- CSCsi45840

  Symptoms: ARP requests to an HSRP virtual IP address may fail.

  Conditions: This symptom is observed when the same HSRP IP address is used alternatively on different interfaces, and when one of these interfaces has the **switchport** command configured and unconfigured several times.

  Workaround: Remove the HSRP configuration from the interface before you enter the **switchport** command on the interface.

- CSCsi46861

  Symptoms: The RP of a Cisco 7600 series that is configured for MPLS may generate the following error message and traceback:

  ```
  %MFI-3-REDISTMGR: Redistribution Manager: stats_updates - not in use 3
  - Traceback= 406298C4 40629E08 428DEA78 40F3D13C 4180B62C 418083C0 41E91C18 426C61E0
  41E9D140 40A475B4 419E032C 419E0758 4155B838 4155B824
  ```

  Conditions: This symptom is observed rarely after a switchover has occurred.

  Workaround: There is no workaround. However, the functionality of the router is not impacted.

- CSCsi49520

  Symptoms: A medium buffer leak may occur on an MSFC.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that function as a PE router after an SSO has occurred.

  Workaround: There is no workaround.

- CSCsi49953

  Symptoms: One of the CPUs of a SIP-200 may crash continuously when an LFI bundle is present on the SIP-200.

  Conditions: This symptom is observed on Cisco 7600 series routers that are connected back-to-back when no traffic is processed.

  Workaround: There is no workaround.

- CSCsi52209

  Symptoms: A SIP-600 may crash, and the following error message may be generated:

  ```
  %PXF-DFC1-2-FAULT: T0 OHB Exception: SLIP FIFO full WARNING: PXF Exception:
  mac_xid=0x40000
  *** PXF OHB SLIP FIFO Full %SIP600-DFC1-2-UNRECOVERABLE_FAILURE: SIP-600
  Unrecoverable Failure
  ```

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

  Workaround: There is no workaround.

- CSCsi53644

  Symptoms: After an SSO switchover has occurred, when the standby RP enters the hot standby mode, an MLS CEF entry may be missing for a loopback interface on the newly active RP. The RP that was the active RP before the SSO switchover occurred and that is now the RP in the hot standby mode still has the correct MLS CEF entry.

  Conditions: This symptom is observed on a Cisco router when you enter the **redundancy force-switchover** to initiate an SSO switchover.

  Workaround: For the loopback interface that does not have the MLS CEF entry on the newly active RP, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command to repopulate the MLS CEF entry.

- CSCsi56504

  Symptoms: The output of the **show atm pvc** command does not show proper QoS values. Even when QoS is configured for VBR or ABR, the command output always shows UBR.

  Conditions: This symptom is observed on a Cisco router that is configured with a PVC bundle.

  Workaround: There is no workaround.

- CSCsi56793

  Symptoms: The following error messages and tracebacks may be generated on the console of a WAN line card that is installed in a Distributed Forwarding Cards (DFC):

  ```
  DFC1: PXF clients started, forwarding code operationalUnexpected call:
  c6k_pwr_get_system_power_sufficiency()
  DFC1: -Traceback= 4057162C 40B4770C 40B454A0 401EF56C 401EF5FC 4011760C 40117838
  401F089C 401F0888Unexpected call: sp_power_mgmt_led()
  DFC1: -Traceback= 40571F08 40B4771C 40B454A0 401EF56C 401EF5FC 4011760C 40117838
  401F089C 401F0888Unexpected call: sp_module_led()
  DFC1: -Traceback= 40571F30 40B47808 40B454A0 401EF56C 401EF5FC 4011760C 40117838
  401F089C 401F0888Unexpected call: sp_system_led()
  DFC1: -Traceback= 40571F84 40B4783C 40B454A0 401EF56C 401EF5FC 4011760C 40117838
  401F089C 401F0888
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when the WAN line card boots.

  Workaround: There is no workaround. However, the error messages and tracebacks are harmless and do not impact the functionality of the router.

- CSCsi59267

  Symptoms: After you have reloaded the router, the Control Plane Policing feature does not function.

  Conditions: This symptom is observed on a Cisco 7600 series that has a policy attached to the control plane.

  Workaround: Remove the policy from the control plane and then re-attach it.

  Further Problem Description: When the symptom occurs, the output of the **show mls qos ip** command does not show that the control plane is programmed. Actually, there is no entry for the control plane policy in the output.

- CSCsi60004

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)

  – Media Gateway Control Protocol (MGCP)

  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsi65363

  Symptoms: When you attempt to bring up a T1 link on a PA-MC-2T3 port adapter, the serial interface may remain in up/down state. In this situation, Layer 1 is fine.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that have a FlexWAN in which a PA-MC-2T3 port adapter is installed when PPP, HDCL, or Frame Relay encapsulation is used on the serial interface.

  Workaround: Move the T1 link to another slot of the PA-MC-2T3 port adapter or move the PA-MC-2T3 port adapter to another slot of the FlexWAN. Also, when you tear down the T1 channel-group configuration and reconfigure, the symptom may disappear.

  Further Problem Description: Note that when you configure a local loopback interface on the controller of the T1 (or T3) interface and configure HDLC encapsulation on the serial interface, you can bring up the serial interface.

- CSCsi65916

  Symptoms: A large I/O memory leak may occur on a Supervisor Engine 720 that functions in a Cisco Mobile Exchange environment.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when MWAM or SAMI processors are configured for remote logging and when many system messages from the MWAM or SAMI processors are directed to the supervisor engine.

  Workaround: There is no workaround.

- CSCsi69350

  Symptoms: The RP on the standby supervisor engine may crash during the boot process when you upgrade the ROMmon of the RP on the standby supervisor from the active supervisor engine.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have redundant Supervisor Engine 720 modules that function in RPR mode when you upgrade the ROMmon of the RP on the standby supervisor from the active supervisor engine by entering the **upgrade rom-monitor slot** *slot-num* **rp file** *filename* command.

  Workaround: There is no workaround.

- CSCsi70356

  Symptoms: You may enter an image name length (including the prefix) of greater than or equal to 64 characters but less than the prefix length plus 64 characters in the **issu loadversion** *active-slot active-image standby-slot standby-image* command. The router should prevent ISSU from occurring in this situation, but it does not. As a result, the standby RP is reloaded but does not enter SSO mode, causing the ISSU software upgrade to fail.

Conditions: This symptom is observed only when Cisco IOS software image is renamed on the file system in such a way that the image name (including the prefix) is larger than or equal to 64 characters but less than the prefix length plus 64 characters.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **write memory** command followed by the **redundancy reload peer** command to recover the standby RP.

- CSCsi72323

  Symptoms: The 10-Mbps and 100-Mbps links of a 20-port Ethernet Services line card (7600-ES20-GE) may go down.

  Conditions: This symptom is observed on a Cisco 7600 series after you have reloaded the platform while diagnostics are enabled. Ports with a copper SFP that are configured for 10-Mbps and 100-Mbps go down after the platform boots. The symptom does not occur when diagnostics are disabled.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ports.

- CSCsi74605

  Symptoms: The state of VPLS VCs on a Virtual Forwarding Instance (VFI) may remain up even though the state of the interface VLAN is down, which can be seen in the output of the **show mpls l2transport vc** command. In this situation, there is no corresponding L2 circuit in the up state, which can be seen in the output of the **show interface vlan** command.

  Conditions: This symptom is observed an a Cisco 7600 series that has the **xconnect vfi** command configured for VPLS services under an interface VLAN.

  Workaround: There is no workaround to prevent the symptom from occurring. You must ensure that the VPLS VCs and the interface VLAN are in the up state so that traffic can flow.

- CSCsi75566

  Symptoms: Packets may be dropped on a Fast ReRouting (FRR) backup tunnel.

  Conditions: This symptom is observed on a Cisco router when the primary MPLS TE tunnel is protected by a backup tunnel and when the protected tunnel interface is a subinterface that goes administratively down.

  Workaround: There is no workaround.

  Further Problem Description: Process-switched traffic (such as traffic that originates from the router itself or a ping with a record option) is not impacted.

- CSCsi91324

  Symptoms: Immediately after an interface in the outgoing interface list (OIL) goes down, a brief period of packet loss to interfaces in the OIL may occur. During this brief period, the Multicast MultiLayer Switching (MMLS) hardware entry on the Distributed Forwarding Card (DFC) is deleted and re-installed.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB in the following configuration:

  – Source Specific Multicast (SSM) is enabled.
  – IGMP Snooping is disabled.
  – A static join is configured on the interfaces.
  – The **mls ip multicast consistency-check** command is enabled.

  Workaround: Disable the **mls ip multicast consistency-check** command.

Further Problem Description: When the **mls ip multicast consistency-check** command is enabled, a linkdown event is detected ahead of multicast route updates, and the inconsistency is corrected. This situation results in a hardware entry reset.

- CSCsi93683

  Symptoms: In Cisco IOS software that is running the Bidirectional Forwarding Detection (BFD) protocol, attempts to remove BFD sessions may fail.

  Conditions: The symptom has been observed after the maximum number of supported sessions has been configured. The maximum number is 128 in most but not all releases.

  Workaround: There is no workaround.

- CSCsi95192

  Symptoms: When a Cisco 7600 series crashes, the crashinfo file that is collected may not be complete, affecting the debug information.

  Conditions: This symptom is observed on a Cisco 7600 that has a Route Switch Processor 720 (RSP 720).

  Workaround: Configure a larger crashinfo file size for the RSP 720, as in the following example:

  ```
  exception crashinfo buffersize 80
  ```

- CSCsi96685

  Symptoms: A router that functions as an LNS and ISG may crash at the “chunk free” function when a call is being freed or disconnected.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB and is caused by a race condition. The symptom may not be release-specific.

  Workaround: There is no workaround.

  Further Problem Description: The following configuration suggestions may reduce the likelihood that the race condition occurs:

  – Change the following in all VPDN groups:

    ```
    l2tp tunnel receive-window 10000
    l2tp tunnel timeout hello 180
    ```

  – Do not configure the router for SSO. Rather, configure RPR+.

  – If the following command is not required, remove it from the configuration:

    ```
    aaa authentication ppp user-auth if-needed group csm-auth-acct
    ```

  – Configure the *seconds* argument of the **radius-server timeout** *seconds* command to 5 seconds.

  – Configure the *tries* argument of the **radius-server dead-criteria tries** *tries* command to its maximum value. (If there is only one RADIUS server, you need to ensure that it is not going to be marked dead.)

  – Periodic accounting every 90 minutes may be too aggressive and may need to be changed.

  – Set the *time-limit* argument of the **ppp timeout ncp** *time-limit* command under the virtual template to 45 seconds.

- CSCsi98993

  Symptoms: When you attempt an FPD downgrade on an ATM SPA, an error message similar to the following may be generated, and the SPA may be disabled:

  ```
  %FPD_MGMT-3-FPD_UPGRADE_FAILED: I/O FPGA (FPD ID=1) image upgrade for SPA- 4XOC3-ATM
  card in subslot 3/0 has FAILED.
  ```

Conditions: This symptom is observed on a Cisco 7600 series that is configured with an SPA-2XOC3-ATM, SPA-4XOC3-ATM, SPA-1XOC12-ATM, or SPA-1XOC48-ATM.

With an SPA-2XOC3-ATM, SPA-4XOC3-ATM or SPA-1XOC12-ATM, the symptom occurs when the hardware version is newer than version 1.0 and when the downgrade FPD image version is older than version 1.26.

With an SPA-1XOC48-ATM, the symptom occurs when the hardware version is newer than version 1.0 and when the downgrade FPD image version is older than version 0.15.

Workaround: There is no workaround to downgrade the FPD for these cases, but the symptom does not actually corrupt the FPD image on the SPA. You can bring up SPA again by entering the **hw-module subslot** *slot-number/subslot -number* **reload** command.

- CSCsi99825

  Symptoms: An SNMP Engine may crash at the “idb_get_swsb” and “mpls_if_get_gen_stats” functions.

  Conditions: This symptom is observed on a Cisco 7613 that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: Disable this SNMP query from the CU.

- CSCsj00449

  Symptoms: An output queuing policy may be rejected by an EFP on an Ethernet Services (ES20) line card when the LLQ policer rate in the policy is more than 1 Gbps, and a warning message is generated that states that rates greater than 1 Gbps are not supported. However, a much higher policer rate is supported.

  Conditions: This symptom is observed on a Cisco 7600 series when you apply a relevant service policy to a service instance.

  Workaround: There is no workaround.

- CSCsj01357

  Symptoms: Two network clock sources may serve the same backplane on a Cisco 7600 series, causing a loop that results in an incorrect clock time.

  Conditions: This symptom is observed when network clocking is configured and distributed to the line cards (that support network clocking) through the backplane and when the active and standby supervisor engines synchronize to the same back plane reference. The symptom occurs after multiple switchovers when the clock sources are configured and unconfigured.

  Workaround: No workaround.

- CSCsj01891

  Symptoms: When a diagnostic test (that is, a “scratch register test”) fails, a memory error may occur, and the Management Processor (NMP) may crash.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: Disable the diagnostic test by entering the **diagnostic monitor** *module num* **test** *test-id* command.

  Further Problem Description: A scratch register test failure is a very rare failure that most likely indicates a hardware issue with one of the devices on the line card.

- CSCsj01961

  Symptoms: A router may not boot and may generate an “INSUFFICIENT MEMORY” error message.

Conditions: This symptom is observed on a Cisco 7600 series that has an RSP720 when the ifIndex table is corrupt, preventing SNMP from initializing because SNMP attempts to use the ifIndex table from NVRAM.

Workaround: There is no workaround

- CSCsj03474

  Symptoms: After you have changed a CEM group on a T1/E1 port of a SPA-24CHT1-CE-ATM from unframed to framed, traffic stops flowing through the port.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Workaround: Reload the SPA.

- CSCsj07328

  Symptoms: When IP interworking is configured on the first port of a PFC that is installed in slot 1 of the chassis of a PE router, an ARP request from a CE router may be not resolved.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a PE router.

  Workaround: Obtain the proxy MAC address on the PE router by entering the **show platform software xconnect mac-addr** command. On the CE router, use this MAC address as the destination IP address by using a static MAC address configuration.

  Alternate workaround: Move the interface to another port of the PFC in slot 1 of the chassis, or move the PFC to another slot.

- CSCsj07616

  Symptoms: A Route Switch Processor 720 (RSP 720) may generate the following error message and incorrect traceback while a CPU hog condition is being debugged:

  ```
  %CPU_MONITOR-SP-2-NOT_RUNNING_TB: CPU_MONITOR
  traceback:
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when a failure occurs because of a CPU hog that is caused by a process or interrupt.

  Workaround: There is no workaround.

- CSCsj08843

  Symptoms: Line card information may be missing on the RP, and the following error message may be generated:

  ```
  %XDR-DFC9-6-XDRLCDISABLEREQUEST: Client XDR Interrupt Priority Client requested to
  be disabled. Due to XDR Keepalive Timeout
  ```

  Conditions: This symptom is observed on a Cisco router after you have repeatedly performed an OIR of the line card.

  Workaround: There is no workaround.

- CSCsj09790

  Symptoms: A line card crash and the following error messages may be generated:

  ```
  %INTR_MGR-DFC4-3-INTR: Queueing Engine (Blackwater) [0]: IPM Invalid packet ID
  %ESM20-DFC4-3-UNEXPECTED_GLOBAL_INT: Unexpected Global Interrupt:
  Blackwater_0/Icewater_0 Error %DFCWLC-DFC4-2-UNRECOVERABLE_FAILURE: DFC WAN Line
  Card Unrecoverable Failure for Device: Queueing Engine (Blackwater)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB in a SPAN configuration.

  Workaround: Remove the SPAN configuration.

- CSCsj10744

  Symptoms: The input queue for an interface on a SPA-2X1GE that is installed in a SIP-400 module may become wedged. When this situation occurs, the output of a **show** command shows the following information:

  ```
  GigabitEthernet2/2/1 is up, line protocol is up Input queue: 1076/75/61420/0
  (size/max/drops/flushes); Total output drops: 0
  ```

  The packets cannot be removed from the input queue. The packets remain in the input queue even after you have shut down and brought the interface.

  Conditions: This symptom is observed on a Catalyst 6000 series switch and Cisco 7600 series router that are configured for Web Cache Communications Protocol (WCCP), functioning in conjunction with the hardware NetFlow table.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs only on SPA interfaces, and only when NetFlow entries fail to install. Typically, this situation occurs when the NetFlow table is full. Each failed installation creates one entry in the input queue.

- CSCsj12034

  Symptoms: When you enter the **fabric switching-mode allow dcef-only** command on the active supervisor engine and you confirm that the standby supervisor engine must reload to change to dCEF mode, the standby supervisor engine does reload, comes up, but then enters ROMmon mode, and cannot be booted from ROMmon mode either.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions in SSO redundancy mode.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur in Release 12.2(33)SRA.

- CSCsj13343

  Symptoms: A router may crash when a SSO switchover occurs while you perform an OIR.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an Xconnect configuration with 16,000 EVCs.

  Workaround: There is no workaround.

- CSCsj15638

  Symptoms: The standby supervisor engine may crash during bootup in SSO mode.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR when a large number of CEM circuits are configured with a CEM class is attached to them.

  Workaround: There is no workaround.

- CSCsj19194

  Symptoms: A Cisco 7600 series may crash when there are many link up/down flaps on a physical interface that has many VLANs associated.

  Conditions: This symptom is observed with the following large numbers of VLANs:

  – Number of existing VLANs: 4023

  – Number of existing VTP VLANs: 1005

  – Number of existing extended VLANs: 3018

  Workaround: There is no workaround.

Further Problem Description: Dequeueing of link up/down events that is handled by the “mls-gc” process occurs at a slower rate than the enqueueing. When the link flaps continue, memory that is allocated for each event is not freed in time, eventually causing the router to run out of memory and crash.

- CSCsj22790

  Symptoms: The power supply remains off when you perform an ISSU upgrade.

  Conditions: This symptom is observed on a Cisco 7600 series only when redundancy mode RPR is configured.

  Workaround: When redundancy mode RPR is configured, do not use ISSU. Rather, use FSU.

- CSCsj27140

  Symptoms: After you have performed an OIR, traffic may not flow on some interfaces of a SPA that is installed in a SIP-400.

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

  Possible Workaround: Reload the SPA or the SIP-400.

- CSCsj27414

  Symptoms: In a Service Control Engine (SCE) over MPLS configuration, when an input policy is configured to set the MPLS imposition experimental (EXP) bit and when the remote peer calls for AToM VC Type 4, the MPLS EXP bit imposition value is not copied into the Type 4 tag priority bits.

  Conditions: This symptom is observed on a Cisco 7600 series that has an Ethernet Services (ES20) line card when the remote peer (100.1.1.5 in the example below) is a Type 4 device. The ES20 line card does not copy the MPLS EXP bit imposition value into the inserted Type 4 dot1q tag. The symptom occurs in the following example configuration:

```
### sample configuration ###
class-map match-all MATCHANY
  match any
!
policy-map SETEXP
  class MATCHANY
   set mpls experimental imposition 5
!


!
interface GigabitEthernet2/0/0
 no ip address
 mls qos trust dscp
 service instance 1 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  service-policy input SETEXP
  xconnect 100.1.1.5 100 encapsulation mpls
 !
```

  Workaround: There is no workaround.

- CSCsj27811

  Symptoms: A supervisor engine may crash because of a low memory condition that is caused by an Ethernet Out of Band Channel (EOBC) buffer leak and a big buffer leak.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that runs Cisco IOS Release 12.2(18)SXF9 but could also affect a Cisco 7600 series router that runs Release 12.2SR.

  Workaround: There is no workaround.

- CSCsj28277

  Symptoms: A platform ignores an IGMPv3 report when the first group address in the packet is 224.0.0.X. This situation causes other groups in the same packet to be ignored too, and, in turn, prevents a multicast stream from being forwarded.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that has a Supervisor Engine 720 that runs Cisco IOS Release 12.(18)SXF8 but may also affect a Cisco 7600 series that runs Release 12.2SR.

  Workaround: Ensure that the end station that sends the IGMPv3 report lists any 224.0.0.x groups as the last group addresses in the report. If this is not an option, there is no workaround.

  Further Problem Description: The following is a sequence of a group record that fails:

```
Internet Group Management Protocol
    IGMP Version: 3
    Type: Membership Report (0x22)
    Header checksum: 0x09b0 [correct]
    Num Group Records: 2
    Group Record : 224.0.0.9  Mode Is Exclude
        Record Type: Mode Is Exclude (2)
        Aux Data Len: 0
        Num Src: 0
        Multicast Address: 224.0.0.9 (224.0.0.9)
    Group Record : 239.255.0.68  Mode Is Exclude
        Record Type: Mode Is Exclude (2)
        Aux Data Len: 0
        Num Src: 0
        Multicast Address: XXX.255.0.68 (xxx.255.0.68)
```

- CSCsj29413

  Symptoms: A router may not boot successfully because configurations for the ifIndex persistence are not read correctly from NVRAM.

  Conditions: This symptom is observed on a cisco 7600 series that has an RSP 720 that runs Cisco IOS Release 12.2SR and occurs only when the SNMP persistence database configuration is enabled.

  Workaround: The main reason for boot failure is the SNMP ifindex file corruption. This file is stored in NVRAM. The following sequence of commands clear the file from NVRAM and enables the RSP 720 to boot:

```
rommon 2> priv
```

```
rommon 3 > fill
Enter in hex the start address [0xfec00e00]:
Enter in hex the test size or length in bytes [0x100]:  0xeff200 Enter in hex the
pattern to be written [0x0]:  0xaaaaaaaa Enter the operation size "l"ong, "w"ord, or
"b"yte  [b]:  l
```

```
*** Data TLB Error Exception ***
PC = 0xfff98554, Vector = 0x1400, SP = 0x4013d24
Rommon 5>  b disk0:
```

- CSCsj29960

  Symptoms: After an SSO switchover has occurred, it may be impossible to connect to a CEoP SPA.

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

  Workaround: Reset the CEoP SPA.

- CSCsj30829

  Symptoms: When a Cisco 7600 series with a SIP-400 in which a POS SPA is installed is configured for Frame Relay encapsulation, traffic that is processed through Low Latency Queueing (LLQ) may be dropped because of a corrupt DLCI number.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB. The following is an example of a policy-map configuration in which the symptom occurs:

  ```
  class-map match-any IP_VOICE_OUT
    match ip dscp ef


  policy-map POLICY_V5
    class IP_VOICE_OUT
     police cir percent 5
      priority
    class class-default
  ```

  Workaround: Configure class-based weighted fair queueing (CBWFQ) with a police statement, as in the following example:

  ```
  policy-map POLICY_V5
    class IP_VOICE_OUT
     police cir percent 5
      bandwidth percent 5
  ```

  Alternate Workaround: Do not use Frame Relay encapsulation. Rather, use HDLC or PPP encapsulation.

- CSCsj31272

  Symptoms: The following debug messages are generated on the console when you configure Xconnect on a module, even when debugs are not enabled:

  ```
  Skipping setup switching for Ethernet interface <name>
    List Enqueue Failed Add to Hotstandby Q
    List Remove Failed Remove from HeldQ
    deallocate segment <num>
    unprovision switch <num>
  ```

  Conditions: This symptom is observed on a Cisco router after an RP switchover has occurred.

  Workaround: There is no workaround.

- CSCsj33346

  Symptoms: A Cisco 7600 series switching processor (SP) may fail to generate a crashinfo file.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when **exception crashinfo** global configuration commands are executed and when the configuration is saved.

Workaround: Do not add a configuration with **exception crashinfo** global configuration commands.

- CSCsj35776

  Symptoms: Some PVCs may remain inactive after an ATM SPA has been reloaded.

  Conditions: This symptom is observed on a Cisco 7600 series when the ATM SPA is configured with OAM-managed PVCs and when these are many PVCs.

  Workaround: Increase the *down-count* and *retry-frequency* OAM management arguments for the affected PVCs by using the **oam retry** command.

  Alternate workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface with the affected PVCs.

- CSCsj37071

  Symptoms: All E1 interfaces on a PA-MC-E3 port adapter may flap continuously even after the traffic has been stopped.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that have a PA-MC-E3 port adapter when you configure 16 or 128 channel groups on each time slot (that is, time slots 1-31) and then generate traffic just above line rate traffic through all the channel groups. Note that the symptom is not platform-specific.

  Workaround: Stop the traffic and reset the E3 controller of the PA-MC-E3 port adapter.

- CSCsj37398

  Symptoms: A CoS value may be incorrectly changed.

  Conditions: This symptom is observed on a cisco 7600 series when a register is not initialized properly, causing traffic to be marked to a random CoS value.

  Workaround: There is no workaround.

- CSCsj38436

  Symptoms: A Cisco 7600 series may generate the following error message and traceback:

  ```
  %ICC-2-NOMEM: No memory available for asynchronous request
  -Traceback= 4062ACB8 4062B1FC 423318EC 42331F6C 42332160 421DDCF4 421EB12C 422BE264
  422BE634 412DAB40 412FC674 412DB7B8 412DC12C 412B7EB4 412B8038 412B7CAC
  ```

  After the error message and traceback have been generated, the CPU usage increases, and eventually the router crashes.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1 when you de-activate and re-activate SLB-GTP and SLB-FWLB and run traffic for GSM users through SLB-GTP and SLB-FWLB for several hours.

  Workaround: There is no workaround.

- CSCsj38796

  Symptoms: When you boot the platform, the supervisor engine and a line card may crash during the “label_entry_get_inlabel” process.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured for MPLS.

  Workaround: There is no workaround.

- CSCsj43677

  Symptoms: When you remove the standby supervisor engine, the active supervisor engine may crash and reload.

  Conditions: This symptom is observed on a Cisco 7600 series that has dual Supervisor Engine 720 modules that are configured for SSO.

  Workaround: There is no workaround.

- CSCsj46613

  Symptoms: When the standby supervisor engine is reset, a memory leak may occur on the active supervisor engine.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR in a redundant configuration.

  Workaround: There is no workaround.

- CSCsj46965

  Symptoms: Diagnostic scheduling may not be effective after forced switchover.

  Conditions: This symptom is observed on a Cisco 7600 series that has a 1-port OC-12c/STM-4c ATM SPA (SPA-1XOC12-ATM).

  Workaround: There is no workaround.

- CSCsj47546

  Symptoms: When an interface of a POS SPA detects a Payload Label Mismatch-Path (PLM-P), it may generate a Remote Defect Indication-Path (RDI-P) to the far end. This is improper behavior.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SPA-2XOC3-POS, SPA-4XOC3-POS, SPA-1XOC12-POS, or SPA-1XOC48POS/RPR.

  Workaround: There is no workaround.

  Further Problem Description: Per the Bellcore GR-253 standard, RDI-P must not be transmitted to the far end when the interface detects PLM-P.

- CSCsj47551

  Symptoms: When you enter the **interface range** command, the standby supervisor engine may reset unexpectedly.

  Conditions: This symptom is observed on a Cisco router that is configured for high availability (HA).

  Workaround: There is no workaround.

- CSCsj55688

  Symptoms: A WAN line card may fail to boot when the following error condition occurs:

  ```
  %ETSEC-5-LATECOLL: PQ3/FE(0), Late collision
  ```

  The late collision error is result of a delay in the collision signal that is received by the MAC address of the line card.

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

  Workaround: There is no workaround.

- CSCsj55865

  Symptoms: When you shut down an interface that is protected by FRR, a client API error may occur, and the following error message and a traceback may be generated:

  ```
  %LSD_CLIENT-3-CLIENTAPI: Client API error
  ```

  Conditions: This symptom is observed when an MLPS traffic engineering (TE) backup path is configured on the interface and when MPLS TE tunnels are not globally configured and enabled.

  Workaround: Configure and enable MPLS TE tunnels globally.

- CSCsj58287

  Symptoms: A SPA services carrier card (7600-SSC-400) may crash after a reload.

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

  Workaround: There is no workaround.

- CSCsj58538

  Symptoms: Line protocol flaps may occur on a router after an SSO switchover. This situation causes traffic loss for a short time until the interfaces come back up and traffic is restored.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a highly scaled environment and that has many interfaces are configured.

  Workaround: There is no workaround.

- CSCsj59997

  Symptoms: When a VTI is created, traffic that is generated by the Route Processor such as a ping and routing protocol hello messages may be dropped at the interface level.

  The output of the **show interface tunnel** *number* command shows the output drops:

  ```
  router#sh int tu 1 | i drop
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 26
  router#
  ```

  The output of the **show ip traffic** command shows that the number of “encapsulation failed” increases:

  ```
  router#sh ip traff | i Drop
    Drop:  26 encapsulation failed, 0 unresolved, 0 no adjacency
  router#
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a SPA-IPSEC-2G when both of the following conditions are present:

  – The tunnel destination is not directly connected to the switch or router.

  – Proxy ARP is not enabled on the next-hop router to the tunnel destination.

  Workaround: Create a dummy ARP entry for each VTI tunnel destination, as in the following example:

  ```
  arp <tunnel destination ip> 1111.1111.1111 arpa.
  ```

- CSCsj60582

  Symptoms: 802.1q tags may be misordered when Xconnect is configured on an service instance that is configured on an Ethernet Services (ES20) line card. When this situation occurs, the misordered 802.1q tags are sent to the MPLS core and the remote EoMPLS peer.

Conditions: This symptom is observed on a Cisco 7600 series when all of the following conditions are present:

- The **rewrite ingress tag** command with a “push dot1q” tag manipulation is configured on the interface. Both single and double tags are affected.
- The **xconnect** *ip-address* **encap mpls** is configured on the service instance.
- The remote peer has negotiated VC Type 4 (Ethernet+VLAN) rather than VC Type 5 (Ethernet only).

Workaround: There is no workaround.

Further Problem Description: The following is an example of an interface configuration with a “push dot1q” tag manipulation:

```
interface GigabitEthernet2/0/0
 no ip address
 no mls qos trust
 no cdp enable
 spanning-tree bpdufilter enable
 service instance 100 ethernet
  encapsulation dot1q 100
  rewrite ingress tag push dot1q 105 symmetric
  xconnect 10.1.1.5 100 encapsulation mpls
 !
```

The following is an example of a VC Type 4 (Ethernet+VLAN) peer configuration:

```
router#sh mpls l2 binding
  Destination Address: 10.1.1.5,  VC ID: 100
    Local Label:  21
        Cbit: 0,    VC Type: Eth VLAN,    GroupID: n/a
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
    Remote Label: 18
        Cbit: 0,    VC Type: Eth VLAN,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: None
              CV Type: None
```

- CSCsj64490

  Symptoms: After you have reloaded the router, some ports on an Ethernet Services (ES20) line card may remain in the down/down state.

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

  Workaround: Reload the line card.

- CSCsj65755

  Symptoms: Packet loss may occur, and an “SPI NOT Available” error message may be generated during a rekey.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with an IPSec VPN SPA and occurs under either one of the following conditions:

- when the first rekey after a switchover or revert back occurs.
- when any SA setup occurs during a switchover or revert back.

Workaround: There is no workaround.

- CSCsj67110

  Symptoms: A router may crash or report an error message similar to the following:

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

  This can be seen for a process other than the “draco-oir” process.

  Conditions: This symptom is observed on a Cisco 7600 series when HSRP is configured. The symptom occurs when there is an event that requires the HSRP configuration to be removed, for example, when you perform an OIR of a module while the **module clear-config** command is enabled. The interface with HSRP does not have to be up for the symptom to occur.

  Workaround: Remove the HSRP configuration before you perform an OIR.

  Alternate workaround: Enter the **no module clear-config** command. (The **module clear-config** command is enabled by default. You must enter **no** form of the command to disable it.)

- CSCsj67336

  Symptoms: A Cisco 7600 series may crash when you perform an OIR of a line card such as a SIP-400 or Ethernet Services (ES20) line card that contains an SFP transceiver.

  Conditions: This symptom is observed when the SFP transceiver has DOM capability.

  Workaround: First, remove the SFP transceiver. Then, perform an OIR of the line card.

- CSCsj68502

  Symptoms: A SPA-24CHT1-CE-ATM for which no card type is configured may crash when you configure an out-of-band clock (that is, when you configure a clock master and slave).

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.(33)SRB1.

  Workaround: First, configure the card type for the SPA-24CHT1-CE-ATM. Then, configure an out-of-band clock.

- CSCsj69176

  Symptoms: When you enter the **standby use-bia** command on an interface and when the HSRP status changes from active to standby on the interface or when HSRP is disabled on an interface that was previously in the active state, the MAC address of the interface is removed from the L2 table. This situation may disrupt L3 connectivity through the interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA, 12.2(33)SRA1, 12.2(33)SRA2, 12.2(33)SRA3, 12.2(33)SRA4, 12.2(33)SRB, or 12.2(33)SRB1.

  Workaround: To prevent the symptom from occurring, do not enter the **standby use-bia** command. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface to restore the MAC address.

Further Problem Description: Cisco IOS Release 12.2(33)SRA is developed for and intended to run on Cisco 7600 series routers. We do not encourage you to run this release on Cisco Catalyst 6500 series switches. However, if you do run Cisco IOS Release 12.2(33)SRA, 12.2(33)SRA1, 12.2(33)SRA2, 12.2(33)SRA3, or 12.2(33)SRA4 on a Cisco Catalyst 6500 series switch, the symptom may occur.

- CSCsj70658

  Symptoms: Counters on 4th interface of a WS-X6704-10GE module may report incorrect traffic levels after 3.4 Gbps of traffic has been exceeded in any one direction.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Workaround: Apply a policy map on the interface to provide correct reporting of the traffic levels.

- CSCsj72723

  Symptoms: The link LED of an Ethernet Services (ES20) line card or an Ethernet SPA that is installed in a SIP-600 may continue to light green even when the port is shut down.

  Conditions: This symptom is observed on a Cisco 7600 series after you have reloaded the line card, the SPA, the SIP-600, or the router.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not impact the functionality of the router because no traffic passes through the port that is shut down even though the LED continues to light green.

- CSCsj73785

  Symptoms: A VLAN check flag is not set for MPLS adjacencies or when incoming packets are routed on the same interface. When this VLAN check failure occurs, packets are punted to RP.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

  Further Problem Description: In an IP-to-IP configuration, you can prevent the symptom from occurring by entering the **no ip redirect** command on the interface. However, when packets are sent from IP to MPLS, this command does not take effect.

- CSCsj78751

  Symptoms: When you enter the **shutdown** command followed by the **no shutdown** command on a 10-Gigabit XFP transceiver module that is installed in an Ethernet Services (ES20) line card, the transceiver module may remain in the down/down state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1 and that has a ES20 line card with a 2x10GE XFP an a DFC 3CXL (7600-ES20-10G3CXL). The symptom occurs only with a 10-Gigabit XFP transceiver module from a particular third-party vendor.

  Workaround: Reset the line card by entering the **hw-module module** *slot-number* **reset** command.

- CSCsj82497

  Symptoms: ATM subinterface statistics are not preserved when the VC is recreated, and are reset to zero.

  Conditions: This symptom is observed on a Cisco router when the VC is recreated, for example, because of a bandwidth or encapsulation change on the VC.

  Workaround: There is no workaround.

- CSCsj84781

  Symptoms: When multicast is configured on a Cisco router, the following error message may be generated in the log:

  ```
  %IPRT-3-NDB_STATE_ERROR: NDB state error (BAD EVENT STATE) (0x8001) 20.0.5.0/24,
  state 7, event 0->1, nh_type 1 flags 4
  - Process= "Exec", ipl= 0, pid= 3
  ```

  Conditions: This symptom is observed when multicast is enabled, that is, when at least one interface is configured with a multicast protocol, and when a route exists as both a unicast route and a native multicast route. For example, the symptom may occur when the following sequence of events occurs:

  – 10.0.0.0 255.0.0.0 is learned in unicast via an IGP.

  – You then configure the same router as a multicast static route:

    ```
    ip route 10.0.0.0 255.0.0.0 192.168.200.1 multicast
    ```

  – Reachability to the multicast route flaps.

  Workaround: There is no workaround.

  Further Problem Description: In addition to the conditions that are stated above, the set of prefixes in the multicast routing table has certain distribution properties. A variety of cases can meet the criteria which are not easily described.

- CSCsj85463

  Symptoms: When a large number of subinterfaces are configured on an interface of an Ethernet Services (ES20) line card and when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface, high CPU usage may occur on the switch processor and/or line card.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB or Release 12.2(33)SRB1.

  Workaround: There is no workaround.

- CSCsj88208

  Symptoms: The digital optical monitoring (DOM) feature may be disabled on Xenpak modules of the type SR, LR, ER, LR+, and ER+. However, when this situation occurs, the Xenpak modules can still be used to pass traffic.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that runs Cisco IOS Release 12.2(33)SXH or Release 12.2(33)SRB.

  Workaround: There is no workaround.

  Further Problem Description: Note that an LR+ Xenpak module is an LR Xenpak module with a part number of “10-1838-04” and that an ER+ Xenpak module is ER Xenpak module with a part number of “10-1888-04”.

- CSCsj89208

  Symptoms: A TLB exception may occur on the RP when you perform an OIR of a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series when a SPA-2X1GE-V2 SPA with a total of 8000 Ethernet virtual connections (EVCs) (4000 per port) is installed in the SIP-400.

  Workaround: There is no workaround.

- CSCsj90451

  Symptoms: When the **mpls ip** interface configuration command is enabled on an interface, the processing of traffic to an MPLS cloud may cause high CPU usage at the interrupt level.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1. The symptom occurs because of an incorrect hardware adjacency for a route that was learned via BGP.

Workaround: Disable the **mpls ip** interface configuration command.

- CSCsj91795

  Symptoms: An application traffic class may not be monitored passively but can only be monitored actively. In addition, application traffic cannot be used for load-balancing.

  Conditions: These symptoms are observed in an optimized edge routing (OER) configuration with a Cisco router that functions as a master controller (MC) that runs Cisco IOS Release 12.4(15)T and a border router (BR) that runs Release 12.2(33)SRB.

  Workaround: Use the active monitoring mode for the performance policy. There is no workaround to load-balance application traffic.

- CSCsj91961

  Symptoms: When you first create the channels for an E3 interface in a particular order on the active supervisor engine and then the standby supervisor engine is reloaded, the ifNumber objects on the active and standby supervisor engines do not match. This situation prevents proper forwarding on the E3 interface after a switchover.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an Enhanced FlexWAN.

  Workaround: Reload the router after you have configured the channels for the E3 interface.

- CSCsj92153

  Symptoms: Prolonged high CPU usage may occur in the “Tag Control” process in steady-state conditions and in the “IP RIB Update” process during route change events.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that function in a network environment with large numbers of BGP routes such as more than 100,000 BGP routes.

  Workaround: There is no workaround. However, if BGP next-hop tracking is enabled, disable it. Doing so helps to alleviate the high CPU usage because there are less route change events.

- CSCsj93195

  Symptoms: A bus error may occur on an MSFC when ISAKMP is enabled, and the following error message may be generated in the logs:

  ```
  %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON Address Error (load or instruction fetch)
  exception, CPU signal 10, PC = 0x41579EB0
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and that runs Cisco IOS Release 12.2(33)SRA2.

  Workaround: There is no workaround.

  Further Problem Description: Cisco IOS Release 12.2(33)SRAs is developed for and intended to run on Cisco 7600 series routers. We do not encourage you to run this release on Cisco Catalyst 6500 series switches. However, if you do run Cisco IOS Release 12.2(33)SRA2 on a Cisco Catalyst 6500 series switch, the symptom may occur.

- CSCsj93495

  Symptoms: A memory leak may occur on a router that functions in an AToM configuration with Virtual Forwarding Instances (VFIs).

Conditions: This symptom is observed on a Cisco router in a scaled configuration when link flaps occur.

Workaround: There is no workaround.

- CSCsj95033

  Symptoms: When a virtual routing and forwarding (VRF) instance is deleted from a configuration, the memory of the VRF is not freed. This situation causes a leak in the processor memory.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that is based on Release 12.2S when a VRF instance is created and then deleted or when CEF is enabled and then disabled.

  Workaround: Configure the router in such a way that VRF instances are not deleted and that CEF is not enabled and disabled.

- CSCsj95268

  Symptoms: A CPUHOG warning is logged for the environment polling process.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1 and could occur because the CPU is busy when the environment polling process runs.

  Workaround: There is no workaround. Note that the router recovers by itself.

- CSCsk01407

  Symptoms: A CEoP SPA may not come up.

  Conditions: This symptom is observed on a Cisco 7600 series that has a CEoP SPA with a golden FPGA image that is corrupted, which may be related to the frequency of FPD updates.

  Because the corrupt golden FPGA image is only required if a failure occurs during the FPD update process, the corruption may be present for a long period of time before being detected.

  Workaround: There is no workaround. When a golden image is corrupted and when an FPD update failure occurs, the SPA does not boot.

  Further Problem Description: Note that the most frequent cause of FPD failures is a mismatch between the FPD image bundle and the running Cisco IOS software image. (FPD image bundles that support Release 12.2(33)SRB are incompatible with subsequent software images.)

- CSCsk01927

  Symptoms: A VC on a PE router remains up after you have shut down the ATM interface on a connected CE router.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has the **oam-ac emulation-enable** command enabled.

  Workaround: There is no workaround.

- CSCsk02933

  Symptoms: When a multiple path RPF interface group is configured, all interfaces in this group should use distributed cache for a known source address. However, in this situation, packets may processed in route cache on one of the interfaces, which is improper behavior.

  Conditions: This symptom is observed on a Cisco 7600 series that has three or more interfaces configured in a multiple path RPF interface group and occurs after you have entered the **issu runversion** command as part of an ISSU, causing the new standby supervisor engine to become active. Note that the symptom does not yet occur when you enter the **issu loadversion** command but only after you have entered the **issu runversion** command.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCsk04241

  Symptoms: When you enable the laser on a 10GE interface of an Ethernet Services (ES20) line card that is installed in a SIP-600, the XFP may enter a “not ready” state, causing the 10GE interface to remain in the down/down state.

  Conditions: This symptom is observed on a Cisco 7600 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the 10GE interface.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, perform a physical OIR of the line card.

- CSCsk08750

  Symptoms: During an SNMP walk that queries the IF-MIB::ifLastChange instance, the timeticks show a value of zero. When you verify this result against the MIB::sysUpTimeInstance, it does not match. Other interfaces have a valid “ifLastChange” instance value.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1 when an SNMP walk is performed on the ifLastChanged MIB for a 4-port channelized T3 to DS0 SPA (SPA-4XCT3/DS0).

  Workaround: There is no workaround.

- CSCsk08765

  Symptoms: When you add the first link to a multilink or MFR bundle, a bus error crash may occur, and the following error message is generated:

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

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA, Release 12.2(33)SRB1, or Release 12.2SXF when you first have attached a policy map to the multilink or MFR interface and then have added the first link to the bundle.

  Workaround: First, add the required number of links to the multilink or MFR interface. Then, attach the service policy to the multilink or MFR interface.

- CSCsk14208

  Symptoms: A WAN line card or module that is configured for WCCP Redirection via the **ip wccp web-cache redirect {out | in}** interface configuration command may not redirect packets to the Cache Engine after an OIR has occurred or after the line card or module has been reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when WCCP redirection is applied to the interfaces that are configured on the WAN line card or module.

  Workaround: Remove and re-apply the WCCP Redirection configuration to the affected WAN interfaces by entering the **no ip wccp web-cache redirect {out** | **in}** interface configuration command followed by the **ip wccp web-cache redirect {out** | **in}** interface configuration command.

  Alternate Workaround: Delete and configure WCCP Redirection globally on the router by entering the **no ip wccp web-cache** router configuration command followed by the **ip wccp web-cache** router configuration command.

- CSCsk16706

  Symptoms: Interface configuration changes on the active supervisor engine may be rejected with the following error message:

  ```
  %ERROR: Standby doesn't support this command
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when a line card is reset while the standby engine is still booting up to its terminal state in SSO or RPR-plus (RPR+) operating mode.

  Workaround: Reboot the standby supervisor engine.

- CSCsk21925

  Symptoms: Both the primary and backup tunnels pass traffic when the primary tunnel is still active and when you have entered the **no shutdown** command on the backup tunnel. This situation causes traffic to reach the peers via both the primary and backup tunnels.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for FRR.

  Workaround: There is no workaround.

- CSCsk22554

  Symptoms: You may not be able to unconfigure a switchport on an Ethernet Services (ES20) line card.

  Conditions: This symptom is observed on a Cisco 7600 series after you first have configured and unconfigured an EFP on an ES20 line card, and then you configure and attempt to unconfigure a switchport.

  Workaround: There is no workaround.

- CSCsk37096

  Symptoms: When there are many Xconnect attachment circuits or VFIs configured on a router, the following error message may be generated on startup:

  ```
  Task is running for (2000)msecs, more than (2000)msecs (4465/4464),process = CDP
  Protocol.
  ```

  Conditions: This symptom is observed on a Cisco router only when there are several thousand Xconnect attachment circuits or VFIs configured.

  Workaround: There is no workaround. However, the message is harmless and can be ignored.

- CSCsk37110

  Symptoms: When there are 1000 to 4000 VFIs configured and when an SSO switchover occurs, multiple tracebacks may be generated on the new primary RP, and there is long delay before the VCs start to switch packets.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB in a configuration with two RPs that function in SSO mode.

  Workaround: There is no workaround.

- CSCsk39340

  Symptoms: High CPU usage may occur when the IP Rewrite Manager (IPRM) is active.

  Conditions: This symptom is observed on a Cisco router when there is a large number of prefixes and when there is network instability.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat alleviates the high CPU usage.

- CSCsk43336

  Symptoms: BGP routes that are reachable via a next hop over a traffic engineering (TE) tunnel may be removed from the RIB for up to one hour when the physical interface on which the TE tunnel is configured flaps.

  Conditions: This symptom is observed on a Cisco router when a link state IGP (IS-IS or OSPF) is configured to use TE tunnels and when the physical interface on which the IGP has a neighbor and that is part of the Label Switched Path (LSP) for the TE tunnel flaps. The symptom occurs when the IGP neighbor is restored and when the TE tunnel comes up before IGP reinstalls the routes that were affected by the interface flap. In this situation, BGP may not be informed about the reachability of the BGP next hop.

  Workaround: There is no workaround. The BGP routes will eventually be restored as a result of a background check that is performed by BGP, but this may take up to an hour.

  Further Problem Description: The symptom does not occur when no multicast protocol is configured.

- CSCsk44055

  Symptoms: After a router has been reloaded, traffic may no longer pass on an interface that has the **switchport trunk encapsulation dot1q** command enabled.

  Conditions: This symptom is observed on rare occasions on a Cisco 7600 series that has a Route Switch Processor 720 (RSP720).

  Workaround: Reset the line card. If this is not an option, there is no workaround. Reloading the router is not a workaround.

  Further Problem Description: The symptom does not on a Cisco 7600 series that has a supervisor engine.

- CSCsk45057

  Symptoms: Layer 2 traffic flooding stops after you have removed a VLAN from the database and then added the VLAN to the VLAN database on a SIP-400. The following is an example of a sequence of commands that causes the symptom to occur:

  ```
  config t
  no vlan vlanid
  vlan vlanid
  exit
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when the core-facing interface is in the label imposition path of an VPLS or EoMPLS VC. Note that traffic that is destined for a known MAC address is not affected.

  Workaround: Enter the following sequence of command to restore the traffic:

  ```
  config t
  interface vlan vlanid
  shutdown
  no shutdown
  ```

- CSCsk48565

  This caveat consists of two symptoms, one condition, and one workaround:

  Symptom 1: When both Distributed Compressed Real-Time Protocol (dCRTP) and QoS are configured, compression does not occur, and the output of the **show ip rtp header-compression** command shows all counters as zero.

Symptom 2: When the **ppp multilink fragment-delay 8** command is configured on an MLP interface, packets are wrongly fragmented.

Conditions: These symptoms are observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

Workaround: There is no workaround

- CSCsk49151

  Symptoms: A policy map with MPLS EXP ingress marking attached to a non-EoMPLS VLAN is removed when the router is reloaded.

  Conditions: This symptom is observed on a Cisco 7600 series after you have reloaded the router.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, re-attach the policy map to the VLAN interface.

- CSCsk53232

  Symptoms: When you reconfigure a POS interface on a SIP-400 from BCP (PPP) bridging to Frame Relay bridging, traffic may not flow.

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

  Workaround: Reload the SIP-400 microcode or reload the SIP-400.

- CSCsk54783

  Symptoms: A Cisco 7600 series may crash when many transmission errors occur in the network and when the router processes a corrupt packet with a size of 9 bytes carries a partial RFC1483 header.

  Conditions: This symptom is observed on a Cisco 7600 series with a SIP-400 in which a ATM SPA is installed that is configured for MPB. YOu can check the SPA error counters to determine the transmission errors.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs when, after the router has received the corrupt packet, the network processor sends a short-length packet to the Encoded Address Recognition Logic (EARL) engine, which, in turn, triggers the Hyperion ASIC to reset.

- CSCsk56395

  Symptoms: A VC on a PE router remains up after you have shut down the ATM interface on a connected CE router, and the **oam-ac emulation-enable** command does not show in the output of the **show running-config** command.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has the **oam-ac emulation-enable** command enabled.

  Workaround: There is no workaround.

- CSCsk57114

  Symptoms: CPUHOG messages may be generated when an “snmpwalk” is performed on the cpwVcMplsNonTeMappingTable object.

  Conditions: This symptom is observed on a Cisco router that has a large number (about 30,000) of pseudowires configured.

  Workaround: Reduce the number of pseudowires that are configured on the router.

- CSCsk59014

  Symptoms: When a bridge domain service instance is configured at boot time, the Switch Virtual Interface (SVI) remains in the down state.

Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-400 that is configured for Multipoint Bridging (MPB).

Workaround: There is no workaround.

- CSCsk62662

  Symptoms: After the router is reloaded, traffic may not be forwarded by one of the line cards. An end-to-end ping may also fail.

  Conditions: This symptom is observed on rare occasions on a Cisco 7600 series that has a Route Switch Processor 720. The symptom does not occur with other supervisor engines.

  Workaround: Reset the line card.

- CSCsk67457

  Symptoms: Traffic stops flowing on an interface that is configured for Bridge Control Protocol (BCP) over Multilink PPP (MLP).

  Conditions: This symptom is observed on a cisco 7600 series when one of the member links of the MLP interface is shut down.

  Workaround: Bring up the member link that is shut down.

  Alternate Workaround: Reset the MLP bundle interface.

- CSCsk72529

  Symptoms: After you have initiated an SSO switchover by entering the **redundancy force-switchover** command, layer 2 traffic flooding stops on the redundant supervisor engine after you have removed a VLAN from the database and then added the VLAN to the VLAN database on a SIP-400. The following is an example of a sequence of commands that causes the symptom to occur:

  ```
  config t
  no vlan vlanid
  vlan vlanid
  exit
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when the core-facing interface is in the label imposition path of an VPLS or EoMPLS VC Note that traffic that is destined for a known MAC address is not affected.

  Workaround: Enter the following sequence of command on the redundant supervisor engine to restore the traffic:

  ```
  config t
  interface vlan vlanid
  shutdown
  no shutdown
  ```

- CSCsk74750

  Symptoms: The standby supervisor engine may crash when you perform an OIR of an Ethernet Services (ES20) line card that has a highly scaled configuration.

  Conditions: This symptom is observed on a Cisco 7600 series that has an ES20 line card (as part of a 7600-ES20-D3CXL bundle) that is configured with 2000 Software Ethernet over MPLS VCs, 4000 Scalable Ethernet over MPLS VCs, and 500 Hardware Ethernet over MPLS VCs.

  Workaround: There is no workaround.

- CSCuk61396

  Symptoms: WCCP service redirection may not work. In particular, packets that are rejected by a third-party vendor appliance device and are returned to the router for normal forwarding may be discarded.

  Conditions: This symptom is observed on a Cisco router when NAT or Cisco IOS Firewall features are enabled on the same interfaces that have WCCP enabled.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsg39837

  Symptoms: HTTP errors may occur while accessing a Win2003 Web Server.

  Conditions: This symptom is observed on a voice gateway that runs Cisco IOS Release 12.4(6)T when a Win2003 HTTP web server is accessed under a heavy load and when the voice gateway has the **ip http client connection persistent** command disabled. Note that the symptom may also affect other releases.

  Workaround: There are two possible workarounds:

  1. Switch to a Win2000 HTTP web server.
  2. On a Win2003 server, set "TcpTimedWaitDelay" to the minimum (30 seconds). This does not totally eliminate but will reduce the occurrences of dropped TCP SYN requests from the Cisco IOS router.

Wide-Area Networking

- CSCek49202

  Symptoms: When an attempt to move an interface from one multilink group to another fails because of platform-specific limitations, the interface is left in an invalid state. The **multilink-group** command still appears in the interface configuration, but the interface does not appear in the output of **show ppp multilink** command.

  Conditions: This symptom may occur on platforms that support distributed implementations of multilink (such as the Cisco 7500 series, Cisco 7600 series, Cisco 10000 series, and Cisco 12000 series routers) when the platform does not allow the interface to be added to a multilink group for some reason, for example, because of resource constraints.

  Workaround: Enter the **no multilink-group** command to remove the interface from its current multilink group before adding it to a new one.

- CSCsi70599

  This caveats consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: When you create a dynamic Frame-Relay map and remove it by entering the **no frame-relay map** command, the standby RP may reboot unexpectedly.

     Condition 1: This symptom is observed on a Cisco 7600 series. However, the symptom may be platform-independent.

     Workaround 1: Do not enter the **no frame-relay map** command to remove a dynamic Frame-Relay map. Rather, enter the **clear frame-relay inarp** command.

2. Symptom 2: When you create a dynamic Frame-Relay map and remove it by entering the **no frame-relay map** command, the router may generate the following error message:

   ```
   %REDUNDANCY-3-CONFIG_SYNC: Active and Standby lbl configuration out of sync
   ```

   Condition 2: This symptom is observed on a Cisco 12000 series. However, the symptom may be platform-independent.

   Workaround 2: Do not enter the **no frame-relay map** command to remove a dynamic Frame-Relay map. Rather, enter the **clear frame-relay inarp** command.

- CSCsi70727

  Symptoms: A fragment size may be incorrect for Link Fragmentation and Interleaving (LFI) over Frame Relay.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink PPP (MLP) over Frame Relay when a script tests LFI over Frame Relay by looking for a fragment size in the output of the **show ppp multilink interface** *number* command.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRB1

Cisco IOS Release 12.2(33)SRB1 is a rebuild release for Cisco IOS Release 12.2(33)SRB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRB1 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCin93236

  Symptoms: The CPU usage of the TACACS+ process may be high.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCeh31423. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh31423. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCir01788

  Symptoms: The **ip-tacacs source-interface** command is missing from the command line interface (CLI).

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsd23056

  Symptoms: Reverse Telnet may not function.

  Conditions: This symptom is observed when AAA authentication is enabled for the asynchronous line over which you attempt to establish a reverse Telnet connection. The AAA authentication prompt takes the console output as input for the AAA authentication process, causing a login failure for reverse Telnet.

  Workaround: There is no workaround.

- CSCsd49317

  Symptoms: When you enter the **no tacacs-server administration** command, the router may crash because of processor memory corruption.

  Conditions: This symptom is observed when you enter the **no tacacs-server administration** command while the **tacacs-server administration** command was not previously configured.

  Workaround: Do not enter the **no tacacs-server administration** command while the **tacacs-server administration** command was not previously configured.

- CSCsh72214

  Symptoms: A router may reject a valid username and password during the authentication of a console or vty session.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the **aaa authentication login local** is configured on the console or vty.

  Workaround: Configure authentication by entering the **aaa authentication login default local** command, which still enables the local username database on the router for authentication.

Interfaces and Bridging

- CSCed79345

  Symptoms: A router crashes when you enter the **default/no bridge-group** *bridge group* **subscriber-loop-control** interface configuration command.

  Conditions: This symptom is observed when there are no existing bridge-group configurations on the router.

  Workaround: There is no workaround.

- CSCek43732

  Symptoms: All packets are dropped from a 1-port OC-3/STM-1 POS port adapter (PA-POS-1OC3) or 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) that is configured for CBWFQ.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1. However, the symptom may be platform-independent.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCed84633

  Symptoms: The *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command do not function.

  Conditions: This symptom is observed on a Cisco platform that integrates the fix for caveat CSCea59206. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCea59206. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

  Further Problem Description: The fix for CSCed84633 re-enables the *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command for both VRF interfaces and non-VRF interfaces.

- CSCek38025

  Symptoms: A Multicast Distribution Tree (MDT) update does not reach a remote PE router.

  Conditions: This symptom is observed when some of the routers in the network core send MDT addresses in the form of VPNv4 extended community attributes and other routers in the network core send MDT addresses in the MDT SAFI format.

  Workaround: Configure all routers in the network core to use only one form of MDT implementation (that is, configure either the VPNv4 extended community format or the MDT SAFI format).

- CSCek45564

  Symptoms: A router crashes because of memory corruption when you bring up Gigabit Ethernet links and BGP neighbor adjacencies, and an error message is generated, indicating that a block overrun and rezone corruption have occurred.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series that are configured for BGP. However, the symptom is not platform-dependent.

  Workaround: There is no workaround.

- CSCek68270

  Symptoms: A router that is configured for EIGRP may crash.

  Conditions: This symptom is observed on a Cisco router that contains an 0.0.0.0/0 address in the EIGRP topology with multiple next hops that change in quick succession.

  Workaround: Limit the 0.0.0.0/0 address to a single next hop.

- CSCek68507

  Symptoms: A router that has the **ip multicast limit** command enabled may crash when you enter the **show running-configuration** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB but is both platform- and release-independent. When you remove or re-enable a tunnel or virtual interface that has the **ip multicast limit** command enabled, a spurious memory access may occur, and the router may crash.

  Workaround: There is no workaround.

- CSCsb96034

  Symptoms: Routes redistributed from other routing protocols to BGP will be deleted and re-added after an NSF switchover, potentially causing traffic to go down for a long period of time.

  Conditions: This symptom may occur when the route is redistributed from other routing protocols (such as OSPF, ISIS, EIGRP) to BGP.

  Workaround: There is no workaround.

- CSCse41484

  Symptoms: A DMVPN hub receives a few unencrypted GRE packets from a spoke during the negotiation of an IPsec security association (SA).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for NHRP and that have an IPsec VPN SPA that functions as a spoke in a DMVPN topology.

  Workaround: There is no workaround.

- CSCse51804

  This caveat consists of two symptoms, two conditions, and two workarounds:

Symptom 1: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

Condition 1: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4 when the DMVPN tunnel is up and when you enter the **show ip nhrp brief** and **clear ip nhrp** commands. When the tunnel comes up again (because of the NHRP registration by the spoke), the NHRP cache entry expires a long time before its expiration time.

Workaround 1: Do not enter the **show ip nhrp brief** command.

Symptom 2: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

Condition 2: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4(6)T or a later release and occurs without any specific action.

Workaround 2: There is no workaround.

Further Problem Description: These symptoms are not release-specific.

- CSCsg83966

  Symptoms: Paths that are imported via VPN may be missing from the VRF. For example, paths that are imported from the same route distinguisher (RD) may be missing from the VRF.

  The route map that is specified in the **import ipv4 unicast map** *route-map* command is meant to be applied to paths that are imported into the VRF from the global table. However, the route map is also incorrectly applied to VPN paths during the VPN import process. When the route map filters some of these paths, they are not imported, which is shown in the output of the **show ip bgp vpnv4 vrf vpn-name** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when you use the **import ipv4 unicast map** *route-map* command to import an address family from the global table into a VRF. The following sequence of events illustrates how the symptom occurs:

  1. Configure an IP prefix list. [example: ip prefix-list COLORADO seq 5 permit 10.1.5.0/24]
  2. Configure a route map by using the prefix list as the matching criteria. [example: route-map UNICAST permit 10 match ip address prefix-list COLORADO]
  3. Import the route map into the VRF. [example: ip vrf isp1 rd 65031:100 import IPv4 Unicast map UNICAST route-target export 65031:100 route-target import 65031:100]
  4. Trigger a routing update by entering the **clear ip bgp** command.
  5. Check the output of the **show ip bgp vpnv4 vrf vpn-name** command. The output does not show entries from the BGP neighbor.

  Workaround: There is no workaround.

- CSCsh02161

  Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

  Conditions: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

  Workaround: There is no workaround.

- CSCsh17035

  Symptoms: A route may flap continuously and the CPU usage may be high continuously.

Conditions: This symptom is observed on a Cisco router that is configured with a static route loop.

Workaround: Do not configure a static route loop.

- CSCsh61119

  Symptoms: ARP may be refreshed excessively on the default interface, causing high CPU usage in the "Collection Process."

  Conditions: This symptom is observed on a Cisco router that has point-to-point interfaces that have non-/32 interface addresses or secondary addresses and that constantly come up or go down.

  Workaround: There is no workaround.

- CSCsh65136

  Symptoms: RSVP reservations may become lost or may not be rebuilt when an SSO switchover occurs. Although RSVP is not SSO-aware, RSVP reservations should be re-established after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with dual Supervisor Engine 720 modules and a Policy Feature Card 3BXL (PFC3BXL) and that functions in the following configuration:

  – The Cisco 7600 series functions as a mid-point router.

  – The router that sends RSVP reservations is a downstream router.

  – The router that should receive the RSVP reservations is an upstream router and is enabled for RSVP CAC.

  The interfaces that are used in the topology are Gigabit Ethernet interfaces and 10-Gigabit Ethernet with subinterfaces.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the mid-point router.

- CSCsh66294

  Symptoms: A Cisco 7600 series that is configured for BGP crashes during normal operation.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions as a PE router in an MPLS environment.

  Workaround: There is no workaround.

- CSCsh91798

  Symptoms: After you have unconfigured a VRFm, the VRF may not be removed properly and remain in the "delete pending" state.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN.

  Workaround: There are no workaround.

ISO CLNS

- CSCek69976

  Symptoms: An IS-IS adjacency message may not be copied correctly between the active RP and the standby RP.

  Conditions: This symptom is observed on a Cisco router when an In Service Software Upgrade (ISSU) is performed between a Cisco IOS software image with IS-IS ISSU support for adjacency message version 2 and a Cisco IOS software image with IS-IS ISSU support for adjacency message version 4.

Workaround: There is no workaround.

- CSCsf26043

  Symptoms: IS-IS protocol packets may not be classified as high-priority. When this situation occurs during stress conditions and when the IS-IS protocol packets are mixed with other packets, the IS-IS protocol packets may be dropped because of their low-priority.

  Conditions: This symptom is observed on a Cisco platform that is configured for Selective Packet Discard (SPD).

  Workaround: Ensure that DSCP rewrite is enabled and then enter the following command:

  mls qos protocol isis precedence 6

Miscellaneous

- CSCeb21064

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)
  – Media Gateway Control Protocol (MGCP)
  – Signaling protocols H.323, H.254
  – Real-time Transport Protocol (RTP)
  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCeg02918

  Symptoms: A Cisco router that is configured with an HTTP authentication proxy may reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs a crypto image of Cisco IOS Release 12.3(9) or Release 12.3(10). Note that the symptom is not release-specific.

  Workaround: Disable the HTTP authentication proxy. If this is not an option, there is no workaround.

- CSCeh18195

  Symptoms: Packets that flow to VPNv4 destinations may be dropped for up to one second when the next-hop router clears its IS-IS overload bit after having been rebooted.

  Conditions: This symptom is observed in a MPLS-TE network with one-hop TE tunnels.

  Workaround: There is no workaround.

- CSCek28110

  Symptoms: XDR tracebacks are generated after an SSO switchover has occurred.

Conditions: This symptom is observed on a Cisco router and seems to occur only after multiple SSO switchovers have occurred.

Workaround: There is no workaround.

- CSCek63433

  Symptoms: An MSFC bus error crash may occur, and the following error message may be generated:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x40B96C4C
  ```

  Conditions: This symptom is observed when multiple processes share a socket, causing the RP to crash during the exit of these processes.

  Workaround: There is no workaround.

- CSCek64847

  Symptoms: On a router that is configured for Hot Standby Router Protocol (HSRP), the hold timer that is configured via the **standby timers msec** command does not function properly when the standby group number is 17 or higher.

  The configured standby hold time changes unexpectedly to 3 times the group number value instead of remaining in the 50-3000 msec range when the standby group is configured in the 17-4095 range.

  Also, when a relatively high number is configured for the standby group, a "%PARSER-4-BADRANGE" error message is generated.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(6)T3 or Release 12.4(11)T but may also affect other releases such as Release 12.2SR.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(5a).

- CSCek65022

  Symptoms: A 7600-SSC-400 SPA services carrier may crash during the boot process of a SPA.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when an IPsec VPN Shared Port Adapter (SPA-IPSEC-2G) that is installed in the 7600-SSC-400 boots.

  Workaround: There is no workaround.

- CSCek66114

  Symptoms: After an SSO switchover has occurred, the standby supervisor may not come up because the startup configuration does not synchronize to the standby supervisor.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB after a single or multiple SSO switchovers have occurred.

  Workaround: There is no workaround.

- CSCek66277

  Symptoms: When you run the TestAclDeny diagnostic test, the output of the **show diagnostic content module** *num* command, with the *num* representing the active supervisor engine, shows the test as "N" to denote non-disruptive. This situation is shown in the following example:

  ```
  18) TestAclDeny ---------------------> M**N****A*** 000 00:00:05.00 n/a
  ```

  In reality, the TestAclDeny diagnostic test for the active supervisor engine is a disruptive test because the test may cause traffic forwarding issues and flapping of the first uplink port.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Do not run the TestAclDeny diagnostic test.

Further Problem Description: The fix for this caveat sets the flag to “D” to denote disruptive.

- CSCek66294

  Symptoms: The TCP MSS Adjustment feature works only in the ingress direction. The feature should work both in the ingress and egress direction.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCek66731

  Symptoms: On a Cisco 7600 series packets that are received by a routed interface that does not have an IPv4 address may be forwarded by CEF.

  Conditions: This symptom is observed when the Cisco 7600 series receives an IP packet on an interface that has no IPv4 address enabled but that has a matching route entry to forward the packet to a destination.

  Workaround: Shut down the interface that has no IPv4 address enabled.

- CSCek67622

  Symptoms: The **bfd interval** command is accepted on EtherChannel and EtherChannel member interfaces.

  Conditions: This symptom is observed on a Cisco router while BFD is not supported on EtherChannels.

  Workaround: Do not enter the **bfd interval** command on EtherChannel and EtherChannel member interfaces.

- CSCek67701

  Symptoms: When an exception occurs on an IPSec VPN SPA (SPA-IPSEC-2G) there is insufficient time to save the crashdump file before the SPA-IPSEC-2G is automatically reset.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables the SPA-IPSEC-2G to save the crashinfo file. In turn, the crashinfo file enables you to find the cause of the exception.

- CSCek68017

  Symptoms: When more than 4000 entries are allocated in a VPN table in an MPLS configuration, the following error message may be generated:

  ```
  %VPNMAP-SP-2-SPACE_EXCEEDED
  ```

  Conditions: This symptom is observed on a Cisco 7600 that runs Cisco IOS Release 12.2(33)SRB when EoMPLS VCs boot or when the router is configured with IPv4 VRFs. The symptom occurs irrespective of whether or not IPv6 is configured.

  Workaround: There is no workaround.

- CSCek68370

  Symptoms: An Xconnect interface that is configured on an Ethernet Virtual Circuit (EVC) may remain down.

  Conditions: This symptom is observed when the encapsulation is set to default or untagged.

  Workaround: There is no workaround.

- CSCek68853

  Symptoms: On a Cisco 7600 series that has redundant Supervisor Engine 32 modules, the standby supervisor engine reloads unexpectedly during the boot process and generates the following error message:

  ```
  %RF-SP-3-NOTIF_TMO: Notification timer Expired for RF Client: Cat6k CAPI(1317)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that functions in SSO mode, that has a scaled Multipoint Bridging (MPB) configuration with 16,000 ATM MPBs and 4000 Frame Relay MPBs, and that is configured for Circuit Emulation over Pseudowires (CEoP), Virtual Private LAN Services (VPLS), and other features.

  Workaround: There is no workaround.

- CSCek68959

  Symptoms: When a second RPR+ switchover occurs and when an OSM-2+4GE-WAN+ module resets during the switchover, the running configuration may become lost on the OSM-2+4GE-WAN+ module. When this situation occurs, the interfaces and the L2 and L3 VPNS that are configured on the OSM-2+4GE-WAN+ module do not come up, and traffic that is processed over these interfaces and VPNS becomes lost.

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

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, copy the startup configuration to the running configuration.

- CSCek69134

  Symptoms: When you enter the **default interface** command on an interface with a scaled Ethernet Virtual Circuit (EVC) service instance configuration, it may take a long time for the command to be executed, and during this time, the CPU usage of the RP may increase to 100 percent. In addition, many error messages may be generated.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when a scaled EVC service instance configuration is enabled on a Gigabit Ethernet port of a 20-port Ethernet Services line card (7600-ES20-GE) that is installed in a SIP-400.

  Workaround: There is no workaround. You must wait until the command has been executed. However, the command functions properly.

  Further Problem Description: The **default interface** command is often used to set an interface to its default state before a configuration is applied, and it is used to remove a scaled configuration from an interface by just entering one command rather than deleting individual configuration lines one-by-one.

  As an alternative, you can enter the **no service instance** command for each service instance on the port. The following example shows steps to simplify the process:

  Instead of entering the **default gi1/0/1** command, do the following:

  1. Enter the **show running interface gi1/0/1 | inc service instance** command.
  2. Cut-and-paste the output into your preferred editor.
  3. Edit the file by placing “no” before each line.
  4. Enter the following configuration:

     conf t int gi1/0/1 <*paste the file*>

     or just copy the file to running configuration.

- CSCek69280

  Symptoms: When you initiate an SSO switchover after several ISSU transitions have been executed, a SIP-400 may reload unexpectedly. When this situation occurs, the following error message is generated:

  ```
  %OIR-SP-3-PWRCYCLE: Card in module 9, is being power-cycled off (Reset - Module
  Reloaded During Download)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

  issu loadversion issu abortversion redundancy force-switchover

  or the following sequence of commands:

  issu loadversion issu runversion issu acceptversion issu abortversion redundancy force-switchover

  Workaround: Do not use the **issu abortversion** command.

  Further Problem Description: The SIP-400 does not normally reload when the **redundancy force-switchover** command is executed. The SIP-400 reloads only if first a sequence of ISSU transitions is performed, and then the **redundancy force-switchover** command is executed.

- CSCek69641

  Symptoms: When you perform an ISSU downgrade after an ISSU upgrade has occurred, a 10-Gigabit Ethernet Switching Module (WS-X6704-10GE) may crash, and the following error messages may be generated:

  ```
  SP: PREDNLD_ERRMSG: IPC: Failed to tx image pkt to IPC port Slot 9/0: REDNLD: retry
  queue flush [for 9/0]
  ```

  ```
  %OIR-SP-6-NOPWRISSU: Card inserted in slot 9 powered down because ISSU is in progress
  ```

  ```
  %MDR_SM-SP-3-SLOT_NOTIFY_TIMEOUT: Notification timeout on MDR slot state machine 9
  for the local client Last SP MDR client (1) in state SLOT_PREDOWNLOAD
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

  First, you perform and ISSU upgrade to the new Cisco IOS software image:

  ```
  issu loadversion
  issu abortversion
  issu runversion
  issu acceptversion
  issu commitversion
  ```

  Then, you perform and ISSU downgrade to the old Cisco IOS software image:

  issu loadversion

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command and restart the ISSU downgrade procedure by entering the **issu loadversion** command.

- CSCek70058

  Symptoms: An Optical Services Module (OSM) may crash because of a memory corruption.

  Conditions: This symptom is observed when you apply a QoS configuration with WRED.

  Workaround: There is no workaround.

- CSCek70210

  Symptoms: Control word information may not be programmed on the forwarding table, causing a datapath failure through an EoMPLS VC.

  Conditions: This symptom is observed very rarely on a Cisco 7600 series that has a VC that is configured for Xconnect.

  Workaround: Remove the Xconnect configuration from the affected VC and then reconfigure it on the VC.

- CSCek70552

  Symptoms: When traffic is directed through a route map that is configured for policy-based routing (PBR) over TE tunnels to a tunnel that is configured for FRR, the traffic may freeze when the protected link flaps.

  Conditions: This symptom is observed on a Cisco 7600 series. When the protected link goes down, traffic does continue through the backup tunnel, but when the protected link returns to normal operation, traffic may freeze.

  Workaround: Detach and re-attach the route map.

- CSCek72661

  Symptoms: SNMP context cannot be properly configured under the address-family IPv4 or IPv6 submode as part of the **vrf definition** *vrf-name* command:

  ```
  vrf definition <vrf-name>
  address-family <address-family name>
  snmp context <context-name>
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN.

  Workaround: There is no workaround.

- CSCek73818

  Symptoms: A router may crash when the **echo revision** command is enabled under an MPLS OAM configuration.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR but is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCek76212

  Symptoms: A ping over a dot1q interface with 118 + n * 256 byte packets (in which n = 0,1,2...) may not go through.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB with a Route Switch Processor 720 (RSP720) when a packet of the size stated in the Symptoms is received on a dot1q interface and must be software-switched. The symptom is specific to the RSP720.

  Workaround: There is no workaround.

- CSCir01182

  Symptoms: A ping that is issued via the **ping mpls pseudowire** command from one PE router to another PE router may fail.

  Conditions: This symptom is observed on a Cisco router on which a FEC 128 AToM static pseudowire is established when AToM VCCV packets are sent to verify the connectivity between the two PE routers. Note that the static pseudowire functionality works fine.

Workaround: There is no workaround.

- CSCir01449

  Symptoms: A router that functions under a heavy load with SSHv2 clients may crash if any of the SSH clients are terminated.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA or Release 12.2(33)SRB when the following conditions are present:

  – The CPU usage is above 70 percent.

  – There are continuous sweep pings from two far-end routers that have the **debug ip packet** command enabled to create continuous logs for the SSH clients.

  – The **no logging console** command is configured.

  – A connection is made from a couple of SSHv2 clients, you enable the **terminal monitor** command, and you terminate the SSHv2 clients while continuous messages are being generated.

  – The TCP window size is reduced.

  Workaround: Do not use SSHv2 when the router is very stressed.

- CSCir02111

  Symptoms: Tracebacks and error messages may be generated on a Supervisor Engine 720.

  Conditions: This symptom is observed when the PSD module in a Cisco 7600 series is reset to the AP mode.

  Workaround: There is no workaround.

- CSCsb54378

  Symptoms: A router may reload due to software forced crash.

  Conditions: This problem has been observed when initiating a Secure Shell (SSH) session from the router or when copying a file to/from the router via SCP.

  Workaround: Do not initiate SSH or SCP sessions from the router.

  Further Problem Description: This was observed on a Cisco 2811 router that was running Cisco IOS Release 12.4(4)T. Note that the symptom is not platform- or release-specific.

  Prior to the crash, the router logs a series of %SYS-3-CPUHOG messages and will eventually crash with %SYS-2-WATCHDOG. See the following example:

```
%SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs
(1426/5),process = Virtual Exec.
-Traceback= 0x41DC8E2C 0x41DC9098 0x41BAA6E0 0x41BA6990 0x41B96B4C 0x41BA6768
0x41BA7490 0x41BA7750
0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8
0x41834200
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Virtual Exec.
-Traceback= 0x41A23CC8 0x41BAA3D8 0x41BA6A08 0x41B96B4C 0x41BA6768 0x41BA7490
0x41BA7750 0x41BAC854
0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8 0x41834200
0x418341E4
%Software-forced reload
```

- CSCsb64767

  Symptoms: When a layer 2 EtherChannel is load-balancing multicast traffic on multiple member ports of a local switch or router, one port may not transmit multicast packets but may drop them. When this situation occurs, the OutMcastPkts counter for this port does not increase.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when an OIR is performed on a line card of the remote switch or router, causing the local port that is a member of the EtherChannel to change its state to link down and then to link up.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on affected member port of the local switch or router. Doing so re-enables multicast forwarding.

- CSCsb85982

  Symptoms: A router that is configured for AAA may crash because of a bus error and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB or Release 12.2SRB and that has AAA authentication enabled.

  Workaround: There is no workaround.

- CSCsc09892

  Symptoms: A spurious memory access may occur on a supervisor engine.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for SNMP and QoS.

  Workaround: There is no workaround.

- CSCsc19259

  The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

  The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml.

- CSCsc22043

  Symptoms: The TCL script feature on Cisco IOS routers allows the use of CLI commands to be issued and the response to be checked for certain matching conditions. When using the TCL script with the **cli_open** command, a VTY for that script is setup for the exec commands to be issued. The output to the VTY only catches (with the **cli_read** and **cli_read_pattern** commands) output which is directly printed out as a result of the command; i.e., allows the script to match the output of the **show interface** command.

Output as the results of debug and syslog cannot be seen by the script. Some test commands on the gateway also uses debug to display the output and this can cause problems trying to monitor for certain conditions.

Conditions: This symptom has been observed by using TCL script to monitor the output of syslog or debug output on the VTY session which the script is using.

Workaround: There is no workaround.

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

  Workaround: There is no workaround.

- CSCsd73598

  Symptoms: A "%SYS-3-MGDTIMER: Uninitialized timer" error message and traceback may be generated when you remove the **bfd interval** command from a GE-WAN interface

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router. However, the symptom may occur on any platform and with any type of interface when you remove the **bfd interval** command.

  Workaround: There is no workaround.

- CSCsd81407

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)

  – Media Gateway Control Protocol (MGCP)

  – Signaling protocols H.323, H.254

  – Real-time Transport Protocol (RTP)

  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS, documented as Cisco bug ID CSCsd85587
- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM) CSCsi97695

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

Note: Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

- CSCsd95575

  Symptoms: A switch or router crashes because of a TEMPALARM message on the SP.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have a Supervisor Engine 720 router and occurs only with an automated script, often when the script runs the **clear ip route *** command.

  Workaround: There is no workaround.

- CSCse02510

  Symptoms: On a Cisco router that is configured for Hierarchal Queuing Framework (HQF), the RP may crash and generate an “ALIGN-1-FATAL” error message when the “PC hqf_process_wfq_command” function is accessed.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXE2 or Release 12.2(18)SXF4 but may also affect other platforms and releases. The symptom occurs on rare occasions after a service policy has been modified on an ATM subinterface or PVC.

  Workaround: There is no workaround.

- CSCse19299

  Symptoms: Some packet drops may occur during SA negotiation between two spokes. The expected behavior is that during SA negotiation between the spokes, the traffic should flow through spoke-to-hub tunnels. Note that when the spoke-to-spoke SA is up, traffic flows fine without any packet drops.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCse24889

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

  Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

  ```
  config t
  ip ssh version 1
  end
  ```

  Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

  ```
  10.1.1.0/24 is a trusted network that
  is permitted access to the router, all
  other access is denied
  ```

  ```
  access-list 99 permit 10.1.1.0 0.0.0.255
  access-list 99 deny any
  ```

  ```
  line vty 0 4
  access-class 99 in
  end
  ```

  Further Problem Description:

  For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

  http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a0080716ec2.html.

  For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

  http://www.cisco.com/warp/public/707/ssh.shtml.

- CSCse40423

  Symptoms: A tunnel interface cannot ping the other end of an IP tunnel.

  Conditions: This symptom is observed when ATM is configured and when the tunnel interface is up.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the tunnel interface.

- CSCse56501

  Symptoms: When two sockets are bound to the same port, the first File Descriptor always receives the requests.

  Conditions: This symptom is observed on a Cisco router when two sockets such as one IPv4 socket and one IPv6 socket are connected to the same UDP port.

  Workaround: Use different UDP ports for different sockets.

- CSCse77758

  Symptoms: The secondary RP may fail to boot (that is, reach the SSO mode) after the **ipv6 unicast-routing** command is disabled on the primary RP. During the reboot of the secondary RP, the following message is displayed on its console:

  ```
  %Cannot disable IPv6 CEF on this platform
  ```

  On the primary RP, the following messages are displayed on its console:

  ```
  Config Sync: Starting lines from PRC file:
  -no ipv6 cef
  ```

  ```
  Config Sync: Bulk-sync failure, Reloading Standby
  ```

  Conditions: This symptom is observed on a Cisco router that has dual RPs and that runs Cisco IOS Release 12.2SB.

  Workaround: First, re-enable IPv6 by entering the **ipv6 unicast-routing** command on the primary RP. Then, reboot the secondary RP.

- CSCse98235

  Symptoms: Hardware-switched multicast traffic may be adversely affected by a subinterface configuration. When a large number of subinterfaces (about 1000) are disables and then enabled by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a physical interface, some of the subinterfaces are missing from the OIF list.

  Conditions: This symptom is observed on a 20-port Ethernet Services line card (7600-ES20-GE) that is installed in a Cisco 7600 series.

  Workaround: Enable the Consistency Checker.

- CSCsf13044

  Symptoms: The outgoing interface (OIF) for bidirectional PIM multicast routes is not updated properly because PIM joins are not received through the MDT tunnel.

  Conditions: This symptom is observed on a Cisco 7600 series that has Gigabit Ethernet interfaces that are configured for dCEF. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsf31458

  Symptoms: The entPhysicalIndex object of the ENTITY-MIB may not remain the same after an SSO switchover has occurred on a Supervisor Engine 32.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsf98858

  Symptoms: Failure detection time with Bidirectional Forwarding Detection (BFD) echo mode takes longer than with BFD asynchronous mode.

  Conditions: This symptom is observed on a Cisco router that has 100 BFD neighbors.

  Workaround: Use the BFD asynchronous mode by entering the **no bfd echo** command on the interface that has BFD enabled.

- CSCsg03739

  Symptoms: A memory leak may occur in the “Crypto IKMP” process.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an IPSec VPN SPA (SPA-IPSEC-2G).

Workaround: There is no workaround.

- CSCsg21429

  Symptoms: The interface of an OSM-1OC48-POS-SI+ module may flap after you have entered the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with redundant Supervisor Engine 720-3BXL modules that function in RPR+ mode.

  Workaround: Repeat the **redundancy force-switchover** command several times.

- CSCsg35506

  Symptoms: After a Gigabit Ethernet (GE) interface has flapped, a mismatch may occur on a port channel, preventing the GE interface from joining the port channel. This situation occurs when the default flow control operational mode on the GE interface is unexpectedly changed from “off/off” to “on” after the GE interface has flapped.

  If the symptom occurs for the first interface of a group of interfaces that is supposed to join the port channel, none of the interfaces in the group can join the port channel, degrading the bandwidth and possibly causing severe packet drops on the channel.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router, and affects the following modules:

  – Supervisor Engines 1 and 1a
  – Supervisor Engine 2
  – WS-X6408-GBIC
  – WS-X6416-GBIC
  – WS-X6516-GBIC and WS-X6516A-GBIC

  Note that the symptom does not occur with the WS-X6724-SFP and the WS-X6748-GE-TX.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected GE interface.

  Further Problem Description:

  – Any operation that causes flow control negotiation triggers the symptom. For example. problem, entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command, resetting the module, performing an OIR, an RPR switchover, and so on.
  – The symptom tends to occur when many ports are brought up simultaneously.

- CSCsg37484

  Symptoms: A router may reload because of a bus error in a crypto map and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x4284A878
  ```

  Conditions: This symptom is observed on a Cisco router that has an IPSec crypto map.

  Workaround: There is no workaround.

- CSCsg37644

  Symptoms: Cisco IOS SLB does not function when the client is located behind the MPLS cloud.

  Conditions: This symptom is observed on a Cisco 7600 series when the response packets to the client are forwarded over the MPLS tunnel interface.

Workaround: There is no workaround.

- CSCsg40391

  Symptoms: When a dot1x port is authenticated and assigned a VLAN by an AAA server and then the line card for the port is reset, the assigned VLAN becomes the configured access VLAN for the port. You can see this situation in the running configuration for the port.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reconfigure the access VLAN for the port to the old value.

  Further Problem Description: If, at a later time, you unconfigure dot1x on the port but do not unconfigure the access VLAN, the configuration for the assigned VLAN remains in place, causing the port to have access to whatever VLAN was previously assigned.

- CSCsg40567

  Symptoms: Malformed SSL packets may cause a router to leak multiple memory blocks.

  Conditions: This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

  Workaround: Disable the **ip http secure server** command.

- CSCsg40573

  Symptoms: A Cisco 7600 series may enter a state in which the FIB is frozen, and the syslog may show information similar to the following:

  ```
  %MLSCEF-SP-2-SANITY_FAIL: Sanity Check of MLS FIB s/w structures failed
  %MLSCEF-SP-2-FREEZE: hardware switching disabled on card
  ```

  In this frozen state the data plane is not affected, but new forwarding information does not take effect on the hardware, causing an inconsistency between MPLS or IP software forwarding and the hardware.

  Conditions: This symptom is observed when the TCAM information for a label or prefix and mask does not match the software version, which prevents the TCAM driver from deleting the label or prefix and mask. For example, the symptom may occur when a label is moved from one type (for example, form an aggregate label) to another other type (for example, to a non-aggregate label).

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the router.

  Further Problem Description: You can check the status of the FIB by entering the **show mls cef hardware | i TCAM** command. When the symptom has occurred, the output of this command shows the following:

  ```
  CEF TCAM v3: (FROZEN)
  ```

- CSCsg43284

  Symptoms: A VPN tunnel may fail to establish a proper connection to a Cisco Catalyst 6500 series switch or Cisco 7600 series router because fragmented ISAKMP packet are dropped by the IPSec VPN Services Module (SPA-IPSEC-2G).

  Conditions: This symptom may occur for many reasons, including the following:

  – The peer sends too many different proposals.

  – The certificate that is used by the peer is too large, for example, because the key is too large, the issuer-name is long, the subject-name is long, the are many CDPs, and so on.

Workaround: In some circumstances, when the peer is an EzVPN client router that runs Cisco IOS Release 12.4T, changing the Cisco IOS software image to Release 12.4 may reduce the size of the proposals.

When the certificate of the peer is too large, reduce the size of the RSA key, and/or remove or reduce long fields in the certificate.

Further Problem Description: When the symptom occurs, a packet capture of all traffic that is received by and sent to the switch or router shows the following:

- The fragmented ISAKMP packets that are sent to the switch or router.
- The response (several seconds or up to one minute later) of the switch or router with the following ICMP packet:

```
Type: 11 (Time-to-live exceeded)
Code: 1 (Fragment reassembly time exceeded)
```

- CSCsg47039

  Symptoms: After a Fast Reroute (FRR) event and multiple failure situations have occurred, any of the following line cards or port adapters may crash:

  - SIP-600
  - 2-port Ethernet Services line card (7600-ES20-10G)
  - 20-port Ethernet Services line card (7600-ES20-GE)

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for MPLS Traffic Engineering Fast Reroute--Link Protection when the line card or port adapter is processing incoming traffic from the MPLS core and when the following sequence of events occurs:

  - You remove the protected TE tunnel configuration from the protected interface.
  - You add back the protected TE tunnel configuration to the same interface.
  - You clear the fault that caused the FRR event.

  The crash occurs after OSPF and LDP are negotiated through the protected interface.

  Workaround: After the FRR event has occurred, do not remove the protected TE tunnel configuration from the protected interface.

- CSCsg51811

  Symptoms: When the OER BGP Inbound Optimization feature is configured and when route control is enforced, route control does not prepend autonomous systems or communities. Rather, router control prepends the same autonomous systems or communities to all external OER interfaces.

  Conditions: This symptom is observed on a Cisco router when OER manages inside prefixes that are either learned or configured.

  Workaround: There is no workaround.

- CSCsg61773

  Symptoms: Egress multicast forwarding may not function when an outgoing interface (OIF) flaps very quickly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when Multicast MultiLayer Switching (MMLS) is configured (MMLS is configured by default).

  Workaround: There is no workaround.

Further Problem Description: When an interface flaps very quickly, the module mask may not be allocated for the interface, causing the egress multicast functionality to be affected. In this situation, the interface may not function properly as an OIF.

- CSCsg62226

  Symptoms: An active HSRP router may crash when you configure and unconfigure Hot Standby Router Protocol (HSRP) multiple times.

  Conditions: This symptom is observed when the active router and the standby router are configured with a single Front Door VRF (FVRF) and a single Inside VRF (IVRF), when routing through a GRE tunnel over a VTI occurs via EIGRP, and when the physical IP connectivity occurs via OSPF.

  Workaround: To prevent the symptom from occurring, do not configure and unconfigure HSRP multiple times, but reload the routers and reconfigure both of them.

- CSCsg64170

  Symptoms: When an SSO switchover occurs for an RSP or supervisor engine, network traffic loss may occur or the active Firewall Services Module (FWSM) may unexpectedly failover to the standby FWSM in an unusual way in that both the active and the standby FWSMs become active (that is, the active FWSM remains active and the standby FWSM becomes active). This situation causes traffic loss to and from the FWSMs until the standby FWSM enters the standby state.

  The symptom is not restricted to the FWSMs but may also occur with the following service modules:

  – WS-SVC-WEBVPN-K9
  – WS-SVC-SSL-1-K9
  – WS-SVC-FWM-1-K9
  – WS-X6066-SLB-APC
  – WS-X6066-SLB-S-K9

  Conditions: These symptoms are observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have service modules installed in slot 1 and slot 2. The symptoms occur when two power supplies are inserted in the chassis but only one power supply is turned on or one power supply fails during normal operation, and then a SSO switchover occurs. The symptoms do not occur when both power supplies are turned on or when there is only one power supply in the chassis.

  Workaround: Ensure that both power supplies are turned on.

  Alternate Workaround: Install the service modules in any slots other than slot 1 or slot 2.

- CSCsg68406

  Symptoms: After a HA switchover occurs because you have entered the **issu runversion** command, a link flap may occur on the uplink ports of the newly active supervisor engine, causing traffic on these ports to be disrupted for several seconds and the following error message to be generated on the console:

  ```
  %EARL-SP-2-SWITCH_BUS_IDLE: Switching bus is idle for 10 seconds. The card grant is 7
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a certain combination of line cards and occurs only during the Enhanced Fast Software Upgrade (EFSU) process. In particular, the symptom is observed when the router has redundant Supervisor Engine 720 cards, one or more legacy line cards such as a WS-X6148-GE-TX, and one or more EFSU-enabled cards such as a WS-X6724-SFP.

  Workaround: There is no workaround.

- CSCsg73179

  Symptoms: After a change in the routing topology, a Bidirectional PIM Rendezvous Point is not updated correctly in the hardware tables, causing Bidirectional PIM multicast flows to be software-switched.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs only when the ACL that is used to statically configure the Rendezvous Point does not have any wildcard entries.

  Workaround: Reinstall the Rendezvous Point.

- CSCsg82389

  Symptoms: When a T1 controller is shut down on a 1-port channelized OC-3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM), the CEM circuit that is attached to the T1 controller remains up. This is not proper behavior: when the T1 is controller is shut down, the CEM circuit should also go down.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when a T1 or T3 controller on a SPA-1CHOC3-CE-ATM is shut down.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command for the individual CEM circuit that is attached to the T1 controller.

- CSCsg90190

  Symptoms: Without the enforcement of a voice daughterboard connector rating, the number of IP phones that can be powered up may exceed the number that the voice daughterboard can handle, that is, the available allocated inline power can exceed the VDB connector rating.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsg94565

  Symptoms: An incorrect MTU may be used for a GRE/IPSec tunnel that is configured on an IPSec SPA VPN module (SPA-IPSEC-2G), causing unexpected fragmentation.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2.

  Workaround: There is no workaround.

- CSCsg99394

  Symptoms: A Frame Relay map may take a long time to be populated after a line card has reset one of the peers.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for dMFR, that dMFR bundles configured on a SPA that is installed in a SIP-200, and that is connected to another router that is also configured for dMFR.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs because Rx and Tx sequence numbers get out of synchronization between the peers.

- CSCsg99877

  Symptoms: Load-sharing on core links may not function.

  Conditions: This symptom is observed on a Cisco router that functions in an AToM configuration with multiple VCs, with traffic flowing through each VC, and with multiple equal-cost paths to the core.

Workaround: There is no workaround.

- CSCsg99914

  Symptoms: A SIP-200 may reset unexpectedly because of a keepalive failure when there is a lot of IPC backplane traffic and when Ethernet Out of Band Channel (EOBC) traffic drops occur because of a low queue size at the EOBC level.

  Conditions: This symptom is observed on a Cisco 7600 series that functions with a scaled configuration when a major and sudden topology change causes many IPC messages on the backplane.

  Workaround: There is no workaround.

- CSCsh01749

  Symptoms: The **mls qos marking ignore port-trust** command may not function.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch or Cisco 7600 series router that has a Supervisor Engine 32 or Supervisor Engine 720. When you enter the **mls qos marking ignore port-trust** command for an interface that is configured with several subinterfaces, each with a service policy, the service policies are supposed to match a unique ingress CoS value and change the corresponding egress MPLS EXP value for transfer across an MPLS cloud. However, after you have entered the **mls qos marking ignore port-trust** command, all egress EXP values show up as 0 because the command has no effect.

  Workaround: There is no workaround.

- CSCsh02724

  Symptoms: The standby RP crashes continuously, that is, the standby RP is reset continuously.

  Conditions: This symptom is observed when an MTR-aware route processor (RP) is paired with a non-MTR-aware RP in a dual-RP ISSU configuration and when the MTR-aware RP is the active RP.

  Workaround: Ensure that both RPs run an MTR-aware Cisco IOS software image.

- CSCsh07037

  Symptoms: A “%SYS-2- CHUNKBADMAGIC” error mat occur on an OSM module and the module may restart.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when Weighted Random Early Detection (WRED) is configured with a maximum threshold of more than 2000 packets but without a queue limit.

  Workaround: Configure a proper queue limit for the class with the WRED configuration. For example, when the **random-detect precedence 3 32000 32000 1** command is configured, configure the queue limit by entering the **queue-limit 32768** command.

- CSCsh11498

  Symptoms: When you boot a switch or router with two SPA-IPSEC-2G SPAs in the same Services SPA Carrier (7600-SSC-400), one of the SPAs does not come up. When you attempt to boot the switch or router again, both SPAs come up properly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsh13291

  Symptoms: When a fatal CEF error occurs on a line card other than the RP, CEF becomes disabled on the RP and therefore on the router.

Conditions: This symptom is observed on a Cisco router after at least one switchover has occurred since the router booted.

Workaround: There is no workaround.

Further Problem Description: Another issue can trigger the symptoms: When two 7600-SSC-400 line cards are present in a Cisco 7600 series, CEF on the active RP disables itself about 100 minutes after the router has booted if one or more switchovers have occurred during these 100 minutes.

- CSCsh13947

  Symptoms: A router that is processing certain MPLS forwarding updates may crash or hang because of a software configuration mismatch.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB but may also occur in other releases. The symptom occurs when EoMPLS or AToM is configured with many virtual circuits (VCs) and when LDP sessions go down because of extreme traffic loads or clearing of the LDP neighbors, causing the forwarding information to be modified.

  Workaround: There is no workaround.

- CSCsh17979

  Symptoms: When inline power ports can not be powered on, a command may be rejected with the following error message:

  Command rejected: there is not enough system power to be allocated to Fa1/47, or the maximum power the backplane of this chassis can support has reached the limit.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a module with a voice daughtercard.

  Workaround: There is no workaround.

- CSCsh18070

  Symptoms: Routing protocols may flap on a service instance or routed VPLS (R-VPLS) interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured with an Ethernet Services (ES20) line card and any WAN module and/or SIP. The symptom occurs when the traffic through the service instance or R-VPLS interface exceeds the line rate in the egress direction or when the traffic exceeds the shape rate in the class-default class of an MQC policy.

  Workaround: There is no workaround. The symptom is less likely to occur when you reduce the traffic on the port to below the line rate or below the shaping rate.

  Further Problem Description: The symptom occurs because control packets are not treated as high-priority packets on the service instance or R-VPLS interface.

- CSCsh20354

  Symptom 1: A third-party vendor VPN client may not be able to establish a VPN tunnel to a Cisco router. When you enable the **debug crypto isakmp** command on the Cisco router, the output shows the following:

  ```
  ISAKMP:(0:4:HW:2):No IP address pool defined for
  ISAKMP! ISAKMP:(0:4:HW:2):deleting SA reason “Fail to allocate ip address” state (R)
  CONF_ADDR (peer x.x.x.x)
  ```

  Symptom 2: Although a third-party vendor VPN client can establish a VPN tunnel to a Cisco router, the client receives only an IP address but no DNS configuration, split-tunnel information, or other data during the mode configuration phase. In this situation, the debug output does not show any errors.

Conditions: Both of these symptoms are observed only when a third-party vendor VPN client connects to a Cisco router that functions as a VPN server.

Workaround: There are no workarounds.

- CSCsh20479

  Symptoms: IP services that are configured on an active software EoMPLS VC may not process L3 control frames.

  Conditions: This symptom is observed on a Cisco router when an active software EoMPLS VC (that is, when an Xconnect statement is configured via an SVI/VLAN interface) is configured with an L3 IP address and L3 control frames such as L3 ARP or OSPF multicast frames.

  Workaround: Remove the SVI interface and recreate the SVI interface with the L3 IP address before you configure the EoMPLS xconnect statement. Doing so enables IP services first and then the EoMPLS VC, allowing both to function properly.

- CSCsh21398

  Symptoms: A Cisco 7600 series in which a WS-F6700-DFC3BXL module with 256 MB of memory is installed may run out of memory and display memory allocation failure messages such as the following:

  ```
  %SYS-DFC2-2-MALLOCFAIL: Memory allocation of 4188 bytes failed from 0x205336A0,
  alignment 0 Pool: Processor  Free: 56780  Cause: Memory fragmentation

  Alternate Pool: None  Free: 0  Cause: No Alternate pool

  -Process= "XDR LC Background", ipl= 0, pid= 181

  -Traceback= 20412DD8 2041331C 2050227C 2050BD08 205336A8 211642AC 2113B39C 211393B4
  2114C100 2114ADBC 2113721C 21137354 2113794C 21137CE8 211B7C78 21202F10

  %FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2): CEF-Common: no memory

  %ADJ-DFC2-3-ALLOCATEFAIL: Failed to allocate an adjacency

  -Traceback= 20412DD8 2041331C 211A3DE0 211A4414 21129664 21129850 21139294

  211393A4 2114C100 2114ADBC 21e1 3t7o2 1aC  f2a1tal err1or.37354 2113794C 21137CE8
  211B7C78 21202F10

  %COMMON_FIB-DFC2-3-NOMEM: Memory allocation failure for path list in Common

  CEF [0x21139490] (fatal) (0 subsequent failures).

  %COMMON_FIB-DFC2-4-DISABLING: Common CEF is being disabled due to a fatal error.

  %FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2): CEF-Common: no memory

  %XDR-DFC2-6-XDRLCDISABLEREQUEST: Client CEF push requested to be disabled.

  -Traceback= 20412DD8 2041331C 21217E98 211B0C48 211B3760 21155594 21159FF4 21153D4C
  21153F10 204F6448 204F6434

  %COMMON_FIB-DFC2-4-DISABLING: Common CEF is being disabled due to a fatal error.
  ```

  Conditions: This symptom is observed in a scaled configuration (which is typical of broadband deployments) when 28,000 access subinterfaces are created and brought up.

  Workaround: There is no workaround.

- CSCsh29863

  Symptoms: On an RPR switchover, the new active crashes during bootup diagnostics.

  Conditions: This symptom occurs when bad SFPs are plugged into the SFP- capable ports. Bad SFP means incompatible/unsupported/faulty SFP.

  Workaround: Remove incompatible/unsupported/faulty SFPs from the SFP port(s) and plug in a good one if needed.

- CSCsh31287

  Symptoms: The source MAC address for multicast on a tunnel that is accelerated by a crypto engine may remain zero.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an IPSec VPN Services Module (SPA-IPSEC-2G).

  Workaround: There is no workaround.

- CSCsh31306

  Symptoms: Output drops occurs on a T1 serial interface. These drops are shown in the output of the **show interface serial** command but are not shown at the QoS level, that is, the output of the **show policy-map interface** command does not indicate any drops.

  When this situation occurs, the output of the **show controller** command for the serial interface at the VIP or FlexWAN level shows “pascb.tx_polling_high” with any value other than 2.

  Conditions: The symptoms is observed on a Cisco 7500 series (with a VIP) and Cisco 7600 series (with a FlexWAN module) that have a serial interface that is configured for fair-queueing.

  Workaround: Remove and then reconfigure fair-queueing so that “pascb.tx_polling_high” is set to the correct value of 2.

- CSCsh34536

  Symptoms: A Circuit Emulation (CEM) group configuration may become lost on the standby RP.

  Conditions: This symptom is observed on a Cisco 7600 series when you perform the following steps:

  1. You configure a CEM interface and groups on a Circuit Emulation over Packet (CEoP) SPA.
  2. You shut down the SPA.
  3. You reload the standby supervisor engine and wait until it comes up.
  4. You bring up the SPA from the active RP.

  At this point, the CEM group configuration is lost on the standby RP.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the standby supervisor engine once more.

- CSCsh35236

  Symptoms: A 20-port Ethernet Services line card (7600-ES20-GE) may crash and a “mac_xid=0x10000” PXF exception may be generated.

  Conditions: This symptom is observed on a Cisco 7600 series under a rare condition when a specific (test) source MAC address triggers the crash and when the router function under stress.

  Workaround: There is no workaround.

- CSCsh35451

  Symptoms: In an HA configuration when the router is in the runversion-switchover state, when you enter the **issu runversion** command, the newly active supervisor engine does not come up fully and causes the standby supervisor engine to crash with “Active_Not_Responding” error messages.

  Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

  1. You enter the **issu loadversion** command, and you wait for the router to enter the terminal state.
  2. You enter the **issu runversion** command, and you wait for the router to enter the terminal state.
  3. The active supervisor engine crashes, and then moves to the RunVersionSwitchOver (RVSO) state.

4. The newly active RP and standby RP come up, and you wait for the router to enter the terminal state.
5. Again, you enter the **issu runversion** command on the active supervisor engine.

At this point, the symptom occurs.

Workaround: There is no workaround.

- CSCsh37272

  This caveat consists of three symptoms, three conditions, and one general workaround:

  Symptom 1: “Invalid element for addition!” syslog messages may be generated.

  Condition 1: This symptom is observed in any BFD configuration.

  Symptom 2: The CPU usage may increase unexpectedly to 99 percent for 30 seconds.

  Condition 2: This symptom is observed on a Cisco 7600 series that has a Route Switch Processor 720 (RSP 720) and that is configured for BFD.

  Symptom 3: The router may reload unexpectedly.

  Condition 3: This symptom is observed on a Cisco 7600 series that is configured with a SIP-400 in which a SPA-2X1GE is installed on which there are many subinterfaces, most of which have the **no bfd echo** command enabled.

  Workaround: There is no workaround.

- CSCsh40540

  Symptoms: When a service instance is configured for Xconnect, the pseudowire fails to come up, and an “%SW_MGR-SP-3-CM_ERR” error message is displayed.

  Conditions: The symptom is observed on a Cisco 7600 series only when encapsulation is configured as default.

  Workaround: There is no workaround.

- CSCsh40567

  Symptoms: When OAM cells are transported over a local-switched connection that is configured for AAL5 and for which the VPI or VCI do not match at both endpoints, OAM cells are dropped.

  Conditions: This symptom is observed on a Cisco 7600 series on an ATM SPA that is installed in a SIP-200 or on an ATM port adapter that is installed in a FlexWAN or Enhanced FlexWAN module.

  Workaround: Ensure that the VPI or VCI are the same at both endpoints of the local-switched connection.

- CSCsh42857

  Symptoms: After a TE tunnel has been reoptimized, AToM traffic may no longer pass through because the outgoing label and outgoing interface are not updated in the hardware.

  Conditions: This symptom is observed on a Cisco 7600 series that has AToM circuits configured over a TE tunnel that connects to a CE router.

  Temporary Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the interface that faces the CE router or configure and deconfigure the **xconnect** command on the interface that faces the CE router. Doing so re-establishes traffic forwarding until a new reoptimization occurs.

- CSCsh45829

  Symptoms: An interface that is configured for Xconnect fails to come up.

Conditions: This symptom is observed on a Cisco 7600 series that is configured with a Supervisor Engine 32 and that runs Cisco IOS Release 12.2(33)SRB.

Workaround: There is no workaround.

- CSCsh45905

  Symptoms: A newly active SP may not be set up correctly with the required Xconnect session information for any of the configured Xconnect sessions.

  Conditions: This symptom is observed when you initiate an HA switchover on a Cisco 7600 series that functions as a PE router and that has a large number of Xconnect sessions configured.

  Workaround: There is no workaround.

- CSCsh47823

  Symptoms: CPU usage may become very high. When this situation occurs, a line card may become unable to respond to keepalive polling from the supervisor engine, and the Switch Processor (SP) may reset the line card.

  Conditions: This symptom is observed on a Cisco 7600 series that has a scaled QoS configuration when the Route Processor (RP) sends many configuration changes to the line card.

  Workaround: On both the RP and the SP, disable resetting of the line card for keepalive response failures. On the RP, enter the **test scp linecard keepalive disable** command; on the SP, enter the **debug oir no-reset-on-crash** *slot* command.

- CSCsh51688

  Symptoms: A Cisco 7600 series may crash unexpectedly because of a bus error on the Switch Processor (SP). The following error message may be generated prior to the crash:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x40B450D4
  ```

  Conditions: This symptom is observed on a Cisco 7600 series and the trigger is currently not known.

  Workaround: There is no workaround.

- CSCsh54325

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: When frames require PXF punting to the RP (or SP), PPP LCP frames may not be forwarded to the RP (or SP), causing link negotiation to fail. Or, HDLC keepalives may not be forwarded to the RP (or SP), causing the link to remain down.

  Condition 1: These symptoms are observed on a Cisco Catalyst 6503, Cisco Catalyst 6503-E, and Cisco 7604 that are configured with a SIP-600 in which a POS SPA is installed and occurs when the supervisor engine resides in slot 1 or slot 2 of the chassis.

  Workaround 1: There is no workaround.

  Symptom 2: When frames require PXF punting to the RP (or SP), CFM PDUs may not be properly forwarded to the RP (or RP).

  Condition 2: This symptom is observed on a Cisco 7604 that is configured with a SIP-600 or Ethernet Services line card (ES20) and occurs when the supervisor engine resides in slot 1 or slot 2 of the chassis.

  Workaround 2: There is no workaround.

- CSCsh56121

  Symptoms: After you have reloaded a Cisco 7600 series that has redundant supervisor engines, or after you have forced a redundancy switchover, the RSA key on the standby supervisor engine may be lost.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the RSA key.

- CSCsh57212

  Symptoms: After you have entered the **issu runversion** command, the policy counters in the output of the **show policy-map** command may be zero.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for QoS.

  Workaround: Remove and re-apply the policy.

- CSCsh58337

  Symptoms: After a SSO switchover has occurred, a service policy does not function properly.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that has a service policy that is attached to a CEM circuit.

  Workaround: After the SSO switchover has occurred, reload the SPA on which the CEM circuit is configured by performing a soft OIR.

- CSCsh59439

  Symptoms: You may not be able to configure the same HSRP virtual MAC address on several interfaces or subinterfaces of the same router. When you attempt to do so, the following error message is generated:

  ```
  % MAC address already specified on another group on a different interface.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for HSRP and is not release-specific.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4.

- CSCsh59650

  Symptoms: After you have performed an OIR of an Ethernet Services (ES20) line card that has EFP or EVC service instances configured, control plane information may not be re-downloaded onto the line card. This situation prevents data-plane traffic from being passed, even though the RP does not generate any error messages.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: Reload the line card by entering the **hw-module module** *slot-number* **reset** command.

- CSCsh61393

  Symptoms: When the standby supervisor engine becomes active after an RPR+ switchover has occurred, the transmission of all traffic stops.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an EoMPLS environment. The symptom occurs because a VRF-VLAN with an explicit null label is not properly programmed on the SP and DFC after the standby supervisor engine has become active. This situation can be seen in the output of the following commands:

  On the RP:

  Enter the **show mls cef mpls detail labels** *value* command. For the *value* argument, enter the VRF-VLAN with the explicit null label.

On the SP:

- Enter the **show mls cef mpls detail labels** *value* command. For the *value* argument, enter the VRF-VLAN with the explicit null label.
- Then, enter the **show mls cef adjacency entry** *index* command. For the *index* argument, enter the adjacency index shown in the output of the **show mls cef mpls detail labels** *value* command.

Workaround: There is no workaround.

- CSCsh61851

  Symptoms: A PIM neighborship does not come up on an MDT tunnel when VRFs are removed and added back immediately on PE routers.

  Conditions: This symptom is observed on Cisco 7600 series routers that run Cisco IOS Release 12.2(33)SRB.

  Workaround: Wait for 3 to 4 minutes after you have removed the VRFs on the PE routers so that the backbone entries that are associated with the VRFs expire. Then, add back the VRFs.

  Further Problem Description: The VPN ID is not re-used when a VRF is removed and recreated. This situation results in stale VPN information on the supervisor engine and DFC because backbone entries that are associated with the old VRF can exist until they expire. When a new VPN ID is issued because you recreate the VRF, the hardware entry may not be programmed correctly because of the stale VPN information, preventing the PIM neighborship from being established over the MDT tunnel.

- CSCsh61946

  Symptoms: After an SSO switchover has occurred, the second of two 6000 W DC power supplies in the chassis is shut down.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 router when both power supplies are powered on before the SSO switchover occurs.

  Workaround: There is no workaround.

- CSCsh65322

  Symptoms: A Cisco 7600 series with an Enhanced FlexWAN in which a PA-A3-OC3SMI port adapter is installed may drop packets steadily from the ATM interface. This situation may be verified under the “Total output drops” in the output of the **show interfaces atm** command.

  Conditions: This symptom is observed when the router is configured for PPPoA connections. There is no correlation between the packet drops on the interface and any particular ATM PVCs or virtual-access interfaces. The symptom may also occur on other platforms that are configured with a PA-A3-OC3SMI port adapter.

  Workaround: There is no workaround.

  Further Problem Description: note that the symptom does not occur with a FlexWAN.

- CSCsh66675

  Symptoms: When Circuit Emulation circuits are configured in a very short period via a script and then an RPR+ switchover occurs, the interface of a Circuit Emulation over Packet (CEoP) SPA may shut down.

  Conditions: This symptom is observed rarely on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: After the RPR+ switchover has occurred, enter the **no shutdown** interface configuration command on the interface of the CEoP SPA.

- CSCsh66793

  Symptoms: After you have performed an OIR of a line card, the number of queues that correspond to QoS policies are smaller than before the OIR because not all queues are recreated.

  Conditions: This symptom is observed on a Cisco 7600 series that has a large number of Ethernet Virtual Circuit (EVC) instances on which QoS policies are configured and that are spread across several interfaces.

  Workaround: Perform another OIR of the line card.

- CSCsh73935

  Symptoms: A router may reload when you perform an snmpwalk on the ciscoMvpnMrouteMdtTable.

  Conditions: This symptom is observed when all of the following conditions are present:

  – IP multicast routing is enabled on a VPN routing/forwarding instance (VRF)

  – This VRF is associated with an interface.

  – The Multicast Distribution Tree (MDT) default group address is not configured for the VRF.

  Workaround: Configure the MDT default group address for the VRF by entering the **mdt default** *mdt group* command in VRF configuration mode.

- CSCsh73972

  Symptoms: Traffic that arrives on an interface of a SIP-600 and that should be forwarded over a GRE tunnel with tunnel protection as encrypted packets may be sent unencrypted.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that contain a SIP-600 in one slot and a Services SPA carrier card in which an IPSec VPN SPA (SPA-IPSEC-2G) is installed in another slot.

  Workaround: There is no workaround.

- CSCsh75001

  Symptoms: After a SIP-400 or the router reloads, interfaces remain down until you enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP- 400 in which the following SPAs are installed:

  – a 2-port GE SPA (SPA-2X1GE)

  – a 1-port channelized OC-3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM)

  The interfaces of these SPA are configured with more than 3000 Ethernet Virtual Connection (EVC) flexible instances that are configured for QoS.

  Workaround: There is no workaround.

  Further Problem Description: Configuring more than 3000 EVC instances with QoS on a SIP-400 in which both a SPA-2X1GE and a SPA-1CHOC3-CE-ATM are installed is not supported. A large configuration of EVC instances with QoS can be achieved only without a SPA-1CHOC3-CE-ATM in the SIP-400 in which the SPA-2X1GE is installed.

- CSCsh75176

  Symptoms: A standby RP with a VRF configuration may reload continuously.

  Conditions: This symptom is observed on a Cisco router that is configured for SSO.

  Workaround: There is no workaround.

- CSCsh75609

  Symptoms: When you enter the **show class cem detail** command, the RP of a Cisco 7600 series may crash because of a TLB exception.

  Conditions: This symptom is observed when the CEM class group is defined by and associated to CEM circuits that are shown in the output of the **show class cem detail** command.

  Workaround: There is no workaround.

- CSCsh75730

  Symptoms: Explicit Congestion Notification (ECN) does not function when ECN-capable Transport (ECT) or CE bits are set to 1.

  Conditions: This symptom is observed on a Cisco router that is configured for QoS and that sends traffic.

  Workaround: There is no workaround.

- CSCsh76923

  Symptoms: A Cisco Catalyst 6500 series switch may crash because of memory corruption or a bus error.

  Conditions: This symptom is observed when NAT is configured. The symptom may also affect a Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsh83467

  Symptoms: A standby Supervisor Engine 720 may reset when an entire Circuit Emulation (CEM) configuration is removed and then reconfigured.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the **recovered-clock** command is present in the removed configuration.

  Workaround: Do not remove an entire CEM configuration.

  Alternate Workaround: Disable the **recovered-clock** command before you remove and then reconfigure an entire CEM configuration.

- CSCsh83559

  Symptoms: A Cisco Catalyst 6000 series switch may leak memory in the IP Input task in the Cisco IOS-BASE process. The memory is leaked in a small amount per packet that is process switched over a VRF on the switch. Non-VRF traffic is not affected.

  Conditions: This symptom is seen on a Cisco Catalyst 6000 series switch that is running Cisco IOS Modularity. This can only happen if there are VRFs configured on the switch.

  Workaround: Do not use VRFs.

- CSCsh90556

  Symptoms: Traffic may fail to match the VLAN TCAM, causing traffic to be dropped from a SPA that is installed in a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series when an Xconnect service is configured and when double-tagged frames are sent via a service instance that is configured with single-tag encapsulation.

Workaround: Configure two service instances, as in the following examples:

– A service instance to handle single-tagged packets with VLAN ID = 100:

service instance *10* **ethernet**

encapsulation dot1q *100*

– A service instance to handle double-tagged packets with the outer tag = 100:

service instance *20* **ethernet**

encapsulation dot1q *100* **second-dot1q** *any*

- CSCsh90762

  Symptoms: The hardware adjacencies that correspond to 6PE aggregate labels may be wrongly programmed.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a 6PE router.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interfaces that are associated with the IPv6 prefixes that correspond to the affected 6PE aggregate labels.

- CSCsh92709

  Symptoms: The output of the **show users** command may display the wrong mode of the connection with the user. For example, a PPPoE connection may be shown as a PPPoX25 connection.

  Conditions: This symptom is observed on a Cisco router that is configured with a virtual-template interface.

  Workaround: There is no workaround.

- CSCsh94940

  Symptoms: An active supervisor engine may crash because of memory corruption in the SP processor pool, and the following error message may be generated:

  ```
  %SYS-SP-3-BADFREEMAGIC: Corrupt free block at [...] (magic [...])
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 32 when a periodic SNMP query is made to the L2 MAC table. Because of a race condition, freed memory may be written by another thread, causing memory corruption.

  Note that the symptom does not occur with a Supervisor Engine 1 and Supervisor Engine 2.

  Workaround: Disable the SNMP query to the L2 MAC table.

- CSCsi01422

  Symptoms: Frame Relay traffic shaping in a configuration with a child policy and hierarchical QoS does not function. Traffic does not respond to BECN or FECN marking.

  Conditions: This symptom is observed on a Cisco 7600 series when a service policy is configured under a Frame Relay map class. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsi02033

  Symptoms: On a PE router, a subinterface on which an EoMPLS VC is configured may stop forwarding traffic from the backbone to a CE router. Traffic that is sent from the PE router to the CE router goes through fine. Traffic forwarding from the backbone is affected.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA3 or an earlier release and that functions as a PE router. The symptom occurs when you configure a new subinterface and an IP address on a Gigabit Ethernet (GE) interface that is installed in a SIP-400 and that connects to a remote CE router. In this situation, another subinterface (on the same GE interface) that is configured for EoMPLS no longer functions for traffic that is forwarded from the backbone to the CE router.

Workaround: Remove and reconfigure Xconnect on the affected subinterface.

Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the physical interface on which the affected subinterface is configured.

- CSCsi02778

  Symptoms: When the MPLS Traffic Engineering (TE)-Fast Reroute (FRR) Link and Node Protection feature is enabled, VPLS traffic does not flow from end-to-end after it has been rerouted to single-hop backup tunnel.

  Conditions: This symptom is observed on a Cisco 7600 series when the primary tunnel is a multihop tunnel with implicit-null as the next-hop label and when the backup tunnel is single-hop tunnel. After traffic has been rerouted to the backup tunnel, VCs do come up and the egress path for VPLS VCs is shown correctly as the backup tunnel. However, the traffic does not reach the egress PE router.

  Workaround: There is no workaround.

  Further Problem Description: From the egress line card, enter the following **show** commands to collect information to further debug this issue:

  – Enter the **show platform atom ether-vc** command to identify the egress index of the VPLS VC.

  – Enter the **show platform mpls imposition-table details** command to look at the egress information.

  After traffic has been rerouted to the backup tunnel, the egress label operation is incorrectly programmed to forward the original primary TE label on the label stack.

- CSCsi04396

  Symptoms: Dynamically changing the **rewrite ingress tag** command for an Ethernet virtual circuit (EVC) service instance may not work.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: Remove the service instance and re-add it with the new tag manipulation that is to be performed on the frame ingress to the service instance.

- CSCsi06759

  Symptoms: When you run the **snmpwalk** command, the ifIndex for the subinterfaces of a SIP-200 is not retrieved although the output of a **show** command does show the ifIndex. When you run the **snmpwalk** command, the following error message and a possible traceback are generated:

  ```
  %SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe regn with SNMP IM by driver having ifIndex
  <index> and ifDescr <description>
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router after you have replaced a FlexWAN module with a SIP-200.

  Workaround: There is no workaround.

- CSCsi10219

  Symptoms: A SIP-200 may crash, and a SIP heartbeat failure message may be generated on the console of the RP.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-200 that is configured for hardware-based MLP and cRTP and in which a SPA-8XCHT1/E1, SPA-1XCHSTM1/OC3, SPA-2XCT3/DS0, or SPA-4XCT3/DS0 is installed. The symptom occurs when RTP traffic is processed on the MLP bundle.

  Workaround: Do not configure hardware-based MLP. Rather, when cRTP is required, configure software-based MLP.

- CSCsi10458

  Symptoms: A SIP-200 may unexpectedly reset and generate “SIP-1-PAUSE” error messages.

  Conditions: This symptom is observed when large BGP updates occur simultaneously with IPC/EOBC problems.

  Workaround: There is no workaround.

- CSCsi14145

  Symptoms: The runt counter is updated with runt frames with CRC errors while runt frames with proper CRCs are ignored.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when packets with a size smaller than 64 bytes are received. The output of the **show interface** command accounts only for packets as runt frames that are smaller than 64 bytes and that have CRC errors. Thus, statistics are lost.

  Workaround: There is no workaround.

  Further Problem Description: According to the 802.3 specifics and information on the IEEE website, the definition of runt frames is:

  Runts: Frames that are smaller than the minimum frame size for IEEE-802.3 standard frames. Runt frames typically are caused by collision fragments and are propagated through the network. If the number of runt frames exceeds the number of collisions, there is a problem with a transmitting device.

- CSCsi15821

  Symptoms: When an SSO switchover occurs after you have enabled and disabled the **mls mpls recir-agg** command or removed the recirculated aggregated labels, the newly active supervisor engine may not place the aggregate labels in VPN CAM.

  Conditions: This symptom is observed on a Cisco 7600 series when the total number of aggregate labels that is created is greater than the maximum number of aggregate labels that can be placed in the VPN CAM.

  Workaround: There is no workaround.

- CSCsi22291

  Symptoms: A SIP-200 may unexpectedly reset and generate “SIP-1-PAUSE” error messages.

  Conditions: This symptom is observed when large BGP updates occur simultaneously with IPC/EOBC problems.

  Workaround: There is no workaround.

- CSCsi25583

  Symptoms: The standby supervisor engine may reset continuously and the following messages are generated in the log:

  ```
  Config Sync: Starting lines from MCL file:
  controller E1 2/0/0
  ! <submode> "controller"
  - framing UNFRAMED
  ! </submode> "controller"
  controller E1 2/0/2
  ! <submode> "controller"
  - framing UNFRAMED
  ! </submode> "controller"
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SPA-8XCHT1/E1 and occurs only when the controller functions in unframed mode.

  Workaround: There is no workaround.

- CSCsi26184

  Symptoms: A router may crash and generate the following error messages:

  ```
  %SYS-2-CHUNKBOUNDSIB: Error noticed in the sibling of the chunk pak subblock
  -Process= "LFDp Input Proc"
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk
  -Process= "LFDp Input Proc"
  %Software-forced reload
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB2 and that is configured for MPLS. Note that the symptom is not release-specific.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(28)SB5.

- CSCsi29423

  Symptoms: Unable to ping when packet verification is turned on.

  Conditions: This symptom occurs when packets are corrupted at tail part.

  Workaround: There is no workaround.

- CSCsi35931

  Symptoms: Traffic is dropped when it traverses an EoMPLS pseudowire that is configured for Xconnect on an interface of a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that has a Supervisor Engine 720. The symptom occurs when a packet leaves one side of the layer 2 network with a payload of 1500 bytes and is destined for the SIP-400 side of the pseudowire. The packet is dropped before it arrives at the SIP-400.

  Workaround: When traffic must traverse an EoMPLS pseudowire that is configured for Xconnect, do not use a SIP-400 to terminate this connection. Rather, use another card. A possible workaround may be to change the MTU of the interface of the SIP-400 to 1522 bytes.

- CSCsi64093

  Symptoms: When an Ethernet Services (ES20) line card functions in a VPLS or Multipoint Bridging (MPB) configuration and faces the core, half of the imposition traffic may be dropped in the core.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

The symptom occurs in a VPLS or MPB configuration when, for core-facing packets, the address of the imposition router is used as the source MAC address. In this situation, the upper 16 bits of this address is corrupted with either 0 or 0xFFFF. Some core routers and switches may drop packets with 0xFFFF address corruption, which can be verified by looking at the core-facing source MAC addresses with a sniffer. Because of the distribution of 0 and 0xFFFF source MAC addresses, the amount of dropped packets may be approximately 50 percent of the imposition traffic.

Workaround: There is no workaround.

- CSCsi71285

  Symptoms: An SNMP walk of VLAN statistics or executing the **show vlan counters** command causes the console to wait indefinitely or causes a CPUHOG condition.

  Conditions: This symptom is observed only on a Cisco 7600 series that runs Cisco IOS Release 12.2SRA when VLAN statistics are collected from cached entries.

  Workaround: Do not collect VLAN statistics from cached entries. Rather, ensure that VLAN statistics are collected real-time.

  Further Problem Description: Both SNMP queries and CLI commands block while retrieving non-routed VLAN counters. An SNMP query on any of the ifTable counters for a non-routed VLAN interface blocks the SNMP agent indefinitely. This situation causes the SNMP AGENT queue to fill up and, consequently, SNMP packets to be dropped. In turn, this situation prevents the Network Management application from accessing any other MIB objects that are not related to the non-routed VLANs. Restarting the SNMP agent clears the thread, but as soon as another objects related to the non-routed VLAN is accessed, the SNMP agent blocks again.

- CSCsi99825

  Symptoms: An SNMP Engine may crash at the “idb_get_swsb” and “mpls_if_get_gen_stats” functions.

  Conditions: This symptom is observed on a Cisco 7613 that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: Disable this SNMP query from the CU.

- CSCuk61773

  Symptoms: CPU spikes may occur on a router that is configured for Web Cache Communication Protocol (WCCP) earlier than Release 4.0.7.

  Conditions: This symptom is observed on a Cisco 7600 series when WCCP is in communication with a Cisco Wide Area Application Services (WAAS) appliance. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

Conditions: This symptom is seen under the following conditions:

- The router must have RCP enabled.
- The packet must come from the source address of the designated system configured to send RCP packets to the router.
- The packet must have a specific data content.

Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

- CSCsf33034

  Symptoms: The following error message and tracebacks are generated during the boot process:

  ```
  %TCP-2-INVALIDTCB: Invalid TCB pointer: 0x4704D088
  -Process= "IP Input", ipl= 0, pid= 122
  -Traceback= 409F00FC 409E4C50 407A032C 407D8EAC 4077FF38 407911D0 4078EC2C 4078EDE8
  4078F004
  ```

  Conditions: This symptom is observed on a Cisco platform when a TCP server is configured.

  Workaround: There is no workaround.

  Further Problem Description: A TCP control block that is already freed is referenced or accessed, causing the error message to be generated. This situation does not affect the proper functioning of the platform in any way.

Wide-Area Networking

- CSCsd72854

  Symptoms: When IS-IS is configured on an MLP interface of a 6-port channelized T3 Engine 0 line card, the line card may fail to come up because PPP fails to negotiate OSICP on the MLP interface.

  Conditions: This symptom is observed on a Cisco 12000 series router after you have reloaded the router. Note that the symptom may also occur on other platforms and in other releases.

  Workaround: Increase the PPP timeout retry interval to 10 seconds by entering the **ppp timeout retry 10** command on the interface. (The default timeout retry interval is 2 seconds).

- CSCsi43652

  Symptoms: A Cisco 7600 series that is configured for In Service Software Upgrade (ISSU) may not initialize the standby RP.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for SSO when the active RP runs Cisco IOS Release 12.2(33)SRB or an earlier release and when the standby RP runs Release 12.2(28)SB or a later release.

  Workaround: Do not configure SSO. Rather, configure RPR or RPR+.

Open Caveats—Cisco IOS Release 12.2(33)SRB

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRB. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Interfaces and Bridging

- CSCsf20174

  Symptoms: An enhanced FlexWAN module may reload with certain traffic flows.

  Conditions: This symptom is observed rather rarely on a Cisco 7600 when the enhanced FlexWAN module is configured with an ATM port adapter, has 1483 configurations, and processes traffic.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCek34591

  Symptoms: In a scaled MTR configuration, a memory leak may occur and the memory may be depleted.

  Conditions: This symptom is observed on a Cisco router when you remove the BGP process or when BGP prefixes are advertised or withdrawn.

  Workaround: There is no workaround.

- CSCek69784

  Symptoms: The **redistribute static route-map** command may not function as expected.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for BGP.

  Workaround: There is no workaround.

- CSCsb96034

  Symptoms: Routes redistributed from other routing protocols to BGP will be deleted and re-added after an NSF switchover, potentially causing traffic to go down for a long period of time.

  Conditions: This symptom may occur when the route is redistributed from other routing protocols (such as OSPF, ISIS, EIGRP) to BGP.

  Workaround: There is no workaround.

- CSCsc26247

  Symptoms: Conflicts may occur between the routes in a BGP table and an IP routing table.

  Conditions: This symptom is observed on a Cisco router when BGP routes that are learned via multipaths are reported as locally generated routes (0.0.0.0) in the IP routing table.

  Workaround: There is no workaround.

- CSCsd27372

  Symptoms: BGP may not converge in the specified time and the CPU usage may be near 99 percent.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for VPN and BGP and that functions in a large-scale configuration.

  Workaround: There is no workaround.

- CSCsg25995

  Symptoms: Networks do not show in the Multiprotocol BGP (MBGP) table, as can be seen in the output of the **show ip mbgp** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SR, Release 12.4, or Release 12.4T.

Workaround: Enter the **clear ip bgp** *neighbor-address* command to enable the networks to enter the MBGP table.

- CSCsh02161

  Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

  Conditions: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

  Workaround: There is no workaround.

- CSCsh12384

  Symptoms: Removing a loopback interface when RSVP sessions are active causes a traceback.

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

  Workaround: There is no workaround. However, there is no functional impact to the router.

- CSCsh32655

  Symptoms: A router may crash when you remove a configuration that consists of multiple instances of BGP and the **ip access-list** command.

  Conditions: This symptom is observed on a Cisco router when you remove the configuration through a TFTP server.

  Workaround: Do not use a TFTP server to remove a BGP configuration.

- CSCsh58933

  Symptoms: Route convergence for MPLS VPN routes is slower than expected.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for BGP when the MPLS VPN routes are received by another router that functions as a provided edge (PE) router.

  Workaround: There is no workaround.

- CSCsh64985

  Symptoms: After a switchover occurs on a remote PE router, a tunnel interface that has the **ip pim vrf** *vrf-name* **rp-address** command enabled cannot be found on the local PE router.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router, that is configured for MVPN, and that functions in a provider core network.

  Workaround: There is no workaround.

- CSCsh73139

  Symptoms: IPv6 routes that are redistributed via the **redistribute connected** address family configuration command may disappear after you have performed an OIR of an Enhanced FlexWAN line card.

  Conditions: This symptom is observed on a Cisco 7600 series. Note that only IPv6 is affected, IPv4 works fine.

  Workaround: Disable and then re-enable the **redistribute connected** address family configuration command.

- CSCsh78416

  Symptoms: Stale routes are not flushed from the routing table after the stale path timer has expired during a graceful restart of a BGP session. As a result, all unwanted traffic continues to be processed by the router for those stale routes.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for BGP graceful restart. The symptom occurs when, during the graceful restart of the BGP session, a non-established active session resets.

  Workaround: Clear or restart the BGP process on the router to remove all stale routes.

- CSCsh78786

  Symptoms: When you enter the **no address-family ipv4 mdt** command followed by the **address-family ipv4 mdt** command, a Multicast Distribution Tree (MDT) peer may not come up.

  Conditions: This symptom is observed on a Cisco router that functions in a topology with route reflectors and MDT peers.

  Workaround: Enter the **clear ip bgp** *neighbor-address* **ipv4 mdt** command for the affected MDT peer.

- CSCsh79862

  Symptoms: When IP options packets are received at the rate of 1000 pps, excessive BGP and/or OSPF flaps may occur. These flaps stop on automatically after 15 minutes.

  Conditions: This symptom is observed on a Cisco 7600 series while there is a heavy CPU load during the BGP and/or OSPF route reconvergence process.

  Workaround: Enabling a rate limiter for the IP options packets to ensure that the symptom does not occur.

ISO CLNS

- CSCek69976

  Symptoms: An IS-IS adjacency message may not be copied correctly between the active RP and the standby RP.

  Conditions: This symptom is observed on a Cisco router when an In Service Software Upgrade (ISSU) is performed between a Cisco IOS software image with IS-IS ISSU support for adjacency message version 2 and a Cisco IOS software image with IS-IS ISSU support for adjacency message version 4.

  Workaround: There is no workaround.

Miscellaneous

- CSCeh32251

  Symptoms: A mismatched bandwidth may generate corrupt packets that are not detected in the hardware when CRC-16 is configured on the interfaces. The corrupt packets may cause the CPU usage of the RP to increase to 100 percent, and the corrupt packets may be dropped.

  Conditions: This symptom is observed on a Cisco platform that is configured with a 2-port or 4-port clear channel T3/E3 SPA (SPA-2XT3/E3 or SPA-4XT3/E3) or 4-port channelized T3 (DS0) SPA (SPA-4XCT3/DS0) that is configured for T3 DSU Kentrox mode with a subrate bandwidth above 35,000 when the far-end is also configured for DSU Kentrox mode but with a mismatched bandwidth that is less than 35,000

Workaround: When you use DSU Kentrox mode, configure CRC-32 on the interfaces and configure the correct bandwidth before you enable the interfaces.

- CSCek28110

  Symptoms: XDR tracebacks are generated after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco router and seems to occur only after multiple SSO switchovers have occurred.

  Workaround: There is no workaround.

- CSCek48810

  Symptoms: The SNMP community still exists after you have entered the following commands:

  ```
  snmp-server comm public rw
  snmp-server comm private rw
  end
  auto secure management no-interact
  ```

  The expected behavior is that the SNMP community is removed after you have entered the **auto secure management no-interact** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA or Release 12.2(33)ZW.

  Workaround: There is no workaround.

- CSCek50234

  Symptoms: The standby RP may reload when you enter the **enrollment url** *url* command on the active RP and when the *url* argument represent any device that is visible on the active RP but not the standby RP. When this situation occurs, the following error messages are generated on the console of the active RP:

  ```
  Config Sync: Bulk-sync failure due to PRC mismatch. Please check the full list of PRC failures via:
    show issu config-sync failures prc

  Sync: Starting lines from PRC file:
  crypto pki trustpoint abcd
   ! <submode> "crypto-ca-trustpoint"
  - enrollment url <url> pem
   ! </submode> "crypto-ca-trustpoint"

  Config Sync: Bulk-sync failure, Reloading Standby
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that uses the Public Key Infrastructure (PKI) for authorization. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCek50806

  Symptoms: The standby RP may reload when you enter the **aps revert** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCek53704

  Symptoms: When you first configure and attach more than 255 class maps in a single policy to an interface and when you then remove the policy map, the router crashes.

  Conditions: This symptom is observed on a Cisco router and occurs because a maximum of 255 class maps (that is, 254 user-defined class maps and one default class map) are supported in a single policy map.

  Workaround: There is no workaround. Ensure that you do not configure more than 255 class maps, including the default class map, in a single policy map.

- CSCek61489

  Symptoms: An OSM-2+4GE-WAN+ module may reload unexpectedly because of memory corruption.

  Conditions: This symptom is observed on a Cisco 7600 series when an RPR+ switchover occurs or when you first attach an Input VLAN with a policy map with 250 class maps via the **match input vlan** command to an interface and then detach this Input VLAN from the interface.

  Workaround: There is no workaround.

- CSCek63459

  Symptoms: When you enter the **ping mpls traffic-eng tunnel 1 ttl 1** command, a Cisco 7600 series may crash in the “ldap_explode_dns()” process.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for LDAP.

  Workaround: There is no workaround.

- CSCek63548

  Symptoms: Weighted Random Early Detection (WRED) may not function properly when it is configured at the first level and when a policer is configured at the first and second level over Frame Relay, ATM, or HDLC interfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCek64619

  Symptoms: The APS manual trigger information may become lost in the k1k2 bytes after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7600 series that has a scaled configuration on a 1-port channelized OC-3/STM-1 SPA. The symptom occurs when you first force the working channel to the protect channel by entering the **aps force** command and then an SSO switchover occurs. In this situation, the k1k2 bytes may be reset.

  Workaround: Enter the **aps force** command once more.

  Further Problem Description: This symptom may become problematic when a Add-Drop Multiplexer (ADM) is present and when the channel states are not synchronized in relation to the ADM.

- CSCek64634

  Symptoms: A spurious memory access may be generated at the “memcpy” process during an SSO switchover. The traceback and decode shows the following information:

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs when the FIB IDB of a virtual interface does not properly synchronize after the SSO switchover has occurred.

Workaround: There is no workaround.

- CSCek65003

  Symptoms: When you send multicast traffic through a GRE/IPsec tunnel, the output of the **show interface status** command does not show the correct count for outgoing packets. (Note that the counter for incoming packets functions correctly.)

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an IPsec VPN SPA (SPA-IPSEC-2G).

  Workaround: There is no workaround.

- CSCek65211

  Symptoms: An IPsec VPN SPA may crash when multicast traffic with large packet sizes (incrementing from 5000 to 6000 bytes) is sent at a rate of 10 pps through a GRE tunnel with 50 replications.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an IPsec VPN SPA and occurs only when the IPsec VPN SPA has interface VLANs with different MTUs, causing the GRE tunnels to adapt these different MTUs. When the interface VLANs have identical VLANs, the GRE tunnels function with the same MTU, and the symptom does not occur.

  Workaround: Configure the same MTU on all interface VLANs.

- CSCek65259

  Symptoms: When multicast packets are fragmented, GRE packets are not encapsulated by a crypto card, even though the **show crypto vlan** command shows that the tunnel is accelerated by the crypto card.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Ensure that the GRE packet sizes are smaller than the MTU to enable the crypto card to perform encapsulation.

- CSCek66092

  Symptoms: An IPv6 demultiplexer configuration is rejected over an Ethernet interface when there is an IP address configured on the same interface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(33)SRB or a release later than Release 12.2(31)SB and that is configured for Xconnect.

  Workaround: There is no workaround.

  Further Problem Description: The following example shows a configuration in which the symptom occurs:

  ```
  router(config)#interface FastEthernet5/0
  router(config-if)#ip address 10.10.10.10 255.255.255.0
  router(config-if)#xconnect 192.168.200.200 100 pw-class ipv6_demux
  Incompatible with ip address command on Fa5/0 - command rejected.
  ```

- CSCek66731

  Symptoms: On a Cisco 7600 series packets that are received by a routed interface that does not have an IPv4 address may be forwarded by CEF.

Conditions: This symptom is observed when the Cisco 7600 series receives an IP packet on an interface that has no IPv4 address enabled but that has a matching route entry to forward the packet to a destination.

Workaround: Shut down the interface that has no IPv4 address enabled.

- CSCek67814

  Symptoms: The *bandwidth* argument of the **ip rtp priority** *starting-rtp-port-number port-number-range bandwidth* interface configuration command does not appear when you enter the **show running-config** command.

  The same situation may occur for the **ip rtp reserve** *lowest-udp-port range-of-ports [maximum-bandwidth]* command.

  The rest of the command is correctly displayed and the bandwidth value that is stored internally is correctly set at 0.

  Conditions: This symptom is observed when the *bandwidth* argument (or *maximum-bandwidth* argument) is configured as 0. If any other valid value is configured, it will correctly appear in the output of the **show running-config** command.

  Workaround: There is no workaround.

- CSCek68156

  The following caveat has been closed because a crypto connection is supported only on a Gigabit Ethernet subinterface of an IPsec VPN SPA (SPA-IPSEC-2G).

  Symptoms: A crypto connection does not function when you attempt to establish one on a Gigabit Ethernet subinterface of a line card or module other than a SPA-IPSEC-2G.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCek68370

  Symptoms: An Xconnect interface that is configured on an Ethernet Virtual Circuit (EVC) may remain down.

  Conditions: This symptom is observed when the encapsulation is set to default or untagged.

  Workaround: There is no workaround.

- CSCek68378

  Symptoms: CEF may be unexpectedly disabled after the router has booted or when CEF entries are added at a high rate to an Ethernet module that functions in conjunction with a DFC. When this situation occurs, the output of the **show ip cef** command displays an "%IPv4 CEF not running" message.

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720, that runs Cisco IOS Release 12.2(33)SRA2, and that has an Ethernet module such as a WS-X6816-GBIC module that functions in conjunction with a DFC.

  Workaround: There is no workaround.

- CSCek68511

  Symptoms: Packets that match a policy map are shown as zero in the output of the **show policy-map interface** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that processes unicast traffic.

Workaround: There is no workaround.

- CSCek68959

  Symptoms: When a second RPR+ switchover occurs and when an OSM-2+4GE-WAN+ module resets during the switchover, the running configuration may become lost on the OSM-2+4GE-WAN+ module. When this situation occurs, the interfaces and the L2 and L3 VPNS that are configured on the OSM-2+4GE-WAN+ module do not come up, and traffic that is processed over these interfaces and VPNS becomes lost.

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

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, copy the startup configuration to the running configuration.

- CSCek69063

  Symptoms: L3 control packets may not be properly processed when an IP address is configured on a switch virtual interface (SVI).

  Conditions: This symptom is observed on a Cisco 7600 series when an IP address is configured on an SVI on which an **xconnect** is enabled.

  Workaround: Remove the **xconnect** command from the SVI, add the IP address to the SVI, and then re-add the **xconnect** to the SVI.

- CSCek69280

  Symptoms: When you initiate an SSO switchover after several ISSU transitions have been executed, a SIP-400 may reload unexpectedly. When this situation occurs, the following error message is generated:

  ```
  %OIR-SP-3-PWRCYCLE: Card in module 9, is being power-cycled off (Reset - Module
  Reloaded During Download)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

  ```
  issu loadversion
  issu abortversion
  redundancy force-switchover
  ```

  or the following sequence of commands:

  ```
  issu loadversion
  issu runversion
  issu acceptversion
  issu abortversion
  redundancy force-switchover
  ```

  Workaround: Do not use the **issu abortversion** command.

  Further Problem Description: The SIP-400 does not normally reload when the **redundancy force-switchover** command is executed. The SIP-400 reloads only if first a sequence of ISSU transitions is performed, and then the **redundancy force-switchover** command is executed.

- CSCek69498

  Symptoms: When sustained cell rate (SCR) is configured in port mode on an interface that is configured for ATM over MPLS (AToM), a VC may not come up.

  Conditions: This symptom is observed on a Cisco router that has the **mpls l2transport route** command enabled.

Workaround: Unconfigure and then reconfigure the **mpls l2transport route** command. Doing so enabled the VC to come up.

- CSCek69541

  Symptoms: When a first RPR+ switchover occurs, an OSM-2+4GE-WAN+ module or other OSM may crash at the “hqf_layer_cleanup” function.

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

  Workaround: There is no workaround.

- CSCek69576

  Symptoms: The standby Route Switch Processor 720 (RSP720) may become stuck when it reloads after a switchover has occurred. Eventually, the RSP720 resets and boots fine thereafter. When the symptom occurs, the following error messages are generated:

  ```
  %ONLINE-SP-6-TIMER: Module 8, Proc. 0. Failed to bring online because of timer event
  %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded, changing to Simplex
  mode)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCek69635

  Symptoms: When you perform an ISSU downgrade after an ISSU upgrade has occurred, a SIP-400 may crash and may not record or save the crashinfo file, and the following error messages may be generated:

  ```
  %OIR-3-CRASH: The module in slot 6 has crashed %OIR-6-REMCARD: Card removed from slot
  6, interfaces disabled
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

  First, you perform and ISSU upgrade to the new Cisco IOS software image:

  ```
  issu loadversion
  issu abortversion
  issu runversion
  issu acceptversion
  issu commitversion
  ```

  Then, you perform and ISSU downgrade to the old Cisco IOS software image:

  ```
  issu loadversion
  ```

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command and restart the ISSU downgrade procedure by entering the **issu loadversion** command.

- CSCek69641

  Symptoms: When you perform an ISSU downgrade after an ISSU upgrade has occurred, a 10-Gigabit Ethernet Switching Module (WS-X6704-10GE) may crash, and the following error messages may be generated:

  ```
  SP: PREDNLD_ERRMSG: IPC: Failed to tx image pkt to IPC port Slot 9/0: REDNLD: retry
  queue flush [for 9/0]
  %OIR-SP-6-NOPWRISSU: Card inserted in slot 9 powered down because ISSU is in progress
  ```

```
%MDR_SM-SP-3-SLOT_NOTIFY_TIMEOUT: Notification timeout on MDR slot state machine 9
for the local client Last SP MDR client (1) in state SLOT_PREDOWNLOAD
```

Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

First, you perform and ISSU upgrade to the new Cisco IOS software image:

```
issu loadversion
issu abortversion
issu runversion
issu acceptversion
issu commitversion
```

Then, you perform and ISSU downgrade to the old Cisco IOS software image:

```
issu loadversion
```

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command and restart the ISSU downgrade procedure by entering the **issu loadversion** command.

- CSCek69770

  Symptoms: When you enter the **context snmp** VRF configuration command, the command is accepted but does not appear in the running configuration.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS 12.2(33)SRB and that is configured for MPLS VPN.

  Workaround: There is no workaround.

- CSCek69798

  Symptoms: A router that is configured for QoS may crash without any clear trigger.

  Conditions: This symptom is observed when you change the redundancy mode from RPR+ to SSO.

  Workaround: There is no workaround.

- CSCek69876

  Symptoms: Explicit bumping values are not shown in the output of the **show atm bundle** command.

  Conditions: This symptom is observed on a Cisco router that functions as a CE router when you enter the **no bump explicit** command for an ATM VC class. In this situation, the output of the **show atm bundle** command should show a null value, which it does not.

  Workaround: There is no workaround.

- CSCek69878

  Symptoms: The connectivity check between two CE router may stop functioning.

  Conditions: This symptom is observed on a Cisco router that functions in an ATM and MPLS configuration when you change the experimental bits on the PVC link between two PE routers that are associated with the CE routers.

  Workaround: There is no workaround.

- CSCsb08994

  Symptoms: The **test ip** command returns an ambiguous command error.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS interim Release 12.4(2.5) or interim Release 12.4(2.2)T and that is configured with an NPE-G1 (revision B) processor. However, not that the symptom is both platform- and release-independent.

Workaround: There is no workaround.

- CSCsb28210

  Symptoms: When you establish a Telnet connection to the IP address of a virtual server, you are unexpectedly connected to a Server Load Balancing (SLB) device on which the virtual IP address is configured.

  Conditions: This symptom is observed when the virtual server functions in dispatch mode, when a real server in a serverfarm that is associated with the virtual server is down, and when the ARP entry for the real server is marked as incomplete.

  Workaround: Clear the ARP table in the SLB device before you establish a connection to the virtual server.

  Alternate Workaround: Use ping probes to detect a failure of the real server so you can prevent SLB from assigning connections to the failed real server.

- CSCsb29314

  Symptoms: A ping probe does not function in client NAT mode.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that function in a Server Load Balancing (SLB) configuration.

  Workaround: There is no workaround.

  Further Problem Description: Note that the symptom does not occur in Cisco IOS Release 12.2(18)SXF5.

- CSCse23576

  The following caveat has been closed because the situation that is described is a known issue when there is a configuration with a large number of tunnels.

  Symptoms: When you toggle a configuration by entering the **no crypto engine accelerator** *slot* command followed by the **crypto engine accelerator** *slot* command on an interface or interface range, the CPU usage on the router may spike.

  You can verify this situation in output of the **show processes cpu sorted** command, which will show the process “FM core” as one of the top CPU utilizers.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB that functions in a configuration with a a large number of tunnels.

  Workaround: There is no workaround.

- CSCse28397

  Symptoms: The crashinfo context section is missing some register values in the crashinfo file.

  Conditions: This symptom is observed after a Cisco 7600 series that runs Cisco IOS Release 12.2SR has crashed.

  Workaround: There is no workaround.

- CSCse52755

  Symptoms: An ELMI link between a PE router and CE router may remain down.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions as a PE router when the following conditions are present:

  – The PE router is configured with a SIP-400 that has a SPA with a Gigabit Ethernet interface that connects to the CE router.

  – The Gigabit Ethernet interface has an Xconnect-based Ethernet Virtual Circuit (EVC) configuration.

Workaround: On the PE router, enter the **ethernet cfm enable** global configuration command.

Further Problem Description: The symptom occurs because the ELMI packets that are sent by the CE router and are destined for the PE router are tunneled to a remote side instead of being punted to the RP of the CE router.

- CSCse60827

  Symptoms: An IKE/IPsec session fails when you use a TACACS server.

  Conditions: This symptom is observed on a Cisco router when PKI is configured along with AAA, as in the following example:

  ```
  ipsecn-7606a(config)#aaa authorization network <list-name> group tacacs+
  ipsecn-7606a(config)#crypto ca trustpoint <trustpoint-name>
  ipsecn-7606a(ca-trustpoint)#authorization list <list-name>
  ipsecn-7606a(ca-trustpoint)#authorization username subjectname country
  ipsecn-7606a(ca-trustpoint)#exit
  ```

  Workaround: There is no workaround. Note that the symptom does not occur when you use a RADIUS server.

- CSCse89100

  Symptoms: Key exchange fails during IKE negotiation at the “IKE_I_MM5” state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA and occurs only when the router is configured for NAT-T and VRF.

  Workaround: There is no workaround.

- CSCse98235

  Symptoms: Hardware-switched multicast traffic may be adversely affected by a subinterface configuration. When a large number of subinterfaces (about 1000) are disables and then enabled by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a physical interface, some of the subinterfaces are missing from the OIF list.

  Conditions: This symptom is observed on a 20-port Ethernet Services line card (7600-ES20-GE) that is installed in a Cisco 7600 series.

  Workaround: Enable the Consistency Checker.

- CSCsf20714

  Symptoms: A DHCP relay may crash at the “print_unaligned_summary” function while requesting an IP address from a DHCP client.

  Conditions: This symptom is observed on a Cisco router after the bridge group has changed from one group to another.

  Workaround: There is no workaround.

- CSCsg10531

  Symptoms: An “Invalid SPI” error message may be generated and packet loss may occur during an SA rekey.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with IPsec tunnels.

  Workaround: There is no workaround.

- CSCsg17537

  Symptoms: The memory consumption of NetFlow Data Export (NDE) is higher than it should be.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2SX or Release 12.2(33)SRB and that is configured for NetFlow.

Workaround: There is no workaround.

- CSCsg22169

  Symptoms: Memory consumption of the NetFlow Data Export (NDE) process is high.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

  Further Problem Description: The NDE process consumes about 133 KB for per-protocol queues. The fix for this caveat reduces the memory consumption to a little more than half the original usage.

- CSCsg26096

  Symptoms: When you enter the **hw-module reset** command on a 1-port CHOC-3/CHSTM-1 SPA that is installed in a Cisco 7600 series at the local end, the network clock at the remote end may become out-of-range (OOR), that is, the network clock goes beyond the acceptable limits of pps, without an error message being generated.

  Conditions: This symptom is observed when the Network Clocking feature is configured on the 1-port CHOC-3/CHSTM-1 SPA.

  Workaround: There is no workaround.

- CSCsg37644

  Symptoms: Cisco IOS SLB does not function when the client is located behind the MPLS cloud.

  Conditions: This symptom is observed on a Cisco 7600 series when the response packets to the client are forwarded over the MPLS tunnel interface.

  Workaround: There is no workaround.

- CSCsg40482

  Symptoms: ISDN L2 may remain in the “TEI_ASSIGNED” state.

  Conditions: This symptom is observed on a Cisco router after you have performed a hard OIR of a PA-MC-4T1 port adapter.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reload the router.

- CSCsg40573

  Symptoms: A Cisco 7600 series may enter a state in which the FIB is frozen, and the syslog may `show information similar to the following:`

  ```
  %MLSCEF-SP-2-SANITY_FAIL: Sanity Check of MLS FIB s/w structures failed
  %MLSCEF-SP-2-FREEZE: hardware switching disabled on card
  ```

  In this frozen state the data plane is not affected, but new forwarding information does not take effect on the hardware, causing an inconsistency between MPLS or IP software forwarding and the hardware.

  Conditions: This symptom is observed when the TCAM information for a label or prefix and mask does not match the software version, which prevents the TCAM driver from deleting the label or prefix and mask. For example, the symptom may occur when a label is moved from one type (for example, form an aggregate label) to another other type (for example, to a non-aggregate label).

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the router.

Further Problem Description: You can check the status of the FIB by entering the **show mls cef hardware | i TCAM** command. When the symptom has occurred, the output of this command shows the following:

```
CEF TCAM v3: (FROZEN)
```

- CSCsg42753

  Symptoms: Some MPLS TE tunnels may be resignaled on the tunnel headend following an SSO switchover.

  Conditions: This symptom is observed on a Cisco 7600 series that has dual RPs that function in SSO mode when and RSVP Graceful Restart is configured in full mode. The symptom occurs only when there are more than 200 tunnel headends established when the SSO switchover occurs.

  Workaround: There is no workaround.

  Further Problem Description: After the SSO switchover has occurred, the output of the **show ip rsvp high-availability counters** command shows that some LSPs failed recovery:

  ```
  LSPs for which recovery:
    Attempted: 600
    Succeeded: 595
    Failed:    5
  ```

  TE prevents new LSPs from being signaled during the RSVP HA recovery period immediately after the SSO switchover has occurred. For any TE tunnels that fail to recover, traffic that is routed onto those tunnels is dropped. However, the tunnels are resignaled after the RSVP HA recovery period, which may take up to two minutes.

- CSCsg42825

  Symptoms: When you attempt to configure more than 1056 traffic engineering (TE) tunnels, the following error message may be generated:

  ```
  "%ERROR: Standby does not support this command"
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when all tunnels are configured at once via a script or via a copy-and-paste operation of the configuration.

  Workaround: Provide an interval between each 10 tunnels so that the tunnels are not configured all at once.

- CSCsg47039

  Symptoms: After a Fast Reroute (FRR) event and multiple failure situations have occurred, any of the following line cards or port adapters may crash:

  – SIP-600

  – 2-port Ethernet Services line card (7600-ES20-10G)

  – 20-port Ethernet Services line card (7600-ES20-GE)

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for MPLS Traffic Engineering Fast Reroute--Link Protection when the line card or port adapter is processing incoming traffic from the MPLS core and when the following sequence of events occurs:

  – You remove the protected TE tunnel configuration from the protected interface.

  – You add back the protected TE tunnel configuration to the same interface.

  – You clear the fault that caused the FRR event.

  The crash occurs after OSPF and LDP are negotiated through the protected interface.

Workaround: After the FRR event has occurred, do not remove the protected TE tunnel configuration from the protected interface.

- CSCsg62226

  Symptoms: An active HSRP router may crash when you configure and unconfigure Hot Standby Router Protocol (HSRP) multiple times.

  Conditions: This symptom is observed when the active router and the standby router are configured with a single Front Door VRF (FVRF) and a single Inside VRF (IVRF), when routing through a GRE tunnel over a VTI occurs via EIGRP, and when the physical IP connectivity occurs via OSPF.

  Workaround: To prevent the symptom from occurring, do not configure and unconfigure HSRP multiple times, but reload the routers and reconfigure both of them.

- CSCsg64557

  Symptoms: The tunnel interface counter does not increment in tunnel protection mode.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with GRE tunnels when an IPsec VPN SPA (SPA-IPSEC-2G) processes the GRE tunnels and when the crypto functionality is configured for tunnel protection mode.

  Workaround: There is no workaround. However, to trace the packet path other interface counters (such as counter on the physical interface or VLAN interface) can be checked.

- CSCsg68406

  Symptoms: After a HA switchover occurs because you have entered the **issu runversion** command, a link flap may occur on the uplink ports of the newly active supervisor engine, causing traffic on these ports to be disrupted for several seconds and the following error message to be generated on the console:

  ```
  %EARL-SP-2-SWITCH_BUS_IDLE: Switching bus is idle for 10 seconds. The card grant is 7
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a certain combination of line cards and occurs only during the Enhanced Fast Software Upgrade (EFSU) process. In particular, the symptom is observed when the router has redundant Supervisor Engine 720 cards, one or more legacy line cards such as a WS-X6148-GE-TX, and one or more EFSU-enabled cards such as a WS-X6724-SFP.

  Workaround: There is no workaround.

- CSCsg78244

  Symptoms: You can still ping a Server Load Balancing (SLB) virtual IP (VIP) address after all of the real server in the serverfarm fail.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

  Further Problem Description: One example in which the symptom occurs is the following:

  When there is a redundant configuration of two SLBs devices with similar configurations and when the real servers that are bound to a virtual server in the primary connection fail, the secondary SLB device handles the connections. Even when the real servers that are bound to the virtual server in the primary SLB connection fail, you can still ping the VIP, which means that the virtual server is still in service. This situation causes traffic to continue to be routed to the VIP on the primary SLB device.

- CSCsg79129

  Symptoms: Multicast traffic may not be forwarded on a routed VPLS (R-VPLS) interface that is configured for PIM Sparse Mode (SM).

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-600 on which an RPF interface is configured and occur when egress replication mode is enabled.

  Workaround: Change the multicast replication mode from egress mode to ingress mode by entering the **mls ip multicast replication-mode ingress** command.

- CSCsg84374

  Symptoms: CPUHOG messages may be generated on the console of the RP when you run the cbQosPoliceCfg MIB object of the Cisco Class-Based QoS MIB.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a scaled configuration.

  Workaround: There is no workaround.

- CSCsg84522

  Symptoms: A router may crash because of ATM Inverse ARP (InARP) timer issues.

  Conditions: This symptom is observed on a Cisco router when you configure or deconfigure the InARP timer.

  Workaround: There is no workaround.

- CSCsg87290

  Symptoms: When you enter the **shutdown** command followed by the **no shutdown** command on the SONET controller of a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3), an extra flap occurs for T3 links that are configured on the SONET controller.

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

  Workaround: There is no workaround.

- CSCsg98041

  Symptoms: The TCP checksum is incorrect when both NAT-T and transport mode are configured.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB for TCP sessions that are terminated on the router.

  Workaround: Do not use transport ode. Rather, use tunnel mode.

  Alternate Workaround: Configure GRE keepalives on termination point (TP) tunnels to protect TCP traffic that is destined for the router.

- CSCsh02510

  Symptoms: A router crashes when you configure an Xconnect service on a main interface.

  Conditions: This symptom is observed on a Cisco router that has two or more L2VPN connections that are configured for Xconnect service on a subinterface of the main interface. Even after you have deleted the subinterface, the router crashes when you configure Xconnect service on the main interface.

  Workaround: There is no workaround.

  Further Problem Description: This symptom was initially observed on a Cisco 10000 series when you configured Xconnect service on a main interface of a 6-port channelized T3 line card or 4-port channelized STM-1/OC-3 line card. However, the symptom appeared to be platform-independent.

- CSCsh12653

  Symptoms: When an ISG receives VSAs that cannot be parsed by the SIP parser, the ISG disconnects the established session and does not respond with a CoA Nak message.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG when an incorrect VSA is sent via a CoA message and when the SIP parser returns a DENY message to the ISG.

  Following are examples of incorrect VSAs:

  – a vc-weight that is larger than the maximum that is allowed:
  cisco-avpair = “atm:vc-weight=3000”

  – a non-existent service-policy name:
  cisco-avpair = “atm:vc-qos-policy-out=non_exist_policy”
  cisco-avpair = “atm:vc-watermark-max=1”

  Workaround: There is no workaround.

- CSCsh16387

  Symptoms: When the default ACL of an interface is configured as a software bridge, all traffic that enters this interface is punted to the RP.

  Conditions: This symptom is observed when a Cisco 7600 series boots with a large number of VPN interfaces.

  Workaround: There is no workaround.

- CSCsh18070

  Symptoms: Routing protocols may flap on a service instance or routed VPLS (R-VPLS) interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured with an Ethernet Services (ES20) line card and any WAN module and/or SIP. The symptom occurs when the traffic through the service instance or R-VPLS interface exceeds the line rate in the egress direction or when the traffic exceeds the shape rate in the class-default class of an MQC policy.

  Workaround: There is no workaround. The symptom is less likely to occur when you reduce the traffic on the port to below the line rate or below the shaping rate.

  Further Problem Description: The symptom occurs because control packets are not treated as high-priority packets on the service instance or R-VPLS interface.

- CSCsh19574

  Symptoms: A Cisco 7600 series takes about 20 minutes to boot completely.

  Conditions: This symptom is observed when the router has a scaled subinterface configuration with 2000 to 4000 subinterfaces. The boot process is adversely affected when the **ip pim** command is configured on the subinterfaces.

  Workaround: There is no workaround.

- CSCsh20354

  1. Symptom 1: A third-party vendor VPN client may not be able to establish a VPN tunnel to a Cisco router. When you enable the **debug crypto isakmp** command on the Cisco router, the output shows the following:

     ```
     ISAKMP:(0:4:HW:2):No IP address pool defined for ISAKMP!
     ISAKMP:(0:4:HW:2):deleting SA reason "Fail to allocate ip address" state (R)
     CONF_ADDR     (peer x.x.x.x)
     ```

2. Symptom 2: Although a third-party vendor VPN client can establish a VPN tunnel to a Cisco router, the client receives only an IP address but no DNS configuration, split-tunnel information, or other data during the mode configuration phase. In this situation, the debug output does not show any errors.

Conditions: Both of these symptoms are observed only when a third-party vendor VPN client connects to a Cisco router that functions as a VPN server.

Workaround: There are no workarounds.

- CSCsh20479

  Symptoms: IP services that are configured on an active software EoMPLS VC may not process L3 control frames.

  Conditions: This symptom is observed on a Cisco router when an active software EoMPLS VC (that is, when an Xconnect statement is configured via an SVI/VLAN interface) is configured with an L3 IP address and L3 control frames such as L3 ARP or OSPF multicast frames.

  Workaround: Remove the SVI interface and recreate the SVI interface with the L3 IP address before you configure the EoMPLS xconnect statement. Doing so enables IP services first and then the EoMPLS VC, allowing both to function properly.

- CSCsh21398

  Symptoms: A Cisco 7600 series in which a WS-F6700-DFC3BXL module with 256 MB of memory is installed may run out of memory and display memory allocation failure messages such as the following:

```
%SYS-DFC2-2-MALLOCFAIL: Memory allocation of 4188 bytes failed from 0x205336A0,
alignment 0 Pool: Processor  Free: 56780  Cause: Memory fragmentation

Alternate Pool: None  Free: 0  Cause: No Alternate pool

 -Process= "XDR LC Background", ipl= 0, pid= 181

 -Traceback= 20412DD8 2041331C 2050227C 2050BD08 205336A8 211642AC 2113B39C 211393B4
2114C100 2114ADBC 2113721C 21137354 2113794C 21137CE8 211B7C78 21202F10

%FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2): CEF-Common: no memory

%ADJ-DFC2-3-ALLOCATEFAIL: Failed to allocate an adjacency

-Traceback= 20412DD8 2041331C 211A3DE0 211A4414 21129664 21129850 21139294 211393A4
2114C100 2114ADBC 21e1 3t7o2 1aC  f2a1tal err1or.37354 2113794C 21137CE8 211B7C78
21202F10

%COMMON_FIB-DFC2-3-NOMEM: Memory allocation failure for path list in Common CEF
[0x21139490] (fatal) (0 subsequent failures).

%COMMON_FIB-DFC2-4-DISABLING: Common CEF is being disabled due to a fatal error.

%FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2): CEF-Common: no memory

%XDR-DFC2-6-XDRLCDISABLEREQUEST: Client CEF push requested to be disabled.

-Traceback= 20412DD8 2041331C 21217E98 211B0C48 211B3760 21155594 21159FF4 21153D4C
21153F10 204F6448 204F6434

%COMMON_FIB-DFC2-4-DISABLING: Common CEF is being disabled due to a fatal error.
```

  Conditions: This symptom is observed in a scaled configuration (which is typical of broadband deployments) when 28,000 access subinterfaces are created and brought up.

  Workaround: There is no workaround.

- CSCsh22171

  Symptoms: After an MPLS-TE path is rerouted, the Virtual Private LAN Services (VPLS) feature stops decapsulating Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames that are received from a remote PE router. This situation may result in an STP loop.

Conditions: This symptom is observed on a Cisco 7600 series that functions as a PE router in an MPLS network, that has many MPLS-TE tunnels configured, and that has the **l2protocol-tunnel stp** command enabled.

Workaround: Enter the **no l2protocol-tunnel stp** command.

- CSCsh22671

  Symptoms: IPsec security associations (SAs) may not be deleted from a spoke.

  Conditions: This symptom is observed when the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command is entered on the interface of the hub that is connected to the spoke.

  Workaround: Enter the **clear crypto sessions** command on the spoke.

- CSCsh23176

  Symptoms: A router crashes when you unconfigure RIP.

  Conditions: This symptom is observed on a Cisco router and is more likely to occur when there are many RIP routes configured.

  Workaround: Remove all network statements that are defined under the **router rip** command, wait for all RIP routes to age-out, then remove the **router rip** command.

- CSCsh31679

  Symptoms: PVCs that are configured on MFR interfaces may become inactive for some time after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the active supervisor engine crashes and causes an SSO switchover to occur.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, note that the PVCs do come up after some time. Otherwise, reset the affected line cards.

- CSCsh34529

  Symptoms: An ATM interface configuration may become lost on the standby RP.

  Conditions: This symptom is observed on a Cisco 7600 series when you perform the following steps:

  1. You configure an ATM main interface on a SPA.
  2. You configure PVCs on the ATM main interface.
  3. You shut down the SPA.
  4. You reload the standby supervisor engine and wait until it comes up.
  5. You bring up the SPA from the active RP.

  At this point, the ATM interface configuration is lost on the standby RP.

  This symptom is observed with both 8-port OC-3c/STM-1 ATM SPAs and Circuit Emulation over Packet (CEoP) SPAs.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the standby supervisor engine once more.

- CSCsh34536

  Symptoms: A Circuit Emulation (CEM) group configuration may become lost on the standby RP.

Conditions: This symptom is observed on a Cisco 7600 series when you perform the following steps:

1. You configure a CEM interface and groups on a Circuit Emulation over Packet (CEoP) SPA.
2. You shut down the SPA.
3. You reload the standby supervisor engine and wait until it comes up.
4. You bring up the SPA from the active RP.

At this point, the CEM group configuration is lost on the standby RP.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the standby supervisor engine once more.

- CSCsh35236

  Symptoms: A 20-port Ethernet Services line card (7600-ES20-GE) may crash and a "mac_xid=0x10000" PXF exception may be generated.

  Conditions: This symptom is observed on a Cisco 7600 series under a rare condition when a specific (test) source MAC address triggers the crash and when the router function under stress.

  Workaround: There is no workaround.

- CSCsh35451

  Symptoms: In an HA configuration when the router is in the runversion-switchover state, when you enter the **issu runversion** command, the newly active supervisor engine does not come up fully and causes the standby supervisor engine to crash with "Active_Not_Responding" error messages.

  Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

  1. You enter the **issu loadversion** command, and you wait for the router to enter the terminal state.
  2. You enter the **issu runversion** command, and you wait for the router to enter the terminal state.
  3. The active supervisor engine crashes, and then moves to the RunVersionSwitchOver (RVSO) state.
  4. The newly active RP and standby RP come up, and you wait for the router to enter the terminal state.
  5. Again, you enter the **issu runversion** command on the active supervisor engine.

  At this point, the symptom occurs.

  Workaround: There is no workaround.

- CSCsh36614

  Symptoms: When Server Load Balancing (SLB) is configured and when policy-based routing is applied to the outbound path, the first response packet (that is, the syn-ack packet) from the real server is process-switched instead of switched via the special switching path.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 720.

  Workaround: There is no workaround.

- CSCsh37219

  Symptoms: IPv6 multicast convergence takes 25 to 30 minutes on a Route Switch Processor 720 when an ATM interface on a SIP-200 functions as the uplink between the two routers.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with 32,000 (S,G) entries with 4000 groups from four sources and 16,000 packets per burst with packets that have a size of 64-bytes.

Workaround: There is no workaround.

- CSCsh39318

  Symptoms: A router may crash when the configured route limit is exceeded. When this situation occurs, the following error message is generated:

  ```
  %MROUTE-4-ROUTELIMIT (x1): [int] routes exceeded multicast route-limit of [dec] - VRF
  [chars]
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multicast VPN but is platform-independent.

  Workaround: There is no workaround.

- CSCsh40540

  Symptoms: When a service instance is configured for Xconnect, the pseudowire fails to come up, and an "%SW_MGR-SP-3-CM_ERR" error message is displayed.

  Conditions: The symptom is observed on a Cisco 7600 series only when encapsulation is configured as default.

  Workaround: There is no workaround.

- CSCsh40567

  Symptoms: When OAM cells are transported over a local-switched connection that is configured for AAL5 and for which the VPI or VCI do not match at both endpoints, OAM cells are dropped.

  Conditions: This symptom is observed on a Cisco 7600 series on an ATM SPA that is installed in a SIP-200 or on an ATM port adapter that is installed in a FlexWAN or Enhanced FlexWAN module.

  Workaround: Ensure that the VPI or VCI are the same at both endpoints of the local-switched connection.

- CSCsh45829

  Symptoms: An interface that is configured for Xconnect fails to come up.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a Supervisor Engine 32 and that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsh45862

  Symptoms: When a 24-port channelized T1/E1/J1 ATM CEoP SPA (SPA-24CHT1-CE-ATM) that functions ATM mode is heavily oversubscribed with traffic in one direction (either ingress or egress), the SPA may block all ping packets while still allowing other traffic to pass through. When this situation occurs, interfaces remain up, and there are no other error signals.

  Conditions: This symptom is observed on a Cisco 7600 series and is likely to occur with small packets such as 46-byte packets of an L3 payload.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the SPA by entering the **hw-module subslot** *slot*/*subslot* **reload** command.

- CSCsh46540

  Symptoms: A router crashes when the **format disk0:** and **copy tftp: disk0:** commands are executed in parallel.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system when the commands are entered through two different sessions.

  Workaround: Do not enter the above-mentioned commands in parallel.

- CSCsh47823

  Symptoms: CPU usage may become very high. When this situation occurs, a line card may become unable to respond to keepalive polling from the supervisor engine, and the Switch Processor (SP) may reset the line card.

  Conditions: This symptom is observed on a Cisco 7600 series that has a scaled QoS configuration when the Route Processor (RP) sends many configuration changes to the line card.

  Workaround: On both the RP and the SP, disable resetting of the line card for keepalive response failures. On the RP, enter the **test scp linecard keepalive disable** command; on the SP, enter the **debug oir no-reset-on-crash** *slot* command.

- CSCsh48705

  Symptoms: VPLS traffic may be dropped from the egress path on a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series when the VPLS traffic passes through a traffic engineering tunnel that is protected by FRR. The primary tunnel is on the SIP-400; the backup tunnel is on another line card. The symptom occurs when the following events take place:

  After you have configured FRR and reset the SIP-400, FRR switching occurs and the VPLS traffic is switched to the backup tunnel on the other line card. When the SIP-400 boots, the VPLS traffic is switched back to the primary tunnel as a result of L3 MPLS reconvergence. However, from this time on, the VPLS traffic is dropped from the egress path on the SIP-400.

  Workaround: Remove the FRR configuration, reset the SIP-400, and reconfigure the FRR configuration.

- CSCsh50878

  Symptoms: When a 4-port T3/E3 serial SPA initialization does not complete, a configuration synchronization mismatch may occur and the standby supervisor engine may reload.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for SSO and occurs after the router has been reloaded multiple times.

  Workaround: While the standby supervisor engine is coming up, enter the **redundancy config-sync ignore mismatched-commands** command on the active supervisor engine.

- CSCsh51688

  Symptoms: A Cisco 7600 series may crash unexpectedly because of a bus error on the Switch Processor (SP). The following error message may be generated prior to the crash:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x40B450D4
  ```

  Conditions: This symptom is observed on a Cisco 7600 series and the trigger is currently not known.

  Workaround: There is no workaround.

- CSCsh52183

  Symptoms: OSPF VRF processes may consume most of the system memory. Commands such as the **show running-config** command and **show process cpu sorted** do not function.

  Conditions: This symptom is observed on a Cisco 7600 series when OSPF is configured on inside VRFs (IVRFs), front-door VRFs (FVRFs), and Virtual Tunnel Interfaces (VTIs). The more tunnels there are, the earlier the symptom occurs.

  Workaround: Configure only a few OSPF routes in a configuration with IVRFs, FVRFs, and VTIs.

  Alternate workaround: Do not use OSFP, Rather, use EIGRP.

- CSCsh52354

  Symptoms: When you change the **encapsulation dot1q** command from a dual VLAN configuration to a single VLAN configuration by entering the **rewrite ingress tag pop 2 symmetric** command specified for a service instance, the command may be rejected and the standby supervisor engine may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7600 series when a service instance is configured in the following way:

  ```
  service instance <x> ethernet
  encapsulation dot1q <vlan-id> second-dot1q <vlan-id>
  rewrite ingress tag pop 2 symmetric
  ```

  Workaround: Disable the **rewrite** command before you change the **encapsulation dot1q** command.

- CSCsh52364

  Symptoms: A 24-port channelized T1/E1 CEoP SPA may not frame its T1 lines properly, causing path code violations to be generated at the remote end.

  Conditions: This symptom is observed on a Cisco 7600 series under rare conditions when the SPA is reloaded. The symptom may not occur with a few pings but could occur when traffic is being processed.

  Workaround: Shut down and bring up the affected port:

  conf t
  controller *(t1|e1) slot/bay/port*
  shutdown
  no shutdown
  exit

- CSCsh53802

  Symptoms: When the PBR Support for Multiple Tracking Options feature is enabled via the **set ip next-hop verify-availability** command and when the first next hop goes down, the router sets the second next hop in software rather than in hardware, even if the second next hop is up and available.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have at least two next hops.

  Workaround: There is no workaround.

- CSCsh54054

  Symptoms: When a 24-port channelized T1/E1/J1 ATM CEoP SPA (SPA-24CHT1-CE-ATM) that functions ATM mode is heavily oversubscribed with traffic in both the ingress and egress directions, the SPA may generate the following error message and then resets:

  ```
  %SPA_PLIM-3-ERRMSG: SPA-24CHT1-CE-ATM[3/2] (CEMA_INT-3-FATAL_INTERRUPT: Fatal
  Winpath Packet Bus Error interrupt: Bus Error: 8-byte read from 0x401b4000 generated
  by WMM TRS: 1 pc:0x3438 data: r64 address: r58)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series and is likely to occur with packets with sizes of 235 or 265 bytes (that is, L3 payload-size packets).

  Workaround: There is no workaround. However, the symptom corrects itself because the SPA is automatically reset.

- CSCsh54380

  Symptoms: After Fast Reroute (FRR) has rerouted traffic over a backup traffic engineering (TE) tunnel, VCs on an Ethernet Services (ES20) line card may not generate correct statistics.

Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-600 in which an ES20 line card is installed that is configured for VPLS EoMPLS in a highly scaled configuration with a large number of VPLS VCs that are protected by FRR. The symptom occurs in the following configuration scenarios:

When one interface of the TE tunnel (either the interface for the primary or the backup tunnel) is configured on:

- a port on a SIP-600, or
- a port from 0 through 19 on a 20-port ES20 line card (7600-ES20-GE), or
- the first port (that is, port 0) on a 2-port version ES20 line card (7600-ES20-10G),

and when the other interface of the TE tunnel (either the interface for the primary or the backup tunnel) is configured on:

- a port from 0 through 19 on a 7600-ES20-GE, or
- the second port (that is, port 1) on a 7600-ES20-10G.

Workaround: There is no workaround.

- CSCsh55166

  Symptoms: PIM neighbors on a core interface become lost when traffic is sent.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a Routed VPLS (R-VPLS) environment when the core interface has PIM enabled but when a switched virtual interface (SVI) that is also configured for R-VPLS does not have PIM enabled.

  Workaround: Configure PIM on the SVI.

- CSCsh56121

  Symptoms: After you have reloaded a Cisco 7600 series that has redundant supervisor engines, or after you have forced a redundancy switchover, the RSA key on the standby supervisor engine may be lost.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the RSA key.

- CSCsh56902

  Symptoms: The output of the **show mls cef** command shows a hidden VLAN instead of an interface as a VRF tag:

  ```
  1025 === tegigX/X
  ```

  output

  ```
  X.X.X.... VRF1025 x.x.x.x
  ```

  should be...

  ```
  X.X.X... tegigX/X x.x.x.x
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: Reload the router or shut down and bring up the affected interface. The symptom does not affect proper functionality of the router.

- CSCsh58526

  Symptoms: When the number of Ethernet Virtual Connections (EVCs) exceeds 1000, EVCs flap and the CPU usage in the “Ethernet CFM” process is significantly higher.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the number of EVCs is in the range of 4000.

  Workaround: Ensure that the number of EVCs is 1000 or smaller.

- CSCsh60202

  Symptoms: Routed VPLS (R-VPLS) multicast packets may flood a SIP-400 on which Ethernet Virtual Circuit (EVC) service instances are configured and may egress the service instances.

  Conditions: This symptom is observed on a Cisco 7600 series when a bridge-domain VLAN matches the R-VPLS switched virtual interface (SVI).

  Workaround: There is no workaround.

- CSCsh61851

  Symptoms: A PIM neighborship does not come up on an MDT tunnel when VRFs are removed and added back immediately on PE routers.

  Conditions: This symptom is observed on Cisco 7600 series routers that run Cisco IOS Release 12.2(33)SRB.

  Workaround: Wait for 3 to 4 minutes after you have removed the VRFs on the PE routers so that the backbone entries that are associated with the VRFs expire. Then, add back the VRFs.

  Further Problem Description: The VPN ID is not re-used when a VRF is removed and recreated. This situation results in stale VPN information on the supervisor engine and DFC because backbone entries that are associated with the old VRF can exist until they expire. When a new VPN ID is issued because you recreate the VRF, the hardware entry may not be programmed correctly because of the stale VPN information, preventing the PIM neighborship from being established over the MDT tunnel.

- CSCsh61926

  Symptoms: The following error message may be generated appears on a Cisco router that is configured for MPLS:

  ```
  LSD_HA-3-GENERAL: Cannot chkpt now
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a large number of VRFs.

  Workaround: There is no workaround.

- CSCsh62612

  Symptoms: A standby supervisor engine may reload continuously while attempting to boot after a supervisor engine switchover has occurred. In this situation, the active supervisor engine functions fine.

  Conditions: This symptom is observed during the bulk synchronization of a configuration from the active supervisor engine to the new standby supervisor engine while the standby supervisor engine comes up after a supervisor engine switchover has occurred.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reload both the active and standby supervisor engines.

- CSCsh64335

  Symptoms: A router may crash when you enter the **mkdir** command to create a directory with a length of more than 127 characters and when you query this directory via SNMP.

Conditions: This symptom is observed on a Cisco router that has an ATA file system.

Workaround: There is no workaround.

- CSCsh65083

  Symptoms: A Circuit Emulation over Packet (CEoP) SPA may reload when an SSO switchover or APS switchover occurs. Note that the SPA functions normally after it has reloaded.

  Conditions: This symptom is observed on a Cisco 7600 series when the following conditions are met:

  – Both Circuit Emulation (CEM) and ATM are configured on the SPA.
  – ATM traffic is being processed on the SPA.
  – Multiple SSO or APS switchovers occur.

  Workaround: Avoid multiple SSO or APS switchovers.

- CSCsh65322

  Symptoms: A Cisco 7600 series with an Enhanced FlexWAN in which a PA-A3-OC3SMI port adapter is installed may drop packets steadily from the ATM interface. This situation may be verified under the “Total output drops” in the output of the **show interfaces atm** command.

  Conditions: This symptom is observed when the router is configured for PPPoA connections. There is no correlation between the packet drops on the interface and any particular ATM PVCs or virtual-access interfaces.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur with a FlexWAN.

- CSCsh67160

  Symptoms: CEF consistency checkers may become disabled, and the following message may be generated:

  ```
  %CEF consistency checkers currently offline (Switchover in progress)
  ```

  Conditions: This symptom is observed on a Cisco router that has the **ip cef** command enabled when an SSO switchover occurs. The symptom does not occur when the **ipv6 cef** command is enabled.

  Workaround: Do not enter the **ip cef** command. Rather, enter the **ipv6 cef** command.

- CSCsh69341

  Symptoms: In a Server Load Balancing (SLB) configuration, input features (except for Policy Based Routing [PBR]) that should not be processed are unexpectedly executed in a special switching path.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch that runs Cisco IOS Release 12.2SXH and Cisco 7600 series that runs Release 12.2SXH or Release 12.2(33)SRB and that are configured with a Supervisor Engine 720.

  Workaround: There is no workaround.

  Further Problem Description: The symptom may cause SLB to behave in an unexpected way. For example, when an input access control list (ACL) is applied on an interface, SLB is supposed to bypass the ACL, which is considered an input feature, so SLB packets can reach their destination without a problem. However, because of the symptom, the ACL is active and may stop SLB packets from reaching their destination.

- CSCsh72267

  Symptoms: A PVC that is configured on an ATM interface that is configured for cell packing may not receive the MNCP and MCPT parameters from the ATM interface. (MNCP = Maximum cells packed in one MPLS packet; MCPT = Maximum time to wait to pack the cells in one MPLS packet.)

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB but is platform-independent.

Workaround: Do not configure cell packing on the ATM interface. Rather, configure cell packing directly on the PVC.

- CSCsh72329

  Symptoms: When APS is triggered by a soft OIR of a working 1-port channelized OC-3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM), some of the CEM VCs may take more than 150 seconds to come up. Because of this situation, there may be a delay in traffic recovery following the APS switchover.

  Conditions: This symptom is observed on a Cisco 7600 series when you perform a soft OIR on the SPA-1CHOC3-CE-ATM by entering the **hw-module subslot** *slot/subslot* **reload** command.

  Workaround: There is no workaround. However, the router recovers automatically.

- CSCsh72407

  Symptoms: When cell packing is configured on a PVP between two PE routers, the MNCP parameter is not exchanged over an AToM L2TPv3 connection. The PE router shows that the MNCP of the peer is 1, but this should be a greater value. (MNCP = Maximum cells packed in one MPLS packet.)

  Note that a ping from one PE router to the other works fine, the Layer 2 tunnel is up, and the connection between CE routers work fine.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for Xconnect. The symptom is platform-independent.

  Workaround: Do not use an L2TPv3 connection. Rather, use an MPLS connection. If this is not an option, there is no workaround.

- CSCsh73675

  Symptoms: An Ethernet Virtual Connection (EVC) that is configured for EoMPLS or another feature may not pass traffic after the router has been reloaded.

  Conditions: This symptom is observed on a Cisco 7600 series with a scalable EVC configuration of 16,000 EVCs on the same Ethernet Services (ES20) line card. The symptom occurs very rarely and is related to a peculiar timing issue.

  Workaround: There is no workaround.

- CSCsh73935

  Symptoms: A router may reload when you perform an snmpwalk on the ciscoMvpnMrouteMdtTable.

  Conditions: This symptom is observed when all of the following conditions are present:

  – IP multicast routing is enabled on a VPN routing/forwarding instance (VRF)

  – This VRF is associated with an interface.

  – The Multicast Distribution Tree (MDT) default group address is not configured for the VRF.

  Workaround: Configure the MDT default group address for the VRF by entering the **mdt default** *mdt group* command in VRF configuration mode.

- CSCsh74127

  Symptoms: ISIS adjacencies may not be established.

Conditions: This symptom is observed on a Cisco 7600 series where the ISIS adjacency is configured to be established over an Ethernet Services (7600 ES20) line card with QinQ subinterfaces that are configured to support double-tagged packets when the default MTU size is 1500 bytes.

Workaround: Configure the MTU to be 1504 bytes.

- CSCsh75001

  Symptoms: After a SIP-400 or the router reloads, interfaces remain down until you enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-400 in which the following SPAs are installed:

  – a 2-port GE SPA (SPA-2X1GE)

  – a 1-port channelized OC-3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM)

  The interfaces of these SPA are configured with more than 3000 Ethernet Virtual Connection (EVC) flexible instances that are configured for QoS.

  Workaround: There is no workaround.

  Further Problem Description: Configuring more than 3000 EVC instances with QoS on a SIP-400 in which both a SPA-2X1GE and a SPA-1CHOC3-CE-ATM are installed is not supported. A large configuration of EVC instances with QoS can be achieved only without a SPA-1CHOC3-CE-ATM in the SIP-400 in which the SPA-2X1GE is installed.

- CSCsh75176

  Symptoms: A standby RP with a VRF configuration may reload continuously.

  Conditions: This symptom is observed on a Cisco router that is configured for SSO.

  Workaround: There is no workaround.

- CSCsh75457

  Symptoms: The RP may crash during the boot process of the router.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured with QoS service policies.

  Workaround: There is no workaround.

- CSCsh78154

  Symptoms: When an interface on a SIP-400 has many subinterfaces with QoS input policies configured, some packets may drop in the form of input errors. The drop rate is very low, typically less than 0.001 percent.

  Conditions: This symptom is observed on a Cisco 7600 series and occurs on Gigabit Ethernet (GE) and POS interfaces (but not on ATM interfaces) when the following conditions are met:

  – The interface has a few hundred subinterfaces per port, each configured with a QoS input policy.

  – Small- to medium-sized packets up to 500 bytes are processed.

  – A moderate to heavy traffic volume is processed. The volume depends on the packet size, for example: 64-byte packets at about 20 percent of the GE line rate, 128-bype packets at about 50 percent of the GE line rate, 256-byte packets at about 85 percent of the GE line rate, and so on.

  Workaround: There is no workaround. The packet drop rate is unnoticeably low, but detectable in performance tests.

- CSCsh80337

  Symptoms: An exception may occur on the active and standby Supervisor Engine 720 modules, they enter ROMmon, and all configurations may become lost.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the following conditions occur:

  1. There is one Supervisor Engine 720 in the chassis.
  2. You insert another Supervisor Engine 720 that contains another Cisco IOS software image into the chassis. The compact flash on this supervisor engine is replaced with another one that also contains Cisco IOS Release 12.2(33)SRB.
  3. You attempt to boot the newly inserted Supervisor Engine 720 as the standby supervisor engine with Release 12.2(33)SRB, it encounters an exception, and enters ROMmon.
  4. The active Supervisor Engine 720 also encounters en exception and enters ROMmon.
  5. You boot the active Supervisor Engine 720 manually.

  At this point, all configurations become lost.

  Workaround: There is no workaround.

- CSCsh83467

  Symptoms: A standby Supervisor Engine 720 may reset when an entire Circuit Emulation (CEM) configuration is removed and then reconfigured.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the **recovered-clock** command is present in the removed configuration.

  Workaround: Do not remove an entire CEM configuration.

  Alternate Workaround: Disable the **recovered-clock** command before you remove and then reconfigure an entire CEM configuration.

- CSCsh84531

  Symptoms: After an SSO switchover has occurred, a large number of Circuit Emulation (CEM) circuits may remain down.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SIP-400 in which a Circuit Emulation over Packet (CEoP) SPA is installed when the router has a very high CPU usage during the SSO switchover.

  Workaround: There is no workaround to prevent the symptom from occurring. Perform a software or hardware OIR of the SIP-400 to recover the CEM circuits.

- CSCsh90556

  Symptoms: Traffic may fail to match the VLAN TCAM, causing traffic to be dropped from a SPA that is installed in a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series when an Xconnect service is configured and when double-tagged frames are sent via a service instance that is configured with single-tag encapsulation.

  Workaround: Configure two service instances, as in the following examples:

  – A service instance to handle single-tagged packets with VLAN ID = 100:

    ```
    service instance 10 ethernet
    encapsulation dot1q 100
    ```

  - A service instance to handle double-tagged packets with the outer tag = 100:

    service instance *20* **ethernet**

    encapsulation dot1q *100* **second-dot1q** *any*

- CSCsh90762

  Symptoms: The hardware adjacencies that correspond to 6PE aggregate labels may be wrongly programmed.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a 6PE router.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interfaces that are associated with the IPv6 prefixes that correspond to the affected 6PE aggregate labels.

- CSCuk60927

  Symptoms: A variety of symptoms may occur on a Cisco router such as a Cisco 7600 series that is configured for distributed CEF (dCEF) switching because of loss of interprocess communication (IPC) messages between line cards and the RP. These symptoms may include the following:

  - Disabling of dCEF switching on the line card after the router has booted or after an SSO switchover, microcode reload, or OIR.
  - Loss of statistics from the line cards.

  Conditions: This symptom is observed only when either there are high quantities of statistics being reported (for example, for very large numbers of AToM endpoints) or when the router synchronizes a very large configuration to the standby RP during the boot process.

  Workaround: In most conditions, entering the **clear cef linecard** command re-enables the line cards.

  Further Problem Description: IPC messages are used for a variety of purposes: most commonly for statistics reporting, but also when a line card is brought up and when dCEF is enabled. The loss of these IPC messages gives rise to one of the symptoms. The probability of drops occurring is normally negligible except in situations in which there is a very high volume of IPC traffic. This high traffic volume may occur when the router synchronizes large configurations to the standby RP and also when extremely large numbers of statistics are sent via IPC.

  Note Note: NetFlow statistics are not sent via IPC and are therefore not affected by nor do they trigger the symptoms.

- CSCuk61396

  Symptoms: WCCP service redirection may not work. In particular, packets that are rejected by a third-party vendor appliance device and are returned to the router for normal forwarding may be discarded.

  Conditions: This symptom is observed on a Cisco router when NAT or Cisco IOS Firewall features are enabled on the same interfaces that have WCCP enabled.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCee32814

  Symptoms: Port numbers for TCP connections originating from the router are chosen in an incremental way making it easy to predict them.

Conditions: Any TCP connection on the router using non-well-known port numbers is subject to this behavior.

Workaround: There is no workaround.

- CSCsh36234

  Symptoms: File paths that start with a double slash may fail to open the file successfully.

  Conditions: This symptom is observed when you enter the **install** command with the **scp** keyword, that is when an SCP application functions as the source.

  Workaround: Move the file to another location where the double slash is not required.

  Alternate Workaround: Use another protocol such as RCP or TFTP to transfer the file.

Wide-Area Networking

- CSCek64788

  Symptoms: A router crashes because of memory corruption. The crashinfo points to the VPDN call manager.

  Conditions: This symptom is observed on a Cisco router when L2TP Active Discovery Relay for PPPoE is enabled.

  Workaround: There is no workaround.

- CSCsg90645

  Symptoms: In an L2TP Dial-Out configuration with a RADIUS or TACACS server for AAA services, the remote name is wrongly mapped to the secondary IP address of the LNS instead of to the primary IP address.

  Conditions: This symptom is observed on a Cisco router that is configured for VPDN. Note that local authentication and authorization function fine.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRB

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SRB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdy11174

  Symptoms: Some object of the ciscoFlashCopyTable and ciscoFlashMiscOpTable cannot be read after row creation.

  Conditions: This symptom is observed for any newly created rows in these tables.

  Workaround: Objects will become readable immediately after being set. Additionally, rows can still be activated in these tables even if all objects cannot be read. Any objects that cannot be read contain their MIB-defined default value.

- CSCeh85133

  Symptoms: A memory leak may occur when an SNMP trap is sent to a VRF destination. The output of the **show processes memory** command shows that the memory that is held by the process that creates the trap increases, and eventually causes a MALLOC failure. When this situation occurs, you must reload the platform.

  Conditions: This symptom is platform-independent and occurs in a configuration in which at least one VRF destination has the **snmp-server host** command enabled.

  Workaround: Ensure that no VRF is associated with the **snmp-server host** command.

- CSCei37916

  Symptoms: A Cisco GGSN does not function properly when wait-accounting and AAA Broadcast Accounting are configured on an APN. When the first RADIUS server responds to an Accounting Start message, the GGSN establishes the PDP context without waiting for responses from all other RADIUS servers. Under a stress condition, the GGSN may reload.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 and GGSN Release 5.2 and occurs only when both wait-accounting and AAA Broadcast Accounting are configured together on an APN. Note that the symptom is not release-specific.

  Workaround: There is no workaround.

- CSCej42445

  Symptoms: MS-CHAP authentication or MS-CHAP and PAP authentication may fail.

  Conditions: This symptom is observed on a Cisco router that is configured to use TACACS+ and MS-CHAP for authentication.

  Workaround: There is no workaround.

- CSCek33076

  Symptoms: A RADIUS progress code is incorrectly reported for a call that fails at IPCP. The progress code reports that the Link Control Protocol (LCP) is the open state.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4(3a) and that is configured for AAA. The symptom is not release-specific.

  Workaround: There is no workaround.

- CSCek37174

  Symptoms: When you configure RADIUS servers via the AAA-SERVER-MIB, the expected behavior is that the last defined RADIUS server receives the lowest priority, but this does not occur.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA and that runs Cisco IOS Release 12.4 or Release 12.4T. However, the symptom is release-independent.

  Workaround: There is no workaround.

- CSCek52249

  Symptoms: A Cisco router crashes when the **default dest-ip** command is entered in IPSLA jitter, UDP Echo and TCP Connect operations.

  Conditions: The issue is seen when the **default dest-ip** command is entered.

  Workaround: There is no workaround.

- CSCek58338

  Symptoms: A Cisco 7600 series may crash because of memory corruption in the chunk memory.

Conditions: This symptom is observed when both the Embedded Resource Manager (ERM) and Bidirectional Forwarding Detection (BFD) are configured.

Workaround: Disable BFD.

- CSCin60071

  Symptoms: After tunnel sessions have flapped on an L2TP Access Concentrator (LAC) or an L2TP Network Server (LNS), the sessions may be re-established on the wrong tunnels.

  Conditions: This symptom is observed when there is a high call rate and a high call volume.

  Workaround: Enable the **radius-server source-ports extended** global configuration command.

- CSCin99433

  Symptoms: Without configuring any command related to Kerberos other than a Kerberos password command, a configuration synchronization failure may occur because of a PRC mismatch.

  Conditions: This symptom is observed when you boot a Cisco router that is configured for AAA.

  Workaround: There is no workaround.

- CSCsa43465

  Symptoms: Users may be able to access root view mode (privilege level) 15 without entering a password.

  Conditions: This symptom is observed on a Cisco router that has the Role-Based CLI Access feature enabled and occurs when the **none** keyword is enabled in the default login method list.

  For example, the symptom may occur when you enter the **aaa authentication login default group tacacs+ none**. When the TACACS+ server is down, users are allowed to enter non-privileged mode. However, users can also access the root view through the **enable view** command without having to enter a password.

  Workaround: Ensure that the **none** keyword is not part of the default login method list.

  Further Problem Description: The fix for this caveat places the authentication of the **enable view** command in the default login method list.

- CSCsb08386

  Symptoms: A router crashes when you enter the **show ip bgp regexp** command.

  Conditions: This symptom is observed on a Cisco router when BGP is being updated.

  Workaround: Enable the new deterministic regular expression engine by entering the **bgp regexp deterministic** command and then enter the **show ip regexp** command. Note that enabling the new deterministic regular expression engine may impact the performance speed of the router.

- CSCsb30875

  Symptoms: When the **aaa accounting system** command is enabled, the active RP may hang after an RPR+ switchover has occurred.

  Conditions: The symptom is observed on a Cisco gateway or router when the console session is closed and reopened for the newly active RP after the RPR+ switchover has occurred.

  Workaround: Do not close and reopen the console session for the newly active RP.

  Alternate Workaround: Disable the **aaa accounting system** command.

- CSCsb89847

  Symptoms: Source and destination Border Gateway Protocol (BGP) autonomous system (AS) information may not be properly updated.

  Conditions: This symptom is observed on a Cisco router that is configured for MSDP and NetFlow.

Workaround: There is no workaround.

- CSCsd10306

  Symptoms: IP SLA packets may be dropped in a network. These dropped packets may also cause a buffer leak on some Cisco routers. The frequency of the symptom is very low; less then 1 percent of the IP SLA packets are dropped.

  Conditions: This symptom is observed for IP SLA packets to which an MPLS label is applied on the source router.

  Workaround: There is no workaround.

  Further Problem Description: The IP SLA packets that are dropped have a corrupted IP header.

- CSCsd26248

  Symptoms: A memory leak may occur in the RADIUS process on a router that is configured for dot1x authentication but that does not have the **aaa authentication dot1x** command enabled. The memory leak may consume all free memory.

  Conditions: This symptom is observed when the router receives attribute 24 (state) or attribute 25 (class) from a RADIUS server.

  Workaround: There is no workaround.

- CSCsd37284

  Symptoms: A router may crash when you use Remote Network Monitoring (RMON) to copy a configuration to the running configuration.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCeg74543. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74543. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCse08044

  Symptoms: A Cisco router may generate export packets in which the first flow record contains incorrect data such as incorrect IP addresses.

  Conditions: This symptom is observed on a Cisco router that is configured for NetFlow and NetFlow Data Export.

  Workaround: Disable NetFlow.

- CSCse10074

  Symptoms: The active RP may crash when traps are sent to a host to which an SNMPv3 user is assigned.

  Conditions: This symptom is observed only when an SNMPv3 user is configured with security level noAuthNoPriv or authPriv, when the same SNMPv3 user is assigned to the host through the **snmp-server host** command, and when this command includes the **priv** keyword. This is an improper configuration.

  For example, the symptom occurs when traps are triggered after the following software configurations has been applied:

  ```
  snmp-server user TESTUSER TESTUSER v3
  snmp-server group TESTUSER v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
  ```

```
snmp-server host 10.1.1.10 version 3 priv TESTUSER
snmp-server enable traps
```

Workaround: Do not create an improper configuration.

- CSCse38956

  Symptoms: A router crashes when you change the authentication method after the user on the client side has entered the user name and is prompted to enter the password but has not yet entered the password.

  Conditions: This symptom is observed when you disable the **aaa authentication enable default group radius** command and enable the **aaa authentication enable default group tacacs** command, or the other way around, before the user on the client side has entered the password.

  Workaround: There is no workaround.

- CSCse49728

  Symptoms: SNMPv3 informs are not sent out after a device reload.

  Conditions: This symptom is observed when SNMPv3 informs have been configured, and the device is reloaded.

  Workaround: Re-enter any of the **snmp-server host** commands.

- CSCse66080

  Symptoms: A memory leak may occur in the Entity MIB API process.

  Conditions: This symptom is observed when an entity is registered with the same name as an entity that is already registered.

  Workaround: There is no workaround.

- CSCsf19881

  Symptoms: A Cisco 7600 series crashes when you remove AAA commands.

  Conditions: This symptom is observed when you remove the **aaa accounting system default** command.

  Workaround: Do not remove the **aaa accounting system default** command. If this is not an option, there is no workaround.

- CSCsg43322

  Symptoms: When you attempt to configure an authentication, authorization, and accounting (AAA) list for a network, the following error message may be generated:

  ```
  AAA: No free accounting lists for "network".
  ```

  Conditions: This symptom is observed on a Cisco router that has not yet reached its maximum of 1024 authentication lists, 1024 authorization lists, and 1024 accounting lists.

  Workaround: There is no workaround.

- 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. Is this not an option, there is no workaround.

EXEC and Configuration Parser

- CSCsd32923

  Symptoms: A router may unexpectedly reload with a bus error when you enter a command while the command buffer is full of white space.

  Conditions: This symptom is observed when you enter a partial command and when the tab key is used while the command buffer is full.

  Workaround: There is no workaround.

IBM Connectivity

- CSCse17611

  Symptoms: When DLSw Ethernet Redundancy is configured, circuits may be established through the wrong switch.

  Conditions: This symptom is observed in the following configuration:

  – Clients are connecting to MAC A.

  – Mapping statements are configured so that Switch 1 has a mapping of MAC A = MAC A and Switch 2 has a mapping of MAC B = MAC A.

  The output of the **show dlsw transparent map** shows that Switch 1 has the active mapping and that Switch 2 has the passive mapping. All circuits should be established on Switch 1, but instead they are established on switch 2.

  The outputs of the **show dlsw trans neighbor** and **show dlsw trans map** commands show correct information, but the output of the **show dlsw cir cache** command shows state “negative” on Switch 1 and state “positive” on Switch 2.

  Workaround: There is no workaround. Note that all circuits are up and running, but they just go through the wrong router.

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

Interfaces and Bridging

- CSCed79345

  Symptoms: A router crashes when you enter the **default/no bridge-group** *bridge group* **subscriber-loop-control** interface configuration command.

  Conditions: This symptom is observed when there are no existing bridge-group configurations on the router.

  Workaround: There is no workaround.

- CSCek43732

  Symptoms: All packets are dropped from a 1-port OC-3/STM-1 POS port adapter (PA-POS-1OC3) or 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) that is configured for CBWFQ.

Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1. However, the symptom may be platform-independent.

Workaround: There is no workaround.

- CSCek46996

  Symptoms: An Enhanced FlexWAN Fast Ethernet port adapter cannot support a VPN in crypto connect mode unless the port can immediately transition to promiscuous mode when you enter the **crypto connect** command on the VLAN interface.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCek65222

  Symptoms: A non-parseable Ethernet configuration is nvgened for a VLAN.

  Conditions: This symptom is observed when you enter the **encap dot1q 1 native** command, and the command is rejected. When you enter the **encap dot1q 1** command, the command is accepted. However, in this situation, the output of the **show running-config** command shows that the **encap dot1q 1 native** command is present, which would have been rejected.

  Workaround: There is no workaround.

- CSCsd40136

  Symptoms: POS interfaces may remain in the up/down state after the router is upgraded to another Cisco IOS software image.

  Conditions: This symptom has been observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router but may also affect other platforms such as the Cisco 7500 series router.

  Workaround: Reload the FlexWAN or VIP in which the POS port adapter is installed.

- CSCsd94687

  Symptoms: The output of the **show vlans** *vlanID* shows the wrong counters. The counters do not match the SNMP counters.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: Use only the SNMP counters.

- CSCse61893

  Symptoms: A ping from a channelized T3 (CT3) port adapter may fail.

  Conditions: This symptom is observed on a Cisco platform that is configured with a CT3 port adapter that functions in unchannelized mode.

  Workaround: There is no workaround.

- CSCuk61108

  Symptoms: Packets may become corrupted with a faulty VLAN tag when they are forwarded over an FE interface.

  Conditions: This symptom is observed when the FE interface has subinterfaces that are configured for dot1q encapsulation.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCef70161

  Symptoms: External BGP neighbors that are configured in the IPv4 VRF address-family context may fall into different update groups, even if the outbound policy is identical. This situation slightly reduces the overall scalability because BGP cannot use update replication when sending updates to the neighbors.

  Conditions: This symptom is observed on a Cisco router and is both release- and platform-independent.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not affect neighbors that are configured in the global IPv4 address-family context.

- CSCeg57155

  Symptoms: A ping, Telnet traffic, FTP traffic, and trace route traffic across a VRF-aware NAT do not function.

  Conditions: This symptom is observed on a Cisco router that is configured for VRF-aware NAT only when the router is not directly connected to a gateway.

  Workaround: There is no workaround.

- CSCei29944

  Symptoms: A CE router that has L2TP tunnels in an MPLS VPN environment with about 1000 VRFs may crash and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x50766038
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)S and that functions as a CE router when BGP neighbors are unconfigured via the **no neighbor** *ip-address* command while the **show ip bgp summary** command is entered from the Aux console. The symptom is not release-specific and may also affect other releases.

  Workaround: There is no workaround.

- CSCek24597

  Symptoms: The BGP Support for Next-Hop Address Tracking feature fails.

  Conditions: This symptom is observed when the BGP Event Process is terminated after BGP has been up.

  Workaround: There is no workaround.

- CSCek31478

  Symptoms: When the access control list (ACL) associated with a multicast boundary is modified to permit a statically joined group that has previously been denied by the boundary, the change does not take effect and the group continues to be blocked.

  This issue also affects the static group memberships underlying MVPN tunnels, disrupting connectivity across them.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4 or Release 12.0(32)S but appears to be platform- and release-independent.

  Workaround: Disable and re-enter the **ip multicast boundary** command.

  Alternate Workaround: Enter the **clear ip mroute *** command.

- CSCek32244

  Symptoms: Not all classful networks are locally generated in the BGP table.

  Conditions: This symptom is observed on a Cisco router that has the **auto-summary** command enabled and occurs when classful networks are provided before the routes are made available in the routing table.

  Workaround: There is no workaround.

- CSCek36037

  Symptoms: After a switchover has occurred or when the router is booted, BGP sessions flap.

  Conditions: This symptom is observed on a Cisco router that is configured with 1200 BGP peers, a keepalive value of10 seconds, and a holdtime value of 30 seconds.

  Workaround: There is no workaround.

- CSCek36056

  Symptoms: When you enter the **ipv6 pim bsr candidate bsr ipv6-address** command, the IPv6 address does not show in the output of the **show running-config** command.

  Conditions: This symptom is observed when you attempt to configure a Cisco router to be an IPv6 candidate bootstrap router (BSR). The symptom does not occur when you configure the router to be an IPv4 BSR.

  Workaround: There is no workaround.

- CSCek38025

  Symptoms: A Multicast Distribution Tree (MDT) update does not reach a remote PE router.

  Conditions: This symptom is observed when some of the routers in the network core send MDT addresses in the form of VPNv4 extended community attributes and other routers in the network core send MDT addresses in the MDT SAFI format.

  Workaround: Configure all routers in the network core to use only one form of MDT implementation (that is, configure either the VPNv4 extended community format or the MDT SAFI format).

- CSCek42700

  Symptoms: A network and host-based configuration download over serial HDLC with an IP address obtained via SLARP fails.

  Conditions: This symptom has been observed with a router that has no startup- configuration (after using the **write erase** command) but is staged for autoinstall over a serial link. An IP address is obtained, but the download fails with the following error message:

  ```
  %Error opening tftp://255.255.255.255/network-confg (Socket error)
  %Error opening tftp://255.255.255.255/cisconet.cfg (Socket error)
  ```

  Without this feature, router deployment with automatic configuration download at remote sites over a serial interface is not possible.

  Workaround: Use another method of autoinstall if possible, or pre-configure the router before deployment.

- CSCek45564

  Symptoms: A router crashes because of memory corruption when you bring up Gigabit Ethernet links and BGP neighbor adjacencies, and an error message is generated, indicating that a block overrun and rezone corruption have occurred.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series that are configured for BGP. However, the symptom is not platform-dependent.

Workaround: There is no workaround.

- CSCek58880

  Symptoms: A Cisco router that has an interface that is configured for MPLS TE and OSPF may crash when you first remove the OSPF process and then modify the OSPF cost on the interface.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software images that integrates the fix for caveat CSCse41174 when the following sequence of events occurs:

  – You enter the **ip ospf cost** command on an interface in the MPLS TE area.

  – You enter the **no router ospf** *process-id* command on the interface in the MPLS TE area.

  – You change the OSPF cost on the interface in the MPLS TE area.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse41174. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCek68270

  Symptoms: A router that is configured for EIGRP may crash.

  Conditions: This symptom is observed on a Cisco router that contains an 0.0.0.0/0 address in the EIGRP topology with multiple next hops that change in quick succession.

  Workaround: Limit the 0.0.0.0/0 address to a single next hop.

- CSCsa87034

  Symptoms: When you attempt to clear the routing table, the neighbor is brought down instead.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 unicast *** or **clear bgp ipv6 unicast *** command, causing respectively the IPv4 neighbor or IPv6 neighbor to be brought down.

  Workaround: There is no workaround.

- CSCsb50606

  Symptoms: Memory usage in the "Dead" process grows gradually until the memory is exhausted. The output of the **show memory dead** command shows that many "TCP CBs" are re-allocated. Analysis shows that these are TCP descriptors for non-existing active BGP connections.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(13), that has an NPE-G1, and that functions as a PE router with many BGP neighbors. However, the symptom is not platform-specific, nor release-specific.

  Workaround: Reload the router. I this is not an option, there is no workaround.

- CSCsb69773

  Symptoms: A router may crash during the redistribution of OSPF, EIGRP, RIP, and static routes.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and NSF after a switchover from the primary RP to the secondary RP has occurred.

  Workaround: There is no workaround.

- CSCsc00378

  Symptoms: Changes in an export map are not picked up by the BGP Scanner.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when you apply an export map to a VRF and when the interface that connects the PE router to a CE router is configured for OSPF.

Workaround: Enter the **clear ip ospf process** command to enable the BGP Scanner to pick up the changes in the export map.

- CSCsc33408

  Symptoms: A router reloads unexpectedly when you unconfigure a static route.

  Conditions: This symptom is observed when you first configure the static route for a BGP and IPv4 multicast address family, then clear the BGP routes, and then unconfigure the static route.

  Workaround: There is no workaround.

- CSCsc36517

  Symptoms: A router reloads unexpectedly when a continue statement is used in an outbound route map.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP.

  Workaround: There is no workaround.

- CSCsc41694

  Symptoms: A router may hang when you enter the **no router bgp** command.

  Conditions: This symptom is observed on a Cisco AS5400 and Cisco AS5850 but may also occur on other platforms.

  Workaround: There is no workaround.

- CSCsc46337

  Symptoms: When about thousand eBGP connections are opened between two routers that are connected back-to-back, additional point-to-point eBGP connections between the routers are not established even if IP connectivity between the BGP next-hops is provided.

  Conditions: This symptom is observed when one Cisco router functions as a PE router and the other Cisco router functions as a CE router that has VRF-lite configured.

  Workaround: Reload the PE router to enable all sessions to become established, including the ones that previously were not established.

- CSCsc67367

  Symptoms: The **set ip next-hop in-vrf** *vrf-name* command does not work in conjunction with import maps.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP.

  Workaround: There is no workaround.

- CSCsc73436

  Symptoms: High CPU usage may occur and the table versions of BGP peers are reset to zero.

  Conditions: This symptom is observed when you update a complex policy on a Cisco router that has a complex configuration of BGP peers.

  Workaround: There is no workaround.

- CSCsc75426

  Symptoms: A router that is configured for BGP and that has the **ip policy-list** command enabled may unexpectedly reload because of a bus error or SegV exception.

Conditions: This symptom is observed when BGP attempts to send an update with a “bad” attribute.

Workaround: There is no workaround.

- CSCsc78813

  Symptoms: While using NAT in an overlapping network configuration, the IP address inside a DNS reply payload from the nameserver is not translated at the NAT router.

  Conditions: This symptom is observed on a Cisco router that has the **ip nat outside source** command enabled.

  Workaround: There is no workaround.

- CSCsd03021

  Symptoms: When loading a large link state database from a third-party vendor router that runs Cisco IOS software, the CPU usage by OSPF may become very high, the router may generate CPUHOG messages, and it may take a long time to reach the FULL state, or the FULL state is not reached.

  Conditions: These symptoms are observed in an environment in which packet drops occur. When the link state request that is sent from the Cisco IOS router is dropped, the routers may still continue to exchange DBD packets. However, the link stay request list on the Cisco IOS router may become long, and it may take a lot of CPU usage to maintain it.

  Workaround: There is no workaround.

  Further Problem Description: See also caveat CSCsd38572.

- CSCsd15749

  Symptoms: Prefixes that are tagged with Site of Origin (SoO) values may not be filtered at the border.

  Conditions: This symptom is observed when SoO values are configured for a peer group. The peer group members may not correctly filter the prefixes that are based on the SoO value at the border.

  Workaround: BGP supports Dynamic Update peer groups, which ensure that packing is as efficient as possible for all neighbors regardless of whether or not they are peer-group members.

  Peer groups simplify configurations, but peer-templates provide a much more flexible solution to simplify the configuration than peer groups.

  If the SoO configuration is applied directly to the neighbor or to a template, the symptom does not occur. Using templates to simplify the configuration is a better solution and Dynamic Update peer groups ensure efficiency.

- CSCsd32373

  Symptoms: Multipath load-balancing may not function for internal BGP (iBGP) paths, and routes are not learned through multipath routing, even after you have cleared BGP.

  Conditions: This symptom is observed after an RP switchover has occurred.

  Workaround: There is no workaround.

- CSCsd41237

  Symptoms: Import maps that are applied to VRFs do not take effect. Routes that are received with imported route targets are not filtered by the import route map.

  Conditions: These symptoms are observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that run Cisco IOS Release 12.2(18)SXF. However, the symptoms are both platform- and release-independent.

  Workaround: There is no workaround.

- CSCsd52667

  Symptoms: When you alter the configuration of the **ip nat pool** command, the router may hang, crash, or both.

  Conditions: This symptom is observed on a Cisco router when you enter the following commands in sequence:

  ip nat pool address 255.255.255.255 255.255.255.255

  ip nat pool no address 255.255.255.255 255.255.255.255

  or

  no ip nat pool *name*

  Workaround: There is no workaround.

- CSCsd67768

  Symptoms: Sessions may flap often on a router that has 1200 BGP peers and that is configured with a keepalive value of 10 seconds and a holdtime value of 30 seconds.

  Conditions: This symptom is observed on a Cisco router that has about 1600 interfaces and a large numbers of QoS policies.

  Workaround: Keep the keepalive and holdtime values at the default settings of respectively 60 seconds and 180 seconds. Reduce the load on router by reducing the number of interfaces and QoS policies.

- CSCsd73245

  Symptoms: Many “IPRT-3-PATHIDX” error messages are generated by the “BGP Router” process when you increase the prefixes in a VRF.

  Conditions: This symptom is observed on a Cisco router that is configured for loadbalancing and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

- CSCsd77247

  Symptoms: PPPoEoQinQ sessions fail to reconnect.

  Conditions: This symptom is observed on a Cisco router that has 31,000 sessions when there is one session per subinterface. The symptom occurs when you shut down the main interface, bring it up again, and then attempt to reconnect the PPPoEoQinQ sessions.

  Workaround: There is no workaround.

- CSCsd84489

  Symptoms: A platform that is configured for Open Shortest Path First (OSPF) and incremental Shortest Path First (SPF) may crash when changes occur in the OSPF topology.

  Conditions: This symptom is observed on a Cisco platform that has the **ispf** command enabled when changes occur in the OSPF topology that cause the intra-area routes to be updated.

  Workaround: Disable the **ispf** command.

- CSCsd89569

  Symptoms: The output of the **show ip interface brief** command shows inconsistent output with the following extra message at the beginning:

  ```
  Any interface listed with OK? value "NO" does not have a valid configuration
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

Workaround: There is no workaround.

- CSCse04220

  Symptoms: The BGP table version remains stuck at 1, and the router may crash.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 uni *** command for IPv4 or the **clear bgp ipv6 uni *** command for IPv6. The symptom may also occur when you enter the **clear bgp nsap uni *** command for a network service access point (NSAP) address family.

  Workaround: Enter the **clear ip bgp *** command to clear the sessions, purge the BGP table, and prevent the router from crashing.

- CSCse05031

  Symptoms: The **neighbor default-originate** command does not function properly when the **route map** keyword and *map-name* argument are defined.

  Conditions: This symptom is observed when the target route that is specified in the route map is added or removed from the routing table after the BGP session has already been established.

  Workaround: Clear and re-establish the BGP neighbor.

- CSCse07118

  Symptoms: A router may reload unexpectedly when you enter the **transmit-interface** interface configuration command on an interface that has a point-to-point OSPF adjacency.

  Conditions: This symptom is observed on a Cisco router when the OSPF network type is configured as point-to-point, either because the interface is, for example, a serial interface, or because the **ip ospf network point-to-point** interface configuration command is enabled on the interface.

  Workaround: When there is an OSPF adjacency on the interface that is being configured, first enter the **shutdown** interface configuration command before you enter the **transmit-interface** interface configuration command.

- CSCse19737

  Symptoms: The **auto-summary** command does not function.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv4 multicast or IPv4 unicast.

  Workaround: There is no workaround.

- CSCse41174

  Symptoms: An Area Border Router (ABR) may reload when you unconfigure OSPF.

  Conditions: This symptom is observed on a Cisco router that functions as an ABR and that has a TE tunnel when OSPF advertises the outgoing TE tunnel interface in one area and the TE tunnel as a forwarding adjacency in another area.

  Workaround: There is no workaround.

- CSCse41484

  Symptoms: A DMVPN hub receives a few unencrypted GRE packets from a spoke during the negotiation of an IPsec security association (SA).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for NHRP and that have an IPsec VPN SPA that functions as a spoke in a DMVPN topology.

  Workaround: There is no workaround.

- CSCse44079

  Symptoms: The CPU usage may reach 100 percent in the IGMP Input process when a ULD interface is down.

  Conditions: This symptom is observed on a Cisco router that has a UDL interface that is connected to a satellite link after you have upgraded the Cisco IOS software image from Release 12.4(5a) to Release 12.4(7a). However, the symptom is not release-specific.

  Workaround: There is no workaround.

- CSCse51804

  This caveats consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

     Condition 1: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4 when the DMVPN tunnel is up and when you enter the **show ip nhrp brief** and **clear ip nhrp** commands. When the tunnel comes up again (because of the NHRP registration by the spoke), the NHRP cache entry expires a long time before its expiration time.

     Workaround 1: Do not enter the **show ip nhrp brief** command.

  2. Symptom 2: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

     Condition 2: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4(6)T or a later release and occurs without any specific action.

     Workaround 2: There is no workaround.

  Further Problem Description: These symptoms are not release-specific.

- CSCse66732

  Symptoms: If Spatial Reuse Protocol (SRP) is used, Enhanced Interior Gateway Routing Protocol (EIGRP) does not respond to the ring drop notification from the interface.

  Conditions: This symptom is observed if SRP is used with EIGRP.

  Workaround: There is no workaround.

- CSCse68877

  Symptoms: A label mismatch may occur between the CEF table and the BGP table, and a new label may not be installed into the CEF table.

  Conditions: This symptom is observed after a BGP flap has occurred on a Cisco router that is configured or MPLS VPN but that does not function in an inter-autonomous system and that does not have multiple VRFs.

  Workaround: There is no workaround. After the symptom has occurred, enter the **clear ip route** command for the affected VRF.

- CSCse92050

  Symptoms: A router may reload unexpectedly when a routing event causes multicast boundary to be configured on a Reverse Path Forwarding (RPF) interface.

  Conditions: This symptom is observed on a Cisco platforms that is configured for PIM.

  Workaround: Remove multicast boundary from the configuration.

- CSCsf02935

  Symptoms: A router that is configured for OSPF Sham-Link and BGP redistribution may crash.

Conditions: This symptom is observed only in network topologies with OSPF routes that traverse two or more sham links. For example, the symptom may occur in a hub-and-spoke topology with sham links between the hub and two or more individual spokes. This symptom was observed on a Cisco 10000 series but may also occur on other platforms.

Workaround: There is no workaround.

- CSCsf20947

  Symptoms: A default route that is defined by the **neighbor default-originate** command may be ignored by the BGP neighbor.

  Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the default route to be relearned.

  Workaround: Manually clear the BGP neighbor to enable the router to correctly relearn the default route.

- CSCsf99057

  Symptoms: The OSPF Stub Router Advertisement feature may stop functioning after an RPR+ or SSO switchover has occurred, and the newly active RP does not originate router LSAs with infinity metric as it should do when the **max-metric router-lsa on-startup** router configuration command is enabled.

  Conditions: This symptom is observed on a Cisco router that has dual RPs that function in RPR+ or SSO mode when NSF is not enabled on the router and when the standby RP is in “Standby-Hot” state.

  Workaround: Do not configure RPR+ or SSO. Rather, configure RPR. If this is not an option, there is no workaround.

- CSCsg32482

  Symptoms: The standby RP does not recover after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco router that functions in an MPLS Traffic Engineering - DiffServ Aware (DS-TE) configuration and that has multiple subinterfaces that have the **ip rsvp bandwidth** command enabled.

  Workaround: There is no workaround.

- CSCsg43140

  Symptoms: A router may crash during the boot process and return to ROMmon.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that has VPNs configured.

  Workaround: There is no workaround.

- CSCsg52336

  Symptoms: A router may crash when you remove an unused and unassigned VRF by entering the **no ip vrf** *vpn-name* command.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has the Multi-VRF capability for OSPF routing configured along with other VRFs that are unused and unassigned.

  Workaround: There is no workaround.

- CSCsg55209

  Symptoms: When BGP updates are received, stale paths are not removed from the BGP table, causing the number of paths for a prefix to increase. When the number of BGP paths reaches the upper limit of 255 paths, the router resets.

  Conditions: This symptom is observed on a Cisco router when the **neighbor soft-reconfiguration inbound** command is enabled for each BGP peer.

  Workaround: Remove the **neighbor soft-reconfiguration inbound** command. A router that runs a Cisco IOS software image that has a route refresh capability, storing BGP updates is usually not necessary.

- CSCsg59699

  Symptoms: The OSPFv3 cost on PortChannel interfaces that is calculated based on the interface bandwidth may not be correct.

  Conditions: This symptom is observed on a Cisco router when OSPF functions in IPv6 router configuration mode and when the **auto-cost reference-bandwidth** command is enabled.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected PortChannel interface.

- CSCsg66635

  Symptoms: The IGP metric may be missing from the TE database.

  Conditions: This symptom is observed on a Cisco router when TE is configured on a subinterface and when you enter the **no shutdown** interface configuration command on the physical main interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the subinterface on which TE is configured.

- CSCsg71344

  Symptoms: On a router that is configured for SSM and that is connected to an upstream router via two interfaces, when one of the interfaces is shut down and brought up again, a PIM Join message is not sent.

  Conditions: This symptom is observed on a Cisco router that is connected to an upstream router via an RPF interface. When the interface of the upstream router that connects to the RPF interface is shut down, the PIM Join message is sent via the other interface on the Cisco router. However, when the interface of the upstream router that connects to the RPF interface is brought up again, the PIM Join message is not sent again, preventing IPv6 multicast from functioning properly.

  Workaround: There is no workaround.

- CSCsg83966

  Symptoms: Paths that are imported via VPN may be missing from the VRF. For example, paths that are imported from the same route distinguisher (RD) may be missing from the VRF.

  The route map that is specified in the **import ipv4 unicast map** *route-map* command is meant to be applied to paths that are imported into the VRF from the global table. However, the route map is also incorrectly applied to VPN paths during the VPN import process. When the route map filters some of these paths, they are not imported, which is shown in the output of the **show ip bgp vpnv4 vrf vpn-name** command.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when you use the **import ipv4 unicast map** *route-map* command to import an address family from the global table into a VRF. The following sequence of events illustrates how the symptom occurs:

1. Configure an IP prefix list.
   [example:
   ```
   ip prefix-list COLORADO seq 5 permit 10.1.5.0/24]
   ```
2. Configure a route map by using the prefix list as the matching criteria.
   [example:
   ```
   route-map UNICAST permit 10 match ip address prefix-list COLORADO]
   ```
3. Import the route map into the VRF.
   [example:
   ```
   ip vrf isp1
      rd 65031:100
      import IPv4 Unicast map UNICAST
      route-target export 65031:100
       route-target import 65031:100]
   ```
4. Trigger a routing update by entering the **clear ip bgp** command.
5. Check the output of the **show ip bgp vpnv4 vrf vpn-name** command. The output does not show entries from the BGP neighbor.

Workaround: There is no workaround.

- CSCsh17035

  Symptoms: A route may flap continuously and the CPU usage may be high continuously.

  Conditions: This symptom is observed on a Cisco router that is configured with a static route loop.

  Workaround: Do not configure a static route loop.

- CSCsh19852

  Symptoms: When an OSPF interface goes down, some Finite State Machine (FSM) events do not occur. For example, old network LSAs may not be removed by the Designate Router (DR).

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCek63900. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCek63900. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCsh61119

  Symptoms: ARP may be refreshed excessively on the default interface, causing high CPU usage in the “Collection Process.”

  Conditions: This symptom is observed on a Cisco router that has point-to-point interfaces that have non-/32 interface addresses or secondary addresses and that constantly come up or go down.

  Workaround: There is no workaround.

- CSCsh65136

  Symptoms: RSVP reservations may become lost or may not be rebuilt when an SSO switchover occurs. Although RSVP is not SSO-aware, RSVP reservations should be re-established after an SSO switchover has occurred.

Conditions: This symptom is observed on a Cisco 7600 series that is configured with dual Supervisor Engine 720 modules and a Policy Feature Card 3BXL (PFC3BXL) and that functions in the following configuration:

- The Cisco 7600 series functions as a mid-point router.
- The router that sends RSVP reservations is a downstream router.
- The router that should receive the RSVP reservations is an upstream router and is enabled for RSVP CAC.

The interfaces that are used in the topology are Gigabit Ethernet interfaces and 10-Gigabit Ethernet with subinterfaces.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the mid-point router.

- CSCsh66294

  Symptoms: A Cisco 7600 series that is configured for BGP crashes during normal operation.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions as a PE router in an MPLS environment.

  Workaround: There is no workaround.

- CSCuk58462

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for redistributed route maps.

ISO CLNS

- CSCse30000

  Symptoms: An L1 LSP that is originated on a local router may not be flooded to its neighbors until the local IS-IS LSP lifetime expires, and the IS-IS floods a new LSP and runs a periodic FSPF.

  Conditions: This symptom is observed on an IS-IS Level 1 - Level 2 (L1L2) router.

  Workaround: Lower the IS-IS LSP lifetime to reduce the period the symptom lasts.

- CSCse40346

  Symptoms: Tracebacks may be generated when you configure IS-IS and LDP features, for example, when you enter the **no ip router isis** *area-tag* command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)SY but may also occur in other releases.

  Workaround: There is no workaround.

- CSCse85158

  Symptoms: Locally advertised networks that are configured for the NSAP address- family under BGP will not be readvertised once they have been cleared from the BGP table.

  Conditions: Once the **clear bgp nsap unicast *** command has been issued, the networks will no longer appear in the output of the **show bgp nsap unicast** command.

Workaround: There is no workaround.

- CSCse93383

  Symptoms: The default value for the CSNP interval may not be set.

  Conditions: This symptom is observed on a Cisco router when you configure a LAN subinterface to be an ISIS point-to-point subinterface by entering the **isis network point-to-point** command. The default value may remain tho one of the LAN.

  Workaround: Manually configure the CSNP interval.

- CSCsg28497

  Symptoms: An IS-IS adjacency may flap when an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco router that is configured for IS-IS Multi-Topology, IS-IS NSF Awareness, and IPv4 and IPv6 unicast.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb05456

  Symptoms: A Cisco platform may reset its RP when two simultaneous **write memory** commands from two different vty connections are executed, and messages similar to the following may appear in the crashinfo file:

  ```
  validblock_diagnose, code = 10
  current memory block, bp = 0x48FCC7D8,
  memory pool type is Processor
  data check, ptr = 0x48FCC808
  next memory block, bp = 0x491AC060,
  memory pool type is Processor
  data check, ptr = 0x491AC090
  previous memory block, bp = 0x48FCBBE8,
  memory pool type is Processor
  data check, ptr = 0x48FCBC18
  ```

  The symptom is intermittent and is related to the way NVRAM is accessed.

  Conditions: This symptom is observed on a Catalyst 6000 series Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXD but is platform- and release-independent.

  Workaround: Set the boot configuration to non-NVRAM media such as a disk or bootflash by entering the following commands:

  ```
  boot config disk0:
  filename
  nvbypass
  ```

- CSCeb68312

  Symptoms: When a virtual server is configured to use port 0 and an HTTP probe is configured to use port 80, the HTTP probe does use port 80, but the host tag shows that the HTTP probe uses port 0. Not only is a port number not required in the host tag, the port number of 0 is invalid. This situation may cause problems with Internet Information Services (IIS) 6.0 running on Windows Server 2003.

  Conditions: This symptom is observed on a Cisco platform that is configured for IOS Server Load Balancing (IOS SLB).

Workaround: Do not configure a virtual server to use port 0 when HTTP probes are used. Rather, configure the virtual server to use a specific port, or use TCP or ICMP probes.

- CSCed36177

  Symptoms: A software-forced crash may occur on the RP in a Cisco Catalyst 6500 series switch or Cisco 7600 series router.

  Conditions: This symptom is observed only with a tunnel configuration and may occur with either crypto or non-crypto images.

  Workaround: There is no workaround.

- CSCef25686

  Symptoms: A number of PVCs may become locked in an inactive state, and the following type of error message may appear in the log:

  ```
  %ATM-3-FAILREMOVEVC: ATM failed to remove VC(VCD=X, VPI=X, VCI=X) on Interface ATM X/X/X,
  (Cause of the failure: PVC removal during recreation failed)
  ```

  Conditions: This symptom is observed when you change the parameters of a VC class while the PVC is active and while you view the PVC status in the output of the **show atm vc interface** *interface-number* command.

  The symptom occurs when you change the PVC speed in a VC class via one Telnet (or console) session and you enter the **show atm vc interface** *interface-number* command via another Telnet (or console) session.

  Workaround: To remotely resolve the symptoms, remotely initiate an HA failover or remotely reload the affected router.

- CSCeg03733

  Symptoms: A router may reload because of a memory corruption when you query via getmany or getbulk the entire ciscoCBQosMIB (1.3.6.1.4.1.9.9.166) or when you poll the cbQosQueueingStatsTable or cbQosPoliceStatsTable.

  Conditions: This symptom is observed on a Cisco 7500 series that runs the rsp-jsv-mz image of Cisco IOS interim Release 12.3(11.4) when the following tables in the CBQOSMIB are polled:

  – getREDClassStats
  – getTSStatsEntry
  – getQueueingStatsEntry
  – getPoliceStatsEntry

  The symptom may not be platform-specific.

  Workaround: Do not query the entire ciscoCBQosMIB and do not poll the cbQosQueueingStatsTable or cbQosPoliceStatsTable.

- CSCeh15378

  Symptoms: When you shut down an ATM main interface, the state of the local ATM circuit goes down as expected. However, when you then enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a subinterface of the same ATM main interface that is shut down, the local circuit state comes back up again, and an “SLI UP” message is sent to a remote PE router.

  Conditions: This symptom is observed on a Cisco router when the subinterface has an Xconnect attachment circuit that is configured for ATM VP Mode.

  Workaround: There is no workaround.

- CSCeh41598

  Symptoms: When RIP is enabled and disabled successively 50 to 60 times in a row, the router reloads unexpectedly during the “RIP managed timer” process.

  Conditions: This symptom is observed on a Cisco router that has 15,000 learned RIP prefixes. However, note that RIP does not properly scale beyond about 5000 routes on a high-end router.

  Workaround: Do not enable and disable RIP successively 50 to 60 times in a row.

  First Alternate Workaround: Limit the number of RIP prefixes to 5000 or less.

  Second Alternate Workaround: Before RIP is disabled, for example through the **no router rip** command, remove the network entries under the **router rip** command.

- CSCei23358

  Symptoms: IPv6 prefixes that match the **network** command remain advertised after the **network** command has been disabled.

  Conditions: This symptom is observed when the **network** command is specified within the **address-family ipv6** command for a BGP configuration, and is subsequently removed by entering the **no network** command.

  Workaround: There is no workaround.

- CSCej08637

  Symptoms: When you run the Entity-MIB on a redundant system, the standby supervisor engine may reset. When you enter the **show environment status** command on the standby supervisor engine, the module information is not shown, nor are inline power sensors on the VDB shown.

  Conditions: These symptoms are observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured for SSO.

  Workaround: There is no workaround.

- CSCek02024

  Symptoms: MNCP negotiations between PE routers fail when cell packing is configured.

  Conditions: This symptom is observed on Cisco routers that function in an L2VPN Pseudowire Switching configuration across Intra-Autonomous Systems and that have VCs that are configured for ATM over MPLS (ATMoMPLS) and Peak Cell Rate (PCR).

  Workaround: There is no workaround. Note that the symptom does not occur when cell packing is not configured.

- CSCek03591

  Symptoms: A traffic class is deleted even when there is traffic that matches the ACL for the traffic class.

  Conditions: This symptom is observed when a subscriber session is configured with a traffic class that is configured with a Layer 4 redirect feature and idle timeout.

  Workaround: There is no workaround.

- CSCek23840

  Symptoms: When a virtual-access interface is invoked, it does not inherit an outbound service policy and a Link Fragmentation and Interleaving (LFI) configuration from the virtual template. Also, 75 percent of the packets are dropped from the interface.

  Conditions: These symptoms are observed on a Cisco router that is configured for MLP.

  Workaround: There is no workaround.

- CSCek26931

  Symptoms: A session-based QoS service policy may not be active.

  Conditions: This symptom is observed when a QoS service policy is attached to a PPPoE session that is forwarded. In this situation, the QoS service policy is not automatically attached to the forwarded session and is therefore not active on the forwarded session.

  Workaround: There is no workaround.

- CSCek31437

  Symptoms: A WS-6516-GE-TX module may not power up, and the following error message may be generated:

  ```
  C6KPWR-SP-4-UNSUPPORTED: unsupported module in slot <slot-no>, power not allowed:
  Module not at an appropriate hardware revision level.
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with a Supervisor Engine 32 that runs Cisco IOS Release 12.2SR or Release 12.2SX.

  Workaround: There is no workaround.

- CSCek35061

  Symptoms: A router may crash when you disassociate a VRF from an MPLS interface.

  Conditions: This symptom is observed on a Cisco router that is configured for L2TP when you enter the **no ip vrf forwarding** *vrf-name* command.

  Workaround: There is no workaround.

- CSCek37222

  Symptoms: Packets are not classified when a service policy is configured with random-detect in the class default.

  Conditions: This symptom is observed on a Cisco 7600 series when the service policy is attached to a Frame Relay interface on an OSM-CT3 line card or OSM-8OC3-POS module. Note that the symptom does not occur when the service policy is attached to a Frame Relay PVC.

  Workaround: There is no workaround.

- CSCek37963

  Symptoms: A QoS policy map may fail on ATM, HDLC, and Frame Relay interfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that has a QoS policy map that is configured for WRED with a police action at the first and second level. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when the QoS policy map is configured for WRED only.

- CSCek39364

  Symptoms: The standby RP reloads when you unconfigure an ATM bundle.

  Conditions: This symptom is observed on a Cisco router when you configure an ATM bundle and PVC bundle and then immediately unconfigure the ATM bundle.

  Workaround: There is no workaround.

- CSCek40394

  Symptoms: The queueing hierarchy is not removed when it should be removed, even though the output of the **show policy-map interface** command indicates that the queueing hierarchy is removed.

  Conditions: This symptom is observed when you detach a service policy that has queueing features in the policy map.

  Workaround: There is no workaround.

- CSCek42751

  Symptoms: The running configuration may not be accessible after you have copied a small file to the running configuration.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system after you have rebooted the router.

  Workaround: Reboot the router once more.

- CSCek43610

  Symptoms: After you perform an OIR of a line card or SPA, there is no more connectivity and a ping fails.

  Conditions: This symptom is observed on a Cisco 7600 series that is connected back-to-back to another Cisco 7600 series over a single-VLAN BCP on OC-3 POS SPAs that are installed in SIP-400 line cards. The symptom occurs after you have performed an OIR of the SPAs or line cards on both sides.

  Workaround: There is no workaround.

- CSCek43669

  Symptoms: An input policy that is configured for a default-class does not function for a class that is not a queueing class such as a class with a marking policy.

  Conditions: This symptom is observed only on an ATM SPA that is configured for QoS and that is installed in a SIP-200.

  Workaround: There is no workaround.

- CSCek44025

  Symptoms: A router may crash when a hierarchical policy is attached to a Frame Relay PVC.

  Conditions: This symptom is observed on a Cisco router when the following conditions are present:

  – The hierarchical policy has the **shape** command enabled in the class default of the parent policy and has a child policy.

  – The Frame Relay PVC is configured for FRF.12 in a map class.

  Workaround: There is no workaround.

- CSCek44427

  Symptoms: An interface of a T3/E3 serial SPA passes traffic even though the output of the **show controller** command shows that there is a “Loss of Frame” alarm. When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the SPA, the alarm is not cleared.

  Conditions: This symptom is observed on a Cisco platform that is configured with a T3/E3 serial SPA.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface at the remote end.

Further Problem Description: The symptom does not affect proper operation of the platform or the traffic. However, the incorrect alarm status may affect network management utilities.

- CSCek44532

  Symptoms: A standby RP may reload repeatedly when you enter the **issu loadversion** command during a period of high checkpointing activity. When you enter the **show checkpoint statistics** command on the active RP, the output shows that the checkpointing IPC flow control status remains set to zero indefinitely:

  ```
  CHKPT FLOW_ON status = 0
  ```

  Conditions: This symptom is observed on a Cisco router when the standby RP reloads as part of the In-Service Software Upgrade (ISSU) process while, for example, a large number of PPPoA sessions are being disconnected.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command to cancel the ISSU process, and then reload the router.

- CSCek45862

  Symptoms: Packets are not classified according to the value of the *mpls-exp-value* argument in the **set mpls experimental imposition** *mpls-exp-value* command.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a 6PE router when packets are processed via a SIP-200.

  Workaround: There is no workaround.

- CSCek46189

  Symptoms: The forced target-probing functionality in Optimized Edge Routing (OER) may not work as expected.

  Conditions: This symptom is observed only when a policy changes in a configuration in which learned prefixes are deleted and new policies take effect.

  Workaround: There is no workaround.

- CSCek46832

  Symptoms: The following message appears on the console:

  ```
  SEC 8:00:08:11: %TAGCON-3-LCLTAG_ALLOC: Cannot allocate local tag
  ```

  Conditions: This symptom has been observed when dual RPs with SSO and VPLS are configured.

  Workaround: There is no workaround.

- CSCek47059

  Symptoms: IPv6 packets may be accounted as MPLS packets in the output of the **show interface accounting** command.

  Conditions: This symptom is observed on a Cisco 7600 series when IPv6 addresses are configured on interfaces of an Optical Services Module (OSM) and when IPv6 traffic or a ping is processed.

  Workaround: There is no workaround.

- CSCek47083

  Symptoms: In a blade-to-blade configuration, when the encryption cards are reloaded at the same time, there are less GRE SAs at the active blade than that there are at the standby blade, causing traffic loss for the GREs that are missing from the active blade.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a blade-to-blade redundancy configuration and that has 500 GRE over IPsec tunnels.

Workaround: Do not reload both encryption cards at the same time. First reload one encryption card and wait until it has come up. Then, reload the other encryption card.

- CSCek47205

  Symptoms: A Cisco 7600 series may crash when a blade-to-blade switchover occurs.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.3(33)SRA, that has an IPSec VPN SPA, and that has the **crypto engine mode vrf** command enabled.

  Workaround: There is no workaround.

- CSCek47506

  Symptoms: NetFlow Data Export (NDE) stops functioning unexpectedly, a memory allocation failure (MALLOCFAIL) occurs, hardware-switching becomes disabled, and, finally, the Distributed Forwarding Card (DFC) is reset.

  When an SSO switchover occurs and when the DFC has a high NetFlow TCAM utilization, the DFC stops functioning immediately and is eventually reset.

  Conditions: These symptoms are observed on a Cisco 7600 series when NDE is enabled, especially NDE version 8 or NDE version 9.

  Workaround: There is no workaround.

  Further Problem Description: When NDE stops functioning, the export packets continue to be generated and are queued, waiting to be sent. These packets use up the memory and cause the DFC to run out of memory because the memory pool becomes too fragmented.

- CSCek47814

  Symptoms: A ping between two CE routers may fail after you have reloaded the CE router on the Ethernet side.

  Conditions: This symptom is observed in an AToM configuration when one CE router is configured for PPP and the other CE router is configured for Ethernet. The symptom occurs because of a MAC address learning failure.

  Workaround: Reconfigure VLAN over MPLS on the corresponding Ethernet interface of the adjacent PE router.

- CSCek50172

  Symptoms: An Embedded Event Manager (EEM) policy that has the **event interface** command enabled cannot be registered, and a traceback is generated.

  Conditions: This symptom is observed when the **event interface** command has the **poll-interval** keyword enabled and when the *poll-int-value* argument has a value that is larger than 2097151.

  Workaround: Specify a *poll-int-value* argument with a value that is lower than 2097151.

- CSCek51919

  Symptoms: A Cisco router that functions as an Intelligent Service Gateway (ISG) may reload while sessions are being cleared.

  Conditions: This symptom is observed only when the port-bundle host key (PBHK) feature is configured for the sessions.

  Workaround: Do not configure the PBHK feature for the sessions.

- CSCek52892

  Symptoms: An enhanced FlexWAN module or other line card may crash.

Conditions: This symptom is observed on a Cisco 7600 series that is configured for MPLS and OAM.

Workaround: There is no workaround.

- CSCek54572

  Symptoms: A switch or router may crash when you configure and unconfigure 500 IPSec VTI tunnels two or three times. The symptom does not occur when you configure and unconfigure the tunnels only once.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series.

  Workaround: After you have configured the tunnels, wait for the tunnels to come up before you unconfigure the tunnels.

- CSCek54946

  Symptoms: On a Cisco 7600 series, the MAC address of one or more interfaces may change unexpectedly when the ifPhysAddress object of the IF-MIB is accessed by SNMP. This situation prevents the router from receiving packets when an ARP entry that contains the MAC address of the router is refreshed.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: To prevent the symptom from occurring, configure static ARP on the devices that must be able to send packets to the router. After the symptom has occurred, reload the router to clear the condition.

- CSCek55001

  Symptoms: A router may crash when you enter the **dir /recursive** command.

  Conditions: This symptom is observed on a router that has a Cisco IOS File System (IFS) and occurs only when 40 subdirectories are created. The symptom does not occur when you enter the **dir** command without the **/recursive** keyword.

  Workaround: When more than 40 subdirectories are created, do not use the **dir /recursive** command. Rather, use the **show disk** command.

- CSCek58360

  Symptoms: The circuit ID and remote ID of option 82 in a DHCP relay reply message may be empty and may cause a DHCP relay reply validation error, resulting in a DHCP lease renewal failure.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when an IP session that is initiated by DHCP involves a VRF transfer.

  Workaround: There is no workaround.

- CSCek58678

  Symptoms: When you attempt to configure an invalid access control list (ACL), the following error message is generated:

  ```
  %SYS-3-INTPRINT: Illegal printing attempt from interrupt level.
  ```

  When the router is configured with a SIP-200, the following message is also generated:

  ```
  SIP200_MP-4-PAUSE: Non-master CPU is suspended for too long.
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for Policy Based Routing (PBR).

  Workaround: There is no workaround.

- CSCek60118

  Symptoms: A traceback may be generated when you configure the L2VPN Pseudowire Redundancy feature.

  Conditions: This symptom is observed on a Cisco 7600 series but may be platform-independent.

  Workaround: There is no workaround. However, note that the functionality of the router is not impacted by the traceback.

- CSCek60775

  Symptoms: A router that has Virtual Tunnel Interfaces (VTIs) may crash.

  Conditions: This symptom is observed when two VTIs are configured with the same IP address and when the inside VRF (IVRF) of one VTI is the same as the Front Door VRF (FVRF) for the other VTI.

  Workaround: There is no workaround. The configuration that is stated in the Conditions is not considered a valid configuration.

- CSCek61974

  Symptoms: You may be able to configure a minimum receive interval as short as 1 ms, which may cause problems on the router.

  Conditions: This symptom is observed on a Cisco router that supports Bidirectional Forwarding Detection (BFD). Note that a minimum receive interval shorter than 50 ms is not supported in Cisco IOS software images.

  Workaround: Configure a minimum receive interval of 50 ms or longer.

- CSCek63629

  Symptoms: When you first reset the standby RP and then a switchover occurs, the following error message and a traceback are generated:

  ```
  %LFD-3-ORPHANNONIPLTE: Found a non-owned non-IP LTE of ptype 5 - label 0/0.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS.

  Workaround: There is no workaround.

- CSCek64847

  Symptoms: On a router that is configured for Hot Standby Router Protocol (HSRP), the hold timer that is configured via the **standby timers msec** command does not function properly when the standby group number is 17 or higher.

  The configured standby hold time changes unexpectedly to 3 times the group number value instead of remaining in the 50-3000 msec range when the standby group is configured in the 17-4095 range.

  Also, when a relatively high number is configured for the standby group, a "%PARSER-4-BADRANGE" error message is generated.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(6)T3 or Release 12.4(11)T but may also affect other releases such as Release 12.2SR.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(5a).

- CSCek65022

  Symptoms: A 7600-SSC-400 SPA services carrier may crash during the boot process of a SPA.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when an IPsec VPN Shared Port Adapter (SPA-IPSEC-2G) that is installed in the 7600-SSC-400 boots.

Workaround: There is no workaround.

- CSCek66294

  Symptoms: The TCP MSS Adjustment feature works only in the ingress direction. The feature should work both in the ingress and egress direction.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCek69134

  Symptoms: When you enter the **default interface** command on an interface with a scaled Ethernet Virtual Circuit (EVC) service instance configuration, it may take a long time for the command to be executed, and during this time, the CPU usage of the RP may increase to 100 percent. In addition, many error messages may be generated.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when a scaled EVC service instance configuration is enabled on a Gigabit Ethernet port of a 20-port Ethernet Services line card (7600-ES20-GE) that is installed in a SIP-400.

  Workaround: There is no workaround. You must wait until the command has been executed. However, the command functions properly.

  Further Problem Description: The **default interface** command is often used to set an interface to its default state before a configuration is applied, and it is used to remove a scaled configuration from an interface by just entering one command rather than deleting individual configuration lines one-by-one.

  As an alternative, you can enter the **no service instance** command for each service instance on the port. The following example shows steps to simplify the process:

  Instead of entering the **default gi1/0/1** command, do the following:

  1. Enter the **show running interface gi1/0/1 | inc service instance** command.
  2. Cut-and-paste the output into your preferred editor.
  3. Edit the file by placing “no” before each line.
  4. Enter the following configuration:

     ```
     conf t
          int gi1/0/1
          <paste the file>
     ```

- CSCin85894

  Symptoms: This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: A “%SYS-3-MGDTIMER” error message followed by a traceback may be generated at the “mgd_timer_complain_uninit” function when an extended ACL is configured with the same name as an active reflexive ACL.

     Condition 1: This symptom is observed when the extended ACL is configured with the same name as the reflexive ACL, when the reflexive timer expires at the moment of configuration, and when the dynamic entries of the reflexive ACL are still in place when you configure the extended ACL.

     Workaround 1: Wait until the reflexive timer expires before you configure an extended ACL with same name as a reflexive ACL.

  2. Symptom 2: A software-forced reload may occur when a standard ACL is configured with the same name as an active reflexive ACL.

Condition 2: This symptom is observed when the standard ACL is configured with the same name as the reflexive ACL, when the reflexive timer expires at the moment of configuration, and when the dynamic entries of the reflexive ACL are still in place when you configure the standard ACL.

Workaround 2: Wait until the reflexive timer expires before you configure a standard ACL with same name as a reflexive ACL.

- CSCir00361

  Symptoms: The E1 layer entries for a channelized E3 port adapter may be missing from the IF-MIB list, causing the absence of the corresponding DS1 layer Descriptor and Stack entries when an SNMP walk is performed.

  Conditions: This symptom is observed on a Cisco router that functions in a very simple configuration in which a channelized E3 port adapter is configured with several E1 layers.

  Workaround: There is no workaround.

- CSCir01449

  Symptoms: A router that functions under a heavy load with SSHv2 clients may crash if any of the SSH clients are terminated.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA or Release 12.2(33)SRB when the following conditions are present:

  – The CPU usage is above 70 percent.
  – There are continuous sweep pings from two far-end routers that have the **debug ip packet** command enabled to create continuous logs for the SSH clients.
  – The **no logging console** command is configured.
  – A connection is made from a couple of SSHv2 clients, you enable the **terminal monitor** command, and you terminate the SSHv2 clients while continuous messages are being generated.
  – The TCP window size is reduced.

  Workaround: Do not use SSHv2 when the router is very stressed.

- CSCsa54608

  The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

  Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

  Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

  Only devices running certain versions of Cisco IOS are affected.

  Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml.

- CSCsa96960

  Symptoms: MPLS OAM echo request packets may be forwarded from a different interface than the interface that is reported in an MPLS echo reply that is sent in response to an LSP traceroute.

Conditions: This symptom is observed on a Cisco router when an LSP traceroute is sent under the following conditions:

- The penultimate hop has multiple parallel paths, at least one of which has MPLS enabled.
- One or more of the parallel paths have MPLS disabled.

Workaround: Ensure that MPLS is enabled on all equal-cost paths at the penultimate hop.

- CSCsb25404

  Symptoms: The startup configuration in NVRAM is not loaded onto line cards when the router is manually reloaded.

  Conditions: This symptom is observed on a Cisco 12000 series that functions as a multiservice edge (MSE) router when the ATM Cell Relay over MPLS feature is configured on 500 connections. The symptom may also occur on other platforms.

  Workaround: After the router has been reloaded, cut and paste the initially rejected configuration onto the line cards.

- CSCsb40304

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsb66799

  Symptoms: After a router has been reloaded, an URL match statement unexpectedly may be removed from the configuration.

  Conditions: This symptom is observed when the **match protocol http url** *url-string* command is enabled. After the router has been reloaded, this command has disappeared from the configuration.

  Workaround: There is no workaround.

- CSCsb79031

  Symptoms: A Cisco Catalyst 6500 series switch or Cisco 7600 series router may crash when you enter the **clear counters** command.

  Conditions: This symptom is observed when a communication problem occurs with one of the CSMs. Internal communication problems can be reported through an ICC, IPC, or SCP error message such as the following ICC-4-HEARTBEAT message:

  ```
  %ICC-4-HEARTBEAT: Card 6 failed to respond to heartbeat.
  ```

  Workaround: Do not enter the **clear counters** command when an ICC-4-HEARTBEAT message is generated for an CSM.

- CSCsb79895

  Symptoms: An authentication check fails for incoming packets. When you enable the **debug ip rip** command, an “invalid authentication” error message is generated.

  Conditions: This symptom is observed on a Cisco router when the RIP routing protocol is configured along with MD5 interface authentication.

  Workaround: There is no workaround.

- CSCsb89043

  Symptoms: The following error message and traceback are generated when an RP switchover occurs:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x603D9154 reading 0x4C
  -Traceback= 603D9154 603DA078 603DA0C0 603DA65C 603DA740 603DA8AC 603DA9AC 603C92F4
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for HA.

  Workaround: There is no workaround. However, the symptoms do not affect the performance of the router or the processing of traffic.

- CSCsb94859

  Symptoms: AToM VCs do not come up after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that is configured with AToM VCs when you perform a soft SSO switchover by entering the **redundancy force-switchover** command, preventing the AToM VCs from coming up on the standby RP and the AToM circuit from being established. Note that the symptom is platform-independent

  Workaround: First, configure an incorrect MTU value on the AToM VCs. Then, change the MTU to the correct value. Doing so brings up the AToM VCs and establishes the AToM circuit.

- CSCsc06891

  Symptoms: There are no traps or notifications send when a compact flash disk is inserted in or removed from device disk0 or disk1.

  When you enter the **show running-config | incl snmp-server enable traps flash snmp-server enable traps flash insertion removal** command, the following output is shown:

  ```
  %FILESYS-SP-5-DEV: PCMCIA flash card removed from disk1
  %FILESYS-SP-5-DEV: PCMCIA flash card inserted into disk1
  ```

  Conditions: This symptom is observed on a Cisco router and switch that are configured with a PCMCIA file system.

  Workaround: There is no workaround.

- CSCsc33990

  Symptoms: A supervisor engine may unexpectedly reset when the TestSPRPInbandPing as part of the Cisco Generic Online Diagnostics (GOLD) fails for 10 consecutive times.

  The following syslog error messages are typically generated right before the supervisor engine resets, and can also be found in the crashinfo files:

  ```
  %CONST_DIAG-SP-3-HM_TEST_FAIL: Module <slot#> TestSPRPInbandPing consecutive failure
  count:5
  %CONST_DIAG-SP-6-HM_TEST_INFO: CPU util(5sec): SP=10% RP=0% Traffic=0%
  netint_thr_active[0], Tx_Rate[4412], Rx_Rate[0]
  %CONST_DIAG-SP-3-HM_TEST_FAIL: Module <slot#> TestSPRPInbandPing consecutive failure
  count:10
  %CONST_DIAG-SP-6-HM_TEST_INFO: CPU util(5sec): SP=10% RP=0% Traffic=0%
  netint_thr_active[0], Tx_Rate[4652], Rx_Rate[0]
  %CONST_DIAG-SP-2-HM_SUP_CRSH: Supervisor crashed due to unrecoverable errors, Reason:
  Failed TestSPRPInbandPing
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that run an integrated Cisco IOS software image. The trigger for the symptom may be possible corruption in TCAM entries that are used to perform the TestSPRPInbandPing.

  Workaround: Enter the **no diagnostic crash** global configuration command to disable exceptions that are being triggered by failed diagnostic monitoring. However, you should do this with discretion because it may also prevent the system from taking proactive measure to mitigate problems that could impact user traffic.

  Further Information: The fix for this caveat is more of an enhancement because it only prevents the system from being over-aggressive in taking exceptions when the TestSPRPInbandPing fails under specific conditions. Therefore, the fix for this caveat does not address all triggers that may cause the TestSPRPInbandPing to fail. Please consult Cisco TAC for further assistance if you experience the same problem after upgrading to a Cisco IOS software image that contains the fix for this caveat.

- CSCsc38127

  Symptoms: The standby supervisor engine may crash when an interface has a stateful inspection policy or when the **ip nbar protocol-discovery** command is enabled.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that run a native Cisco IOS software image.

  Workaround: There is no workaround.

- CSCsc49134

  Symptoms: A platform may crash when you configure an ATM multipoint subinterface.

  Conditions: This symptom is observed on a Cisco platform when there are already some ATM subinterfaces that are configured for ATM PVC discovery.

  Workaround: There is no workaround.

- CSCsc56766

  Symptoms: When channel members of an EtherChannel are located on different forwarding engines and when one channel goes down, traffic may be disturbed for six seconds or longer and a control protocol may be adversely affected. The duration of the traffic disturbance depends on the number of VLANs.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch but may also occur on a Cisco 7600 series router.

  Workaround: Place all members of the EtherChannel on the same forwarding engine.

Alternate Workaround: Limit the number of VLANs on the trunk.

- CSCsc58556

  Symptoms: A Cisco router may crash when an EEM Tcl policy runs.

  Conditions: This symptom is observed when the available memory is very low.

  Workaround: Increase the available memory. If this not an option, there is no workaround.

- CSCsc60249

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)
  – Media Gateway Control Protocol (MGCP)
  – Signaling protocols H.323, H.254
  – Real-time Transport Protocol (RTP)
  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsc71245

  Symptoms: A router that is connected to several VPN clients may unexpectedly reload because of a CPUHOG condition in the crypto IKMP process followed by a watchdog timeout.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router and occurs about every about 24 hours, which is equal to the IKE lifetime.

  Workaround: There is no workaround.

- CSCsc72515

  Symptoms: A downstream interface that becomes a non-designated forwarder (DF) interface may not be deleted from the outgoing interface list (olist) for certain (*,G) groups. This situation causes packets to be incorrectly forwarded and leads to looping.

  Conditions: This symptom is observed on a Cisco router that is configured for Bidirectional PIM when a DF interface that forwards traffic downstream changes to a non-DF interface.

  Workaround: There is no workaround.

- CSCsc80303

  Symptoms: IPC Watermark messages may be generated when a trunking interface goes up or down, and a memory leak may occur.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a dot1q trunking interface that is bundled with more than 2000 VLAN interfaces.

  Workaround: There is no workaround.

- CSCsc94240

  Symptoms: Some line cards may reset when an SSO switchover occurs.

  Conditions: This symptom is observed on a Cisco 7600 series after two or three SSO switchovers have occurred.

  Workaround: There is no workaround.

- CSCsc95875

  Symptoms: After multiple SSO switchovers occur on a Cisco 7600 series, an OSM or FlexWAN module may be reset by the switch processor because of a keepalive or SCP failure.

  The same symptom may occur while toggling hardware switching by entering the **no mls switching** command followed by the **no mls switching** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR and that has a non-fabric-enabled LAN card in its chassis.

  Workaround: There is no workaround.

- CSCsd04299

  Symptoms: A router that has a large number of pending sessions may generate a “Memory Low” message.

  Conditions: This symptom is observed on a Cisco router when 32,000 PPPoEoA sessions are brought up simultaneously and occurs because of limited resources while call admission control is not strictly enforced. In this situation, the remote PPPoE software or host software do not respond fast enough.

  Workaround: Do not bring up 32,000 PPPoEoA sessions simultaneously. Rather, bring up the sessions in increments, for example, bring up 10,000 sessions, then another 10,000 sessions, and then the remaining 12,000 sessions.

- CSCsd20327

  Symptoms: Web Cache Communication Protocol (WCCP) for service 90 is going up and down on a Cisco router that runs Cisco IOS Release 12.4(3b)B. The router has services 81, 82 and 90 configured. The only service that has a problem is 90. The packet traces indicate that the router is sometimes responding to “Here_I_Am” messages from the cache with “I_See_You” messages that contain an incorrect destination IP address. This situation leads to a loss of WCCP service.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(3b) but may also affect other releases.

  Workaround: There is no workaround.

- CSCsd22712

  Symptoms: A memory leak may occur on a SIP-200 when you perform an OIR of a SPA that is installed in the SIP-200 and that has a large service policy applied at the ATM subinterface level.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router. The amount of memory that leaks depends on the number of subinterfaces to which the service policy is applied and the number of class maps for each service policy.

  Workaround: Do not perform an OIR of a SPA that has a relatively large service policy.

- CSCsd29469

  Symptoms: SNMP polls hang at a specific point, after which there is no response for a long time. Then, SNMP polling works fine for a while until it hangs again at a specific point.

When SNMP becomes unresponsive, the following error message may be generated, and SNMP queries may time-out at the application:

```
%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
```

Conditions: These symptoms are observed under the following conditions:

- After a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF2 have been polled for a while.
- After the CISCO-ENHANCED-MEMORY-POOL-MIB is polled on a Cisco 7600 series router that has a Supervisor Engine 720 that runs Cisco IOS Release 12.2(33)SRA.

Workaround: Exclude the CISCO-ENHANCED-MEMORY-POOL-MIB from the SNMP view. Enter the following commands to exclude the CISCO-ENHANCED-MEMORY-POOL-MIB:

```
snmp-server view public-view iso included
snmp-server view public-view ciscoMemoryPoolMIB excluded
snmp-server view public-view ciscoEnhancedMemPoolMIB excluded
snmp-server community public view public-view RO
```

This view should be applied to all community strings that might be used to poll these MIB modules. If views are already applied to a community string then the one above and the existing view should be merged.

If SNMPv3 is in use then this view should be applied to any SNMPv3 groups configured as well.

There is no need to reboot the platform. The symptom should resolve itself within a few minutes. If you must immediately clear the symptom, enter the following two commands (use one of the SNMP server community string commands that are actually configured on the router instead of the ones that are mentioned in the example below, which are based on the information that is presented above):

Disable SNMP and stop the processes:

```
no snmp-server
```

Re-enable SNMP and restore the SNMP configuration:

```
snmp-server community public view public-view RO
```

Further Problem Description: When you enable the **debug snmp packet** command, you can see that the SNMP poll requests are not being acknowledged. However, the output of the **show snmp counters** command shows about the same number of SNMP requests as the number of outputs, even though these outputs were never processed and sent.

- CSCsd33837

  Symptoms: The crypto IPsec and IKE SSO clients do not function, preventing the HA redundancy progression sequence from working correctly, and causing the standby RP to reload.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for SSO and encryption.

  Workaround: There is no workaround.

- CSCsd36608

  Symptoms: A memory leak may occur in the interprocess communications (IPC) when a line card is reset.

  Conditions: This symptom is observed on a Cisco router that is configured for In Service Software Upgrade (ISSU).

  Workaround: There is no workaround.

- CSCsd38693

  Symptoms: Renaming a file to a string that contains multiple trailing dots (“.” characters) corrupts the file system on ATA, CF, and USB flash storage devices.

  Conditions: This symptom is observed when you enter the following commands to rename the file:

  ```
  rename disk0:file2 disk0:file3...
  ```

  Workaround: Avoid renaming a file that contains multiple trailing “.” characters. When the symptom has occurred and the file system is no longer accessible, you must reformat the disk by entering the **format disk0:** command.

- CSCsd40211

  Symptoms: After you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface, ARP may be delayed. After 5 to 30 minutes, ARP finally appears for the interface in the MAC address table of the switch processor.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXD4 or Release 12.2(18)SXE4 and that is configured for NetFlow. The symptom may also affect other releases such as Release 12.2SR.

  Workaround: There is no workaround.

- CSCsd43211

  Symptoms: A SIP-200 may crash when it has a channelized SPA that has a multilink bundle, an LFI configuration, and more than two links in the bundle.

  Conditions: This symptom is observed on a Cisco 7600 series when an SSO or RPR+ switchover occurs while traffic is processed near the line rate, that is, at about 75 percent of the line rate.

  Workaround: There is no workaround.

- CSCsd47475

  Symptoms: A Cisco Catalyst 6000 series switch or Cisco 7600 series router may not be able to resolve ARP requests.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an enhanced FlexWAN module (WS-X6582-2PA) in which a 100BASE-TX port adapter (PA-FE-TX) and an IPSec VPN Acceleration Services Module (WS-SVC-IPSEC-1) are installed.

  Workaround: Configure a static ARP entry.

- CSCsd50101

  Symptoms: When you enter the **issu loadversion** *active-slot active-image standby-slot standby-image* command, the active RP may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series that functions in SSO mode. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsd68445

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: You may not be able to apply a QoS policy map with class-based shaping that is configured in the default class on a dot1q subinterface, and the following error messages may be generated:

     Configuring this shaping class will impact guarantees in other classes under this policy-map

Condition 1: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(27)SBC2 when a hierarchical QoS policy is configured in the following way and when the shape rate is higher than the CIR rate:

```
policy-map child-qos
class user-defined-class priority
police cir cir-rate bc Bc be Be
conform-action transmit
exceed-action drop

policy-map parent-qos
class class-default
shape average shape-rate
service-policy child-qos
```

Workaround 1: There is no workaround.

2. Symptom 2: You may not be able to apply a QoS policy map with class-based shaping that is configured in the default class on a dot1q subinterface, and the following error messages may be generated:

   Configuring this shaping class will impact guarantees in other classes under this policy-map

   Condition 2: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(27)SBC2 when a single policy map with class-based shaping is configured in the following way:

   ```
   policy-map shaping-qos
   class class-default
   shape average shape-rate
   ```

   Workaround 2: Perform the following steps:

   1) Configure a new class map that has the same characteristics as the original class default as in the example below, in which the new class map is called “my-class-default”:

   ```
   class-map match-all my-class-default
   match any
   ```

   2) Configure the new policy map by using the just created class-default equivalent class (“my-class-default”) as following example, in which the new policy map is called “my-policy-map”:

   ```
   policy-map my-policy-map
   class my-class-default
   shape average shape-rate
   ```

   3) Apply the service policy (“my-class-default”) to the dot1q subinterface.

- CSCsd69480

  Symptoms: When links flap on an interface of a PA-MC-STM1 port adapter that is installed in an enhanced FlexWAN module, the following error message may be generated:

  ```
  %HYPERION-4-HYP_RESET: Hyperion Error Interrupt. Resetting ASIC.
  ```

  The output of the **show interface stats** command shows line errors for the flapping line.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that run Cisco IOS Release 12.2(17d)SXB9 but may also occur in other releases.

  Workaround: There is no workaround.

- CSCsd70321

  Symptoms: Traffic stops flowing when you reset a line card and immediately afterwards an SSO switchover occurs.

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

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the line card.

- CSCsd70948

  Symptoms: After an SSO switchover occurs, the supervisor engine stops receiving BPDUs and CDPs. You must reload the platform to enable the platform to receive CDP and BPDUs.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when rate-limiting of layer 2 BPDUs is enabled through the **mls rate-limit layer2 pdu** command.

  Workaround: Disable rate-limiting of layer 2 BPDUs by entering the **no mls rate-limit layer2 pdu** command.

- CSCsd71047

  Symptoms: When the MAC address of a local-source address in a NAT configuration is changed, for example because of a failover between NICs, the corresponding NetFlow entry is not updated, causing return traffic to continue to be send to the old MAC address. In turn, this situation causes traffic to be dropped at the destination or to be send to an incorrect interface until the NetFlow entry times out or is cleared.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when either static NAT or dynamic NAT is configured.

  Workaround: Clear the corresponding NetFlow entry by entering the **clear mls netflow ip destination** *ip-address* command.

- CSCsd75273

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

- CSCsd76528

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: None of the policy classes after the first child policy of a hierarchical QoS policy take effect when you reload the router.

     Condition 1: This symptom is observed on a Cisco 7304 that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

     Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **service-policy output** interface configuration command to enable the child policies to take effect. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

  2. Symptom 2: On a Cisco 10000 series that is configured with hierarchical queueing policies, when you remove the **match vlan** command for a VLAN that matches a dot1q subinterface, the queues that are allocated to the subinterface are not cleared, allowing traffic to continue to flow through these queues.

     Condition 2: This symptom is observed on a Cisco 10000 series that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

Workaround 2: There is no workaround. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

- CSCsd77207

  Symptoms: Hardware-switching of bidirectional PIM traffic may not function when a large number of subinterfaces (about 200) are configured via the **copy** command because the existing multicast hardware entries are unexpectedly removed.

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

  Workaround: Do not configure the subinterfaces via the **copy** command. Rather, configure the subinterfaces manually.

- CSCsd77751

  Symptoms: A router may sends empty or blank syslog messages. For example, this situation may occur after the following error messages have been generated:

  ```
  %SYS-3-LOGGER_FLUSHING, %OIR-SP-STDBY-6-CONSOLE, %SYS-SP-STDBY-3-LOGGER_FLUSHED,
  %PFREDUN-SP-STDBY-6-ACTIVE ...
  ```

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

  Workaround: There is no workaround.

- CSCsd80632

  Symptoms: A change to the 64-bit high capacity (HC) input traffic counter of a main interface does not equal the sum of the changes for the HC input traffic counters of its subinterfaces.

  Conditions: This symptom is observed on a Cisco router that is configured for SNMP when the main interface is configured for Frame Relay.

  Workaround: There is no workaround.

- CSCsd80745

  Symptoms: A router that is configured for IPSec and ISAKMP may reload unexpectedly because of a bus error exception that is triggered by an address error exception.

  Conditions: This symptom is observed rarely during ISAKMP negotiation when a new IKE SA is being negotiated. The symptom is more likely to occur when low lifetimes are used for IKE and IPSec rekeying.

  Workaround: There is no workaround.

- CSCsd81275

  Symptoms: When a standby supervisor engine or standby RP comes up, the following error message may be generated:

  ```
  %PFINIT-SP-1-CONFIG_SYNC_FAIL: Sync'ing the private configuration to the standby
  Router FAILED, the file may be already locked by a command like: show config.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for ISSU.

  Workaround: There is no workaround.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS, documented as Cisco bug ID CSCsd85587
- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM)

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

- CSCsd87844

  Symptoms: When a route distinguisher (RD) that is configured for a VRF is deleted and then reconfigured, the standby RP may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that has dual RPs that function in HA mode and that is configured for MPLS VPN.

  Workaround: Delete the VRF itself and then reconfigure the VRF in order to change the RD. If this is not an option, there is no workaround.

  Further Problem Description: The symptom occurs because the processing of the **no rd** command is completed only on the active RP only. On the standby RP, the processing does not clear a flag that signals the completion of the processing **no rd** command. Then, when the RD is reconfigured, the configuration succeeds on the active RP but fails on the standby RP, causing the standby RP to reload.

- CSCsd88401

  Symptoms: Incoming packets may be dropped at the GE-WAN port 2 on an OSM-2+4GE-WAN+. In addition, the output of the **show platform hardware gt48520 counters** command shows that “mac_rx_error” errors for the OSM-2+4GE-WAN+ are increasing.

  Conditions: This symptom is observed on a Cisco 7600 series that processes IPv4 TCP and UDP packets with a random data pattern on an OSM-2+4GE-WAN+ with hardware revision 2.4 or lower. Note that the symptom occurs only on GE-WAN port 2, not on the other ports.

  Workaround: There is no workaround.

Further Problem Description: Both upgrade the Cisco IOS software image to an image that integrates the fix for caveat CSCsd88401 and change the hardware revision of the OSM-2+4GE-WAN+ to 2.5.

- CSCsd88636

  Symptoms: Continuous CPUHOGs may occur during the “ATM OAM Input” process, locking the console for a long time.

  Conditions: This symptom is observed on the MSFC of a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA and that has an ATM interface with several VCs that are configured for Single Cell Relay (VC Mode). These VCs are configured on a PA-A3-OC3 or PA-A6-OC3 port adapter that is installed in an enhanced FlexWAN module. The symptom occurs after the peer router that is connected to the ATM interface (and on which the PVPs are configured) is reloaded.

  Note that the symptom is not platform- or release-dependent.

  Workaround: When the console is less busy, shut down the ATM interface on the peer router. The CPUHOGs may stop after some time. If this is not an option, there is no workaround.

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  – Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  – Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  – Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd96436

  Symptoms: Non-aggregate random-detect configurations are accepted in service policies that are applied to interfaces on a SIP-600. However, the SIP-600 supports only aggregate random detect configurations.

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

Workaround. Remove any non-aggregate random-detect configurations, and only use aggregate random-detect configurations.

- CSCsd97648

  Symptoms: After more than one switchover has occurred on a router that is configured with a source Encapsulated Remote SPAN (ERSPAN) session, the bit rate of the destination port for the source ERSPAN session drops from the expected rate. For example, even though there are 560,000 packets on the monitored port, only 440,000 packets are counted on the ERSPAN destination port.

  Conditions: This symptom is observed on Cisco 7600 series after more that one switchover has occurred without a system reset.

  Workaround: Remove and reconfigure the ERSPAN source session to restore the data rate.

- CSCsd98390

  Symptoms: A WS-X6148A-45AF module may not boot when you power-cycle the platform. The output of the **show module** shows the module status as "unknown." In addition, one or more modules may lose their configuration.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with eight or more modules.

  Workaround: Do not power-cycle the platform but enter the **reload** command.

- CSCsd98686

  Symptoms: The following error message and traceback may be displayed:

  ```
  %XDR-6-CLIENTISSUBADTXTFM: Failed to xmit_transform message - to slot 6, client CEF
  push, context 0
  -Traceback= 41437E50 4141D584 41432B64 4141D674 41421558 414219DC 41416388 413F4738
  413F4EA0 403E11D0 402652A8 40402AD0 404F23F8 404F23E4
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for SSO and that has dCEF enabled by default. The symptom occurs when you disable dCEF and then re-enable it, for example by entering the no **ip cef** command followed by the **ip cef distributed** command or the **no ip routing** command followed by the **ip routing** command.

  Workaround: There is no workaround.

- CSCse00135

  Symptoms: When MLPoMPLS is configured, a VC comes up but, the first few ping packets from one CE router to another CE router on the far end do not go through.

  Conditions: This symptom is observed in a configuration with Cisco 7600 series routers that functions as CE and PE routers.

  Workaround: There is no workaround. Note that the connectivity recovers after a few pings.

- CSCse00843

  Symptoms: On a router that has an ATM subinterface that is in the "shut" state and that has a PVP that is configured for Xconnect, the standby RP continuously generates the following error message when the router is booted:

  ```
  %CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR: Interface Configuration command 261 playback
  failed for slot 4/1.
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with dual Supervisor Engine 720 modules. The symptom could also occur on other routers.

  Workaround: Enter the **no shutdown** interface configuration command on the ATM subinterface.

- CSCse03277

  Symptoms: When a tunnel is removed and reconfigured, the tunnel interface may not come up.

  Conditions: This symptom is observed on a Cisco router that has a tunnel that is configured on a Virtual Tunnel Interface (VTI).

  Workaround: Shut down the tunnel before you unconfigure the IP address of the tunnel interface, disable the VTI tunnel mode, or remove the VTI tunnel itself.

- CSCse05336

  Symptoms: A subinterface of an OSM-2+4GE-WAN+ that is passing traffic may drop some packets when you create a new subinterface or delete an existing subinterface on the same physical interface as the subinterface that is passing traffic.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF3. The symptom may also affect Release 12.2(33)SRA.

  Workaround: There is no workaround.

- CSCse07011

  Symptoms: After an SSO switchover, traffic may fail on a connection that is configured for Frame Relay-to-Ethernet VLAN Interworking over L2TPv3.

  Conditions: This symptom is observed on a Cisco router that is configured with dual RPs and that functions as a PE router.

  Workaround: There is no workaround.

- CSCse09498

  Symptoms: When you enter the **no shutdown** interface configuration command on an auto-template interface during deployment, some tunnels may be in the up/down state, and the tunnel mode may be GRE instead of the configured tunnel mode of MPLS.

  Conditions: This symptom is observed on a Cisco router with about 70 primary MPLS TE tunnels. The symptom occurs when you first enter the **no interface auto-template** command, then you enter the **tunnel mode mpls traffic-eng** command, and finally you paste the template back.

  Workaround: Reload the router.

  Alternate Workaround: Create an automesh in the following sequence:

```
conf t
access-list 60 permit 10.0.7.3
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12

interface Auto-Template1
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination access-list 60
tunnel mode mpls traffic-eng

........
access-list 60 permit 10.0.7.3
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
```

```
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12
```

- CSCse11794

  Symptoms: A SIP-200 or SIP-400 may crash when you configure 12,000 bridged VCs along with a service policy on an ATM SPA that is installed in the SIP.

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

  Workaround: There is no workaround. To prevent the symptom from occurring, do not configure more than 1000 bridged VCs when there is also a service policy.

- CSCse12154

  Symptoms: A router may crash because of a bus error when you enter the **copy scp** command to copy a configuration.

  Conditions: This symptom is observed on a Cisco router that is configured for SSH.

  Workaround: Do not use SCP. Rather, use Remote Copy Protocol (RCP) or use a TFTP transfer.

- CSCse12195

  Symptoms: Connected ports on a Cisco Catalyst 6000 series or Cisco 7600 series may transition from the up state to the down state with no apparent cause.

  Conditions: This symptom is observed on a 16-port Gigabit Ethernet GBIC line card (WS-X6816-GBIC) when the following two conditions are met:

  – A 1000Base-T GBIC is inserted after the WS-X6816-GBIC has been powered up.

  – Port 1 is enabled, not connected, and set to auto-negotiate.

  Workaround: Disable auto-negotiation on port 1 by entering the **speed nonegotiate** command.

  First Alternate Workaround: Remove all 1000Base-T GBICs that are in use, reset the WS-X6816-GBIC, and refrain from using 1000Base-T GBICs.

  Second Alternate Workaround: Disable port 1.

- CSCse13736

  Symptoms: On a Cisco platform that has 3000 or more IPv6 multicast streams, drops may occur for some of the streams.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that run Cisco IOS Release 12.2(18)SXF2, Release 12.2(33)SRA, or Release 12.2(33)ZW.

  Workaround: There is no workaround.

- CSCse14269

  Symptoms: The encapsulation and decapsulation counters in the output of the **show crypto ipsec sa stats** command are inaccurate because they are not updated correctly during a rekey.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an IPsec VPN SPA.

  Workaround: Do no set the IPsec SA lifetime to prevent rekeying of the IPsec SA.

- CSCse17034

  Symptoms: When the **crypto engine slot** command is applied to a subinterface but not to the main interface, the command does not take effect.

Conditions: This symptom is observed on a Cisco 7600 series that is configured with an IPSec VPN SPA (SPA-IPSEC-2G).

Workaround: Enter the **crypto engine slot** command for both the main interface and the subinterface.

- CSCse17175

  Symptoms: The line protocol may go down on some of the serial interfaces of a 1-port multichannel STM-1 single mode port adapter.

  Conditions: This symptom is observed on a Cisco router when the maximum number of channel groups (256) is configured on the port adapter.

  Workaround: There is no workaround.

- CSCse17380

  Symptoms: Buffer exhaustion may occur in an AToM IP interworking scenario.

  Conditions: This symptom is observed rarely on a Cisco 7600 series that functions as a PE router and that receives many ARP requests at a fast rate from a CE router that are processed at the process level. The symptom occurs when the router does not have sufficient buffers available to deal with the ARP requests.

  Workaround: There is no workaround.

- CSCse17960

  Symptoms: A Cisco 7304 that has an NPE-G100 processor may access a bad virtual address and reload unexpectedly.

  Conditions: This symptom is observed when traffic flows to an ATM VC that is configured for MLP with a QoS policy and when the Qos policy has a priority class.

  Workaround: There is no workaround.

- CSCse18146

  Symptoms: A line card may reset unexpectedly when it receives traffic after a switchover of the RP has occurred.

  Conditions: This symptom is observed on a Cisco 7600 series when NBAR is configured on an interface of the line card via the **match protocol** *protocol-name* command that is contained in a policy that is attached to the interface.

  Workaround: Disable NBAR by removing the **match protocol** *protocol-name* command.

- CSCse19299

  Symptoms: Some packet drops may occur during SA negotiation between two spokes. The expected behavior is that during SA negotiation between the spokes, the traffic should flow through spoke-to-hub tunnels. Note that when the spoke-to-spoke SA is up, traffic flows fine without any packet drops.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCse19351

  Symptoms: On a Cisco 7600 series that has an IPsec VPN SPA, traffic may not pass through an IPsec tunnel when the destination is reached through a front-door VRF (FVRF).

The symptom typically occurs in the following configuration:

```
interface Tunnel105
 ip vrf forwarding black
 ip address 10.0.0.1 255.0.0.0
 tunnel source 10.0.1.1
 tunnel destination 10.0.0.2
 tunnel vrf temp2044
 tunnel protection ipsec profile ipsec_black_105
 crypto engine slot 3/0 inside
```

Conditions: This symptom is observed when the internal VRF table ID that is associated with a FVRF is greater than 1024.

In the example above (in the Symptoms section), the internal VRF table ID that must be confirmed is “temp2044”; enter the **show ip vrf detail temp2044** command to identify the internal VRF table ID.

Workaround: Limit the number of VRFs that are defined on the router to less than 1024.

- CSCse19687

  Symptoms: “%SYS-3-CPUHOG” messages may be generated after an RPR+ switchover has occurred.

  Conditions: This symptom is observed on a Cisco router that is configured with 4000 EoMPLS VCs, each of which has a Qos policy applied.

  Workaround: There is no workaround.

- CSCse20150

  Symptoms: A SPA may cause an RX FIFO FULL error message to be generated on the RP. When this occurs, a VC_CONFIG error message is generated, and subsequently all interfaces on all SPAs that are switching traffic go down.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for MLP or MFR when traffic with 46-byte size packets exceeds about 350 kpps on the MLP or MFR bundles.

  Workaround: When the symptom has occurred, reload the SIP with the affected SPA. To prevent the symptom from occurring, ensure that traffic does not exceed about 350 kpps on the MLP or MFR bundles. If this is not an option, there is no preventive workaround.

  Further Problem Description: The following is an example configuration in which the symptom occurs:

  Consider 110 bundles with 6 members with 4 DS0 interfaces, so each bundle has 1.5 Mbps of bandwidth. When you send an IP packet of 46 bytes, the maximum traffic that will flow through the SIP is as follows:

  110 Bundles * (1536kbps * 1000bits) / (8 * (46bytes + 13bytes)) = 357965 pps (rounded to about 350 kpps)

- CSCse20340

  Symptoms: Upon recovery from a microcode reload on a line card or a router bootup, the controller state for a serial interface of a 2-port or 4-port T3/E3 SPA may remain in the “down” state.

  Conditions: This symptom is observed on a Cisco 7600 series and Cisco 12000 series.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected serial interface to enable the interface to enter the “up” state.

- CSCse22153

  Symptoms: The following error messages may be generated on the console of the standby RP when MPLS TE tunnels are deleted and then added while the standby RP reloads.

  ```
  %IDBINDEX_SYNC-STDBY-3-IDBINDEX_ENTRY_LOOKUP: Cannot find IDB index table entry: "", 0
  ```

  ```
  %COMMON_FIB-STDBY-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface for Tunnel5 with illegal if_number: -1
  ```

  Conditions: This symptom is observed in an MPLS network that has multiple TE tunnels.

  Workaround: Do not delete and add MPLS TE tunnels while the standby RP reloads.

- CSCse23918

  Symptoms: A router may crash when the Pseudowire Redundancy feature is enabled and when a failover occurs from a pseudowire-type link (that is, an AToM link) to an access circuit (that is, a Frame Relay link).

  Conditions: This symptom is observed on a Cisco 7301 and Cisco 7304 when you attempt to unprovision an Xconnect circuit that is configured on a PA-A6 port adapter. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCse24691

  Symptoms: When MLD snooping is enabled and MLD leaves are sent from the last host in a Layer 2 environment, the MAC entry is not cleared but remains in the MLD snooping table. The port list of the MAC entry does not include the last port that was used but points only to the router.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: There is no workaround.

  Further Problem Description: As long as the MLD snooping table is not full, the symptom is harmless. (The default size of the MLD snooping table is 32 KB.) When the MLD joins are sent, the port list is automatically populated. When MLD snooping table is full, the traffic to any new groups is flooded to all Layer 2 ports.

- CSCse26682

  Symptoms: When you enter the **no ipv6 unicast-routing** command followed by the **ipv6 unicast-routing** command, prefixes may be missing from the IPv6 CEF table on a line card. This situation may cause traffic loss.

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

  Workaround: Although you can enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command for every interface that is configured for IPv6, doing so is inefficient. It is more efficient and less disruptive to enter the **clear cef table ipv6** command.

- CSCse26941

  Symptoms: A Cisco 7304 may reload unexpectedly because of a bus error when you enter the **cef table output-chain build favor convergence-speed** command.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB. However, the symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCse28172

  Symptoms: RIP routes that point to the dialer interface remain in the routing table when a DSL link goes down. However the routes are removed from the RIP database.

  Conditions: This symptom is observed on a Cisco 877 that runs Cisco IOS Release 12.4(4)T1 or Release 12.4(6)T when the dialer interface is located within a VRF. The symptom is both platform- and release-independent.

  Workaround: Clear the routing table.

- CSCse30293

  Symptoms: A ping may not go through an IPsec tunnel on a Cisco 7600 series after you have copied a configuration from a disk device to the running configuration.

  Conditions: This symptom is observed on a Cisco 7600 series system that has an IPsec VPN SPA on which tunnels with tunnel protection are configured.

  When the symptom occurs, the encryption and decryption counters in the output of the **show crypto ipsec sa** command for the affected IPsec tunnel do still increment, but a ping to the tunnel IP address does not go through. The output of the **show interface tunnel** *number* shows the tunnel interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected tunnel interface.

- CSCse31859

  Symptoms: The **monitor session** *session* **destination interface** *type/slot/port* command does not function.

  Conditions: This symptom is observed on a Cisco 7600 series after you have configured a Remote SPAN (RSPAN) VLAN.

  Workaround: There is no workaround.

- CSCse33543

  Symptoms: The IKE SA setup may fail when the IKE SA number exceeds 255.

  Conditions: This symptom is observed on a Cisco router that is configured for RSA-Sig as the IKE SA authentication method.

  Workaround: There is no workaround.

- CSCse34615

  Symptoms: A RADIUS virtual server drops RADIUS accounting on and off packets, instead of forwarding the packets to the real servers. The client never receives response packets for the RADIUS accounting on and off packets that were sent.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series.

  Workaround: There is no workaround.

- CSCse34697

  Symptoms: When you configure a crypto map and enter the **reverse-route remote-peer** command, the reverse route that is injected by IPsec when the IPsec tunnel comes up may point to an incorrect interface.

  Conditions: This symptom is observed when the following occurs:

  1. You apply a crypto map to one interface (A).
  2. You apply a crypto map to a second interface (B).
  3. You remove the crypto map from the second interface (B).

In this situation, when the IPsec tunnel comes up, IPsec points to the second interface (B) instead of the first interface (A).

Workaround: To ensure that the reverse route points to the correct interface, re-apply the crypto map to the first interface (A).

- CSCse37587

  Symptoms: When DHCP snooping is enabled in conjunction with VRF, DHCP clients do not receive a DHCP IP address.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that function as a DHCP server.

  Workaround: There is no workaround.

- CSCse38650

  Symptoms: A router that functions as a BGP Route Reflector in an multicast VPN environment may displays error messages and may eventually crash.

  Conditions: This symptom is observed when the router receives multicast updates and attempts to send multicast updates in which it sets itself as the next hop.

  Workaround: There is no workaround.

- CSCse39330

  Symptoms: A router does not boot when you first enter the **secure boot-image** command followed by the **format disk** command and then you use the secure image to attempt to boot the router.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

  Workaround: There is no workaround.

- CSCse39956

  Symptoms: When a pseudowire VC that has negotiated to use of the Control Word (that is, Cbit = 1) is followed by another pseudowire VC) that has negotiated to not use the Control Word (i.e., Cbit = 0), the Control Word (CW) may still be prepended to the pseudowire VC that has negotiated to not use the CW. As a result, the disposition router (or tail endpoint) does not expect a CW and cannot decapsulate the VC packet; instead, the packet is dropped at the disposition router as a corrupted packet.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a SIP-600 and that function in a VPLS environment as egress PE routers.

  Workaround: Ensure that VCs in a VPLS environment do not have a mixture of negotiated CWs (that is, Cbits). The output of the **show mpls l2transport binding** command shows the VCs and Cbits.

  Further Problem Description: One scenario in which the symptom occurs is the following:

  – A VPLS hub-spoke environment is created with a mixture of hardware-based and software-based EoMPLS VCs.

  – When the SIP-600 detects the CW setting for one VC, it assumes that the VC that follows the first VC also has the CW, and inserts the CW.

  – When a hardware-based EoMPLS VC is in the middle of the replication chain, ping failures may occur for CE routers that are located behind the hardware-based EoMPLS VC. A hardware-based EoMPLS VC does not support the CW and ping failures occur because the MAC address of the customer becomes corrupted.

- CSCse41366

  Symptoms: A ping between two CE routers may fail.

  Conditions: This symptom is observed on a Cisco router that is configured for AToM.

  When the symptom occurs, the outputs of the **show mpls l2 vc detail** and **show ssm segment id** commands may show that the connection between the CE routers is up, but the output of the **show sss session** command does not show a session between the CE routers.

  Workaround: There is no workaround.

- CSCse41480

  Symptoms: The CoS VLAN priority may be changed and become corrupted when MPLS packets are sent over an EoMPLS tunnel on Cisco 7600 series even when the **mls qos trust cos** command is enabled on the ingress interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXE2 or Release 12.2(18)SXF4 but may also affect other releases that run on the Cisco 7600 series. The symptom occurs only when packets with Ethertype 8847 and 8848 are processed on the ingress interface, causing an incorrect MPLS EXP bit to be assigned on the ingress interface.

  Note that the symptom does not occur when the payload is IP (Ethertype 0800) or any other Ethertype.

  Workaround: There is no workaround. (However, see the Further Problem Description.)

  Further Problem Description: The fix for this caveat does not resolve the underlying hardware issue but, as a workaround, it does allow you to configure an ingress marking policy on the EoMPLS interface, to match on the incoming MPLS EXP bit values (that is, value 0 through 7), and to set the marking to the same value.

- CSCse45322

  Symptoms: When a tunnel is configured for Path MTU discovery, the configuration may not be propagated from the RP to an IPSec VSA SPA, preventing Path MTU discovery from functioning.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and may occur when a tunnel is configured for the first time after a reboot.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the tunnel interface to force the configuration to be properly propagated to the IPSec VSA SPA.

  Alternate Workaround: Remove and add back the Path MTU discovery configuration.

- CSCse47732

  Symptoms: RFC 1407 and RFC 2496 are not supported on a 1-port channelized STM1/OC3 SPA.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when SNMP queries are performed for CISCO-DS3-MIB objects.

  Workaround: There is no workaround.

- CSCse49388

  Symptoms: On a physical interface or subinterface on which a tunnel is configured and that encrypts or decrypts traffic, when you shut down and bring up the physical interface or subinterface multiple times, MAC entries for all VLANs that support the tunnel may be removed.

  When this situation occurs, when the “RMac reference” counter reaches 1, and when you shut down the physical interface or subinterface for the last time, packets are prevented from traversing the tunnel.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with either a Supervisor Engine 32 or a Supervisor Engine 720 and with a SIP-400 in which an IPsec VPN SPA is installed.

Workaround: To prevent the symptom from occurring, do not shut down and bring up the physical interface or subinterface that supports the IPsec tunnel. When the symptom has occurred, reload the SIP-400 to reset the "RMac reference" counter to the original value.

Further Problem Description: To see if the symptom has occurred, check the "RMac reference" counter as follows:

```
# remote login switch
sp# test mls net debug task 1 stat
...
Netflow RMac List:
0013.5f21.9100[14] <<-- where [n] is the reference count, in this case 14.
Tunnel Interface(s):
...
sp#
```

You can check the counter each time after you have shut down and brought up the physical interface or subinterface. If, after every iteration, the reference count keeps decrementing towards 0, it means the symptom has occurred. A flapping link does not cause this problem. The "RMac reference" counter decreases each time that you shut down the physical interface or subinterface, perform and OIR of the SPA, or reset the SPA.

- CSCse51721

  Symptoms: Counters do not increment when you run the CISCO-SONET-MIB. However, when you enter the **show controllers sonet** command, the counters show properly.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a channelized STM-1 SPA (SPA-1xCHSTM1/OC3) that receives error packets.

  Workaround: There is no workaround.

- CSCse52951

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

- CSCse56921

  Symptoms: A platform that is configured for GPRS Tunneling Protocol (GTP) Server Load Balancing (SLB) may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when the same International Mobile Subscriber Identity (IMSI) is sent in two or more Packet Data Protocol (PDP) requests to different virtual servers and occurs when the sticky table entries time-out.

  Workaround: There is no workaround.

- CSCse62370

  Symptoms: A router may crash when you attach a map class to a Frame Relay data-link connection identifier (DLCI) interface.

  Conditions: This symptom is observed on a Cisco router that is configured with an output policy with Frame Relay Traffic Shaping.

  Workaround: There is no workaround.

- CSCse62462

  Symptoms: When a GRE tunnel is routed over an MPLS cloud, process-switched packets that are destined for the remote end of the GRE tunnel are sent unlabeled.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S when the router functions as a PE router that has a GRE tunnel configured within a VRF that is sourced from another VRF.

  Workaround: There is no workaround.

- CSCse68138

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)
  – Media Gateway Control Protocol (MGCP)
  – Signaling protocols H.323, H.254
  – Real-time Transport Protocol (RTP)
  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCse69713

  Symptoms: When all cache engines in a WCCP service group are inactive, the traffic is handled by the software; the traffic is CEF-switched by the software instead of FIB-switched in the hardware.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Remove and re-enter the **ip wccp webcache** command.

- CSCse73539

  Symptoms: A Supervisor Engine 720 may crash because the EOBC channel is jammed when you insert a second Supervisor Engine 720 in the chassis.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series.

  Workaround: There is no workaround.

- CSCse74713

  Symptoms: Pings may fail across a link on an ATM SPA that is configured for MLP, LFI, and VRF forwarding and that is installed in a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: Reload the router and reapply the VRF configuration to the virtual template.

  Further Problem Description: The symptom does not occur in Release 12.2.18SXF4 and earlier releases.

- CSCse75429

  Symptoms: An LDP neighbor does not come up when the MPLS LDP Graceful Restart feature is enabled.

  Conditions: This symptom is observed when the forwarding state holding timer of the MPLS LDP Graceful Restart feature is configured to a value that is less than 120 seconds, causing the LDP session to be brought down.

  Workaround: Configure the forwarding state holding timer to a value that is greater than or equal to 120 seconds.

- CSCse75904

  Symptoms: RADIUS accounting updates may still be sent periodically for users that have already disconnected.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an IPSec VPN Services Module.

  Workaround: There is no workaround.

- CSCse76036

  Symptoms: In an MPLS TE FRR configuration, a point of local repair (PLR) router may insert an MPLS label that has a value of 3 (that is, an implicit null label) into the outgoing label stack. This situation prevents traffic from being forwarded.

  Conditions: This symptom is observed on a Cisco 7600 series when the primary TE tunnel is a one-hop tunnel that is configured for implicit null labels and LDP. For an MPLS L3VPN prefix, the outgoing packets have a label stack of “3, ldp label, vpn label.” The correct label stack in this case should be “ldp label, vpn label.”

  Workaround: Configure the one-hop primary TE tunnel for explicit-null labels as the outgoing labels.

- CSCse77427

  Symptoms: The throughput performance may be adversely affected on a Cisco 7600 series that has a SIP-600 in which a 1-port 10 Gigabit Ethernet SPA or 10-port Gigabit Ethernet SPA is installed that is configured for Hierarchical Virtual Private LAN Service (H-VPLS) with traffic engineering (TE) tunnels.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when the 1-port 10 Gigabit Ethernet SPA or 10-port Gigabit Ethernet SPA processes incoming packets at 50 percent of the line rate and has the TE tunnels disabled after they were previously enabled for the incoming traffic.

  Workaround: There is no workaround.

- CSCse77758

  Symptoms: The secondary RP may fail to boot (that is, reach the SSO mode) after the **ipv6 unicast-routing** command is disabled on the primary RP. During the reboot of the secondary RP, the following message is displayed on its console:

  ```
  %Cannot disable IPv6 CEF on this platform
  ```

  On the primary RP, the following messages are displayed on its console:

  ```
  Config Sync: Starting lines from PRC file: -no ipv6 cef
  Config Sync: Bulk-sync failure, Reloading Standby
  ```

  Conditions: This symptom is observed on a Cisco router that has dual RPs and that runs Cisco IOS Release 12.2SB.

  Workaround: First, re-enable IPv6 by entering the **ipv6 unicast-routing** command on the primary RP. Then, reboot the secondary RP.

- CSCse77768

  Symptoms: MAC addresses may not be learned when traffic is switched from Multipoint Bridging (MPB) to Virtual Private LAN Services (VPLS).

  Conditions: This symptom is observed on a Cisco 7600 series when traffic is switched from a customer-facing interface that is configured for MPB on a SIP-400 to a core-facing interface that is configured for VPLS and EoMPLS on a SIP-200, SIP-600, enhanced 4-port Gigabit Ethernet OSM, or FlexWAN2.

  Workaround: There is no workaround.

- CSCse78568

  Symptoms: The standby RP resets continuously while loading a large configuration.

  Conditions: This symptom is observed on a Cisco 10000 series but is platform-independent.

  Workaround: There is no workaround.

- CSCse80519

  Symptoms: A router may reload when it receives an extensible markup language (XML) file.

  Conditions: This symptom is observed on a Cisco router that is configured for CNS and occurs when an XML namespace in the operation tag is being declared.

  Workaround: There is no workaround.

- CSCse83031

  Symptoms: A memory leak may occur when you remove an Xconnect configuration from a router, which can be verified by enabling the **show memory debug** command.

  Conditions: This symptom is observed when you configure Xconnect with the Exchange Fabric Protocol (EFP) and then remove the Xconnect configuration.

  Workaround: There is no workaround.

- CSCse84226

  Symptoms: When a VC is down, the output of the **show connection** command on the local side shows that the VC is up, even though the output of the **show mpls l2 vc detail** command shows that the VC is down. The output of the **show connection** command on the remote side shows that the VC is down.

  Conditions: This symptom is observed on a Cisco router that is configured for AToM when the MTU mismatches the Virtual Private Wire Service (VPWS) circuit.

Workaround: There is no workaround.

- CSCse86477

  Symptoms: A router crashes when you detach a map class from a Frame Relay DLCI interface.

  Conditions: This symptom is observed on a Cisco router that is configured with an output policy with Frame Relay traffic shaping.

  Workaround: There is no workaround.

- CSCse86912

  Symptoms: Packets are not switched.

  Conditions: This symptom is observed when you configure a VLAN for Xconnect.

  Workaround: There is no workaround.

- CSCse89636

  Symptoms: The following error messages and tracebacks are generated on a PRE-3 when an In-Service Upgrade (ISU) upgrade (that is, a hardware upgrade) occurs from a PRE-2 that runs Cisco IOS Release 12.2(27)SBB5 to a PRE-3 that runs Cisco IOS Release 12.2(31)SB:

  ```
  %LFD-3-INVINSTALLER: Wrong installer 4 for packet 0/0 update (was 1)
  %LSD-3-LABEL: can’t create rewrite for label=0
  ```

  Conditions: This symptom is observed on a Cisco 10000 series but could occur on any platform when you perform an ISU switchover.

  Workaround: There is no workaround.

- CSCse90586

  Symptoms: A Cisco 7600 series that has a large number of OSPF tunnels with VRFs may run out of memory, many MALLOC failures may occur, and the router may reload because of a “Corrupted Program Counter” error. The crash traceback that is generated is invalid.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA, that is configured for OSPF, and that has 500 tunnels with a VRF configuration.

  Workaround: Reduce the number of tunnels and VRFs in the configuration.

- CSCse90702

  Symptoms: A Frame Relay map may not be established after you perform an OIR of a line card.

  Conditions: This symptom is observed on a Cisco 7600 series when the line card is configured with an MFR bundle.

  Workaround: Create a static Frame Relay map.

  Alternate Workaround: Perform an OIR at both ends simultaneously.

- CSCse91107

  Symptoms: NSF does not function properly for VPN traffic, causing packet loss. This situation can be verified in the output of the **show ip bgp vpnv4 all labels** command.

  Conditions: This symptom is observed on an MPLS PE router after an ISSU upgrade.

  Workaround: There is no workaround.

- CSCse91675

  Symptoms: The RP may generate an “RX FIFO FULL” error message for a SPA, followed by a “VC_CONFIG” error message, and subsequently all interfaces on all SPAs that are processing traffic may go down.

Symptoms: This symptom is observed on a Cisco 7600 series that is configured with MLP or MFR bundles on a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3), 2-port channelized T3/DS0 SPA (SPA-2XCT3/DS0), or 4-port channelized T3/DS0 SPA (SPA-4XCT3/DS0) when traffic exceeds about 350 kpps on these bundles.

Workaround: After the symptom has occurred, reload the affected SPAs or the SIPs in which the affected SPAs are installed. There is no workaround to prevent the symptom from occurring. Therefore, configure the MLP or MFR bundles in such a manner that the 350 kpps threshold is not exceeded.

- CSCse94388

  Symptoms: A SIP-200 that is configured with distributed Multilink Point-to-Point (dMLP) bundles and that has some of the bundles interleaved may crash.

  Conditions: This symptom is observed when you send traffic at line rate through all of the bundles.

  Workaround: There is no workaround.

- CSCse95146

  Symptoms: A Supervisor Engine 720 with a cross-module EtherChannel duplicates all packets that enter or leave the cross-module EtherChannel on the same physical port.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series or Cisco 7600 series that has a Supervisor Engine 720 and an Enhanced FlexWAN module when the supervisor engine functions in bus mode and has a cross-module EtherChannel.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when you remove the cross-module EtherChannel or the Enhanced FlexWAN module.

- CSCse95888

  Symptoms: The bandwidth of an interface on a Fast Ethernet (FE) SPA changes unexpectedly when the interface on the other side is shut down and brought back up, or the other around, brought up and then shut down.

  Conditions: This symptom is observed on a Cisco router such as a Cisco 7600 series or Cisco 12000 series that is configured with an FE SPA.

  Workaround: Use the **bandwidth** command to configure the appropriate bandwidth.

- CSCse97422

  Symptoms: When you enter the **show tech** command with long a regular expression, the platform may crash during the display of the command output. For example, this situation may occur when you enter the following command:

  ```
  show tech |  e (0.00%  0.00%  0.00%|cmd_sts|0  0|ast clearing|packets input|packets
  output|SESs|LMI enq|cast queue|Last input|OAM cells input|reliability 255)
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 720.

  Workaround: Do not use a long regular expression when you enter the **show tech** command.

- CSCse98354

  Symptoms: The interfaces of the SPAs on a SIP-200 may enter the up/down state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXF5 but may also occur in Release 12.2(33)SR.

  Workaround: There is no workaround.

- CSCse98404

  Symptoms: When you apply an input service policy to an AToM PVC, a router may reload and generate the following error message and traceback:

  ```
  Unexpected exception to CPUvector 300, PC = 119B6D0
  -Traceback= 119B6D0 118E2F8 5952270 118FDC4 11B7680 11B78EC 236988 24BDD4 2E95CC
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S3 but is platform- and release-independent. The symptom occurs when you enter the following commands:

  ```
  Router(config)#interface x/y.z point-to-point
  Router(config-subif)# no ip directed-broadcast
  Router(config-subif)# no atm enable-ilmi-trap
  Router(config-subif)# pvc a/b l2transport
  Router(cfg-if-atm-l2trans-pvc)# encapsulation aal5
  Router(cfg-if-atm-l2trans-pvc)# xconnect a.b.c.d xy encapsulation mpls
  Router(cfg-if-atm-l2trans-pvc-xconn)#
  Router(cfg-if-atm-l2trans-pvc-xconn)#service-policy test
  ```

  Workaround: There is no workaround.

- CSCsf03566

  Symptoms: On a router that functions as an EzVPN server, a software-forced crash may occur because of memory corruption.

  Conditions: This symptom is observed on a Cisco 7600 series router that runs Cisco IOS Release 12.2(18)SXF when Extended Authentication (Xauth) is enabled while the crypto session is brought down. The symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCsf04112

  Symptoms: On a Cisco 7600 router, the MAC address of one or more interfaces may change unexpectedly when the ifPhysAddress object of the IF-MIB is accessed by SNMP. This situation prevents the router from receiving packets when an ARP entry that contains the MAC address of the router is refreshed.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: To prevent the symptom from occurring, configure static ARP on the devices that must be able to send packets to the router. After the symptom has occurred, reload the router to clear the condition.

- CSCsf04301

  Symptoms: All multicast data packets on ATM multipoint interfaces may be dropped, regardless of the number of VCs that are configured under a single multipoint interface. When this situation occurs, control plane packets still pass so that routing protocol adjacencies do come up and PIM neighbors are formed.

  Conditions: This symptom is observed on a Cisco 7600 series that has an ATM SPA.

  Workaround: There is no workaround.

  Further Problem Description: The ATM OSM is able to direct multicast packets to a single VC that is configured on a multipoint interface.

- CSCsf04530

  Symptoms: L2TP may be unable to establish a control channel.

  Conditions: This symptom is observed on a Cisco router that connects to a third-party vendor router that conforms to IETF standards but not to Cisco Attribute-Value Pairs (AVPs).

  Workaround: There is no workaround.

- CSCsf05390

  Symptoms: A Cisco 7600 series that has a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3) may generate several CPUHOG messages and may crash.

  Conditions: This symptom is observed when you create the 258th channel group on the SPA-1XCHSTM1/OC3 and then delete one of the channel groups.

  Workaround: There is no workaround.

- CSCsf07232

  Symptoms: Tcl standard I/O operations such as a **puts** command may not display text on the terminal line under which the Tcl code is running. The text may be displayed on the terminal line that was the first one to connect (for example, vty0) or may not be displayed anywhere. Both print to standard output (STDOUT) and standard error (STDERR) streams are affected.

  Conditions: This symptom is observed on a Cisco router when more than one user is logged into a device, when one user enters Tcl Shell mode via the **tclsh** command, and then a second user enters Tcl Shell mode.

  Workaround: Ensure that only one user is connected to the device when Tcl standard I/O operations are run. If this is not an option, there is no workaround.

  Further Problem Description: When Tcl standard I/O operations are run on vty0 with only one user logged in, the text is displayed correctly.

- CSCsf09186

  Symptoms: When you enter the **show ip route** command to check on the installed routes, the output does not show the routes that have been installed by the RIP.

  Conditions: This symptom is observed on a Cisco router when redistribution is enabled under the RIP.

  Workaround: There is no workaround.

- CSCsf11182

  Symptoms: The output of the **show policy-map interface** *interface-name* **vp** *vpi* **input** command for an ATM interface does not show anything and states that the policy is not configured. However, the output of the **show running-config** command does show the service policy for the ATM interface.

  Conditions: This symptom is observed on a Cisco router after an RP switchover has occurred twice.

  Workaround: There is no workaround.

- CSCsf11353

  Symptoms: A FlexWAN, FlexWAN2, or SIP-200 may crash when you attach or remove service policies to or from virtual interfaces such as MLP or virtual-template interfaces or when these virtual interfaces flap.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsf11937

  Symptoms: When you enter the **cd .../.../** command followed by a sequence of **mkdir** commands, the disk becomes corrupt.

  Note that for the **cd .../.../** command, ".../.../" are the arguments, that is, the arguments consist of more than two dots.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

  Workaround: Enter the **format** command for the file system.

- CSCsf13044

  Symptoms: The outgoing interface (OIF) for bidirectional PIM multicast routes is not updated properly because PIM joins are not received through the MDT tunnel.

  Conditions: This symptom is observed on a Cisco 7600 series that has Gigabit Ethernet interfaces that are configured for dCEF.

  Workaround: There is no workaround.

- CSCsf14994

  Symptoms: A ping may not go through an MLP interface that is configured on a channelized T1/E1 SPA, channelized T3 SPA, or channelized STM-1 SPA.

  Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

  1. You remove a multilink interface by entering the **no interface multilink** *multilink-bundle-number* command without first removing the member links from the bundle.
  2. You recreate the same multilink interface.
  3. You configure the multilink bundle by adding links from a different SPA that is installed in the same SIP.

  Workaround: First remove the **multilink-group** command from the member link configuration before you enter the **no interface multilink** *multilink-bundle-number* command.

- CSCsf15429

  Symptoms: When you perform an OIR of an OC-3 POS line card, continuous "FR Broadcast Output" error messages may be generated, first causing a CPUHOG condition, and then causing the router to crash.

  Conditions: This symptom is observed on a Cisco 7304. However, the symptom is platform-independent and is related to the Forwarding Information Base (FIB).

  Workaround: There is no workaround.

- CSCsf19418

  Symptoms: A router may reload unexpectedly when you enter the **show mpls ldp graceful-restart** command.

  Conditions: This symptom is observed when either of the following conditions are present:

  – When the command output has a "Down Neighbor Database" entry that expires by reaching the reconnect timeout limit while the command output is generating the neighbor address list.

  – When the command output is paged at the "--More--" string within the context of displaying addresses.

Workaround: Do not enter the **show mpls ldp graceful-restart** command when a graceful-restart database entry is about to expire. When the command output is paged at the "--More--" string within the context of displaying addresses and when the Down Neighbor Database entry may have expired, type the letter "Q" to abort any further output of addresses.

- CSCsf19575

  Symptoms: A Cisco 7600 series that has an IPsec SPA with mGRE tunnels that function in VRF mode may crash.

  Conditions: This symptom is observed when you enter the **crypto engine slot** *slot/subslot* **inside** command on the mGRE interface.

  Workaround: There is no workaround.

- CSCsf20194

  Symptoms: When you perform an OIR of a SIP-200, the SIP-200 may crash.

  Conditions: This symptom is observed when the same policy map is attached to both the ingress and egress side of an interface on the SIP-200.

  Workaround: There is no workaround.

- CSCsf25712

  Symptoms: A line card such as a SIP-200 may crash when the line card on the other side or SPAs in the line card on the other side are reloaded.

  Conditions: This symptom is observed on a router that has a highly scaled configuration (for example, a configuration that is used for mobile users) with priority traffic and non-priority traffic running at line rate.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs because of memory corruption.

- CSCsf27085

  Symptoms: A SIP-200 may crash when a class with a priority is removed from a service policy while traffic is being processed.

  Conditions: This symptom is observed when the class that is being removed is the last class at a layer in the service policy.

  Workaround: There is no workaround.

- CSCsf27677

  Symptoms: When you perform an In-Service Upgrade (ISU) upgrade (that is, a hardware upgrade) from a PRE-2 to a PRE-3, the Cisco 10000 series may crash and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x40378AAC-
  ```

  Conditions: This symptom is observed on a Cisco 10000 series but may occur on any platform when you perform an ISU. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl? bugid=CSCse89636. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCsf30618

  Symptoms: A DHCP route is unexpectedly removed for an unnumbered DHCP binding.

  Conditions: This symptom is observed when a DHCP address is renewed.

Workaround: There is no workaround. However, during the next DHCP address renewal, the DHCP route is added back.

- CSCsf96069

  Symptoms: IPv6 traffic that is processed on MFR interfaces may not be switched via dCEF.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsf96476

  Symptoms: Bidirectional Forwarding Detection may not function properly.

  Conditions: This symptom is observed on a Cisco platform that is not MIPS-based such as a Cisco 7600 series and Cisco 12000 series.

  Workaround: There is no workaround.

- CSCsf98345

  Symptoms: An MPLS LDP peer on a default VRF resets when a VRF interface goes down.

  Conditions: This symptom is observed on a Cisco router when the VRF interface is configured with a subnetwork address that overlaps with the default router ID.

  Workaround: Reconfigure the VRF interface address so it does not overlap with the default router ID.

- CSCsf98858

  Symptoms: Failure detection time with Bidirectional Forwarding Detection (BFD) echo mode takes longer than with BFD asynchronous mode.

  Conditions: This symptom is observed on a Cisco router that has 100 BFD neighbors.

  Workaround: Use the BFD asynchronous mode by entering the **no bfd echo** command on the interface that has BFD enabled.

- CSCsg02241

  Symptoms: Incorrect NAT translation may occur for one or more faulty Multi-Layer Switching (MLS) flows. You can recognize a faulty MLS flow in the output of the **show mls netflow ip** command: if any two MLS flows show the same adjacency, one of the MLS flows is faulty.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsg02387

  Symptoms: A time-out occurs when you enter an SNMP command for an IPv6 interface. However, you can ping the IPv6 interface.

  Conditions: This symptom is observed on a Cisco 7200 series but is platform-independent.

  Workaround: There is no workaround.

- CSCsg02554

  Symptoms: On a Cisco Catalyst 6500 series or Cisco 7600 series router that has two Optical Services Modules (OSMs) that are configured for APS, a switchover to the protect channel may result in a 30-second traffic loss.

  Conditions: This symptom is observed when the L2 protocol is configured for Frame Relay.

  Workaround: Disable keepalive on the Frame Relay link, or lower the keepalive interval.

- CSCsg02605

  Symptoms: After a packet buffer parity error has occurred on one port of a group of 12 ports, an Ethernet module does not go through the rapid reboot process but rather reboots regularly, which takes about 40 seconds.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and affects the following modules when these are configured for to reset as a corrective action after an error has occurred:

  – WS-X6348-RJ-45
  – WS-X6348-RJ-21V
  – WS-X6248-RJ-45
  – WS-X6248-TEL
  – WS-X6148-RJ-45
  – WS-X6148-RJ-21

  Workaround: There is no workaround.

- CSCsg04681

  Symptoms: Traffic from an MPLS cloud to a tunnel interface within a VRF may stop when the tunnel interface is moved from the supervisor engine to a SPA.

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

  Workaround: First shut down the tunnel interface, then move the tunnel interface to the SPA, and then bring up the tunnel interface.

- CSCsg08200

  Symptoms: The bootup diagnostics for a line card may detect a major failure after an RPR switchover has occurred, and these line cards reset repeatedly and eventually power-down.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs only with a Supervisor Engine 720 that is configured with a PFC3BXL (WS-SUP720-3BXL) or with a DFC3BXL-equipped module.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur after an SSO or RPR+ switchover has occurred.

- CSCsg13828

  Symptoms: A router that is configured for Embedded Event Manager (EEM) may reload unexpectedly.

  Conditions: This symptom is observed when an EMM policy is configured with an event timer or with an action to log output to the console.

  Workaround: There is no workaround.

- CSCsg16425

  Symptoms: The output of the **show ip slb reals** command displays very large connection values (conns) for some real servers.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for Cisco IOS Server Load Balancing (IOS SLB) with inter-firewall routing enabled via the **ip slb route inter-firewall** command. The symptom occurs only when the inter-firewall connections switch from one firewall real to other firewall real in the firewall farm.

Workaround: Remove and reconfigure the real server that is part of the server farm or firewall farm.

Further Problem Description: When the connection value for a real server becomes very large, the server may enter the “MAXCONNS” state. When this situation occurs, you can no longer clear the connections counter by entering the **clear ip slb counters** or **clear ip slb connections** command.

- CSCsg17500

  Symptoms: OSPFv3 neighbors or adjacencies are not formed across MLP and MFR links.

  Conditions: This symptom is observed on a Cisco 7600 series for MLP and MFR configurations on a FlexWAN module that is configured for OSPFv3.

  Workaround: There is no workaround.

- CSCsg17790

  Symptoms: MPLS traffic may be dropped for a few seconds during an RP switchover.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS LDP and occurs because of a timing issue.

  Workaround: There is no workaround.

- CSCsg17957

  Symptoms: A router may crash when forwarding an IP fragment.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(28)SB3 and that is configured for L2TP and QoS. Note that the symptom is not release-specific.

  Workaround: Remove the QoS configuration. If this is not an option, there is no workaround.

- CSCsg18933

  Symptoms: A RIP route is learned from a RIP neighbor via a dialer interface (or other virtual interface type). When the neighbor disconnects and the interface goes down, the RIP route is removed from the RIP database. However, the RIP route remains in the routing table.

  Conditions:

  – RIP is configured with the **no validate-update-source** command.
  – RIP routes are learned via a virtual interface.
  – The virtual interface is using a negotiated address.
  – The problem is platform-independent.

  Workaround: Use the **clear ip route** command to remove the affected routes from the routing table.

- CSCsg19208

  Symptoms: When you reload a PE router, the standby RP crashes.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router in an MPLS configuration with TE tunnels and per-VRF-aggregate labels.

  Workaround: There is no workaround.

- CSCsg21429

  Symptoms: The interface of an OSM-1OC48-POS-SI+ module may flap after you have entered the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with redundant Supervisor Engine 720-3BXL modules that function in RPR+ mode.

  Workaround: Repeat the **redundancy force-switchover** command several times.

- CSCsg22369

  Symptoms: In an MPLS TE Fast ReRoute (FRR) environment, when a protected link flaps, all primary LSPs that traverse the link and that are protected by a backup tunnel are reoptimized, that is the old active LSPs are replaced with new LSP.

  For primary TE tunnels without any bandwidth such as primary auto-tunnels, the new LSP is protected by a suitable NHOP or NNHOP backup tunnel, but when this backup tunnel goes for some reason, the new primary LSP is not re-evaluated and moved off the backup tunnel. However, the FRR state continues to shows as “Ready”.

  Conditions: This symptom is observed on a Cisco router that functions as an MPLS TE FRR Point of Local Repair (PLR) when the following conditions are present:

  – One or more fast-reroutable primary TE tunnels with zero-bandwidth traverse the PLR.

  – A flap of the protected link occurs.

  – An event occurs that requires the LSP for the backup tunnel (that protects the primary TE LSP) to be torn down.

  Workaround: There is no workaround.

- CSCsg24278

  Symptoms: After a Supervisor Engine 32 has been powered-on or reloaded, it may enter a state in which it responds very slowly. For example, the response time to a ping from a directly-connected host is very high such as in the order of hundreds of milliseconds as opposed to under a few milliseconds in a normal state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA1.

  Workaround: There is no workaround.

- CSCsg24609

  Symptoms: A MIB walk on the CISCO-L2-CONTROL-MIB occurs very slowly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that do not have the **mac-address-table limit vlan** *vlan* command enabled.

  Workaround: Enter the **mac-address-table limit vlan** *vlan* command.

- CSCsg29498

  Symptoms: A router may reload when you enter the **show monitor event-trace adjacency all** command.

  Conditions: This symptom is observed when you enter the command after a route to a destination changes from multiple paths to a single path.

  Workaround: There is no workaround.

- CSCsg35439

  Symptoms: After a switch or router boots up, OSPF neighbors continue to flap. This situation occurs because, even though the switch or router correctly sends and receives OSPF hello packets at every interval, it incorrectly detects that the neighbors are down.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series that has a Supervisor Engine 32 and that runs Cisco IOS Release 12.2(18)SXF6 and on a Cisco 7600 series that has a Supervisor Engine 32 and that runs Release 12.2(18)SXF6 or Release 12.2(33)SRA1.

  Workaround: There is no workaround.

- CSCsg36982

  Symptoms: A static route is not removed when you enter the **clear ip dhcp binding** command.

  Conditions: This symptom is observed on a Cisco router when the DHCP binding and route are loaded from a database agent.

  Workaround: Do not use a database agent for the restoration of a binding and router.

- CSCsg38930

  Symptoms: IP fragments may not be forwarded over an GRE tunnel when the tunnel is configured to go through an IPSEC-SPA-2G. These IP fragments may be dropped.

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and an IPSEC-SPA-2G, and that runs Cisco IOS Release 12.2(18)SXF5 when the tunnel is configured in the following manner:

  – Path MTU Discovery (PMTUD) is enabled.

  – IPsec tunnel protection is enabled.

  – The **crypto engine slot** *slot/subslot* **inside** command is enabled.

  The symptom may also affect other releases.

  The output of the **show crypto vlan** command shows the VLAN that is associated with the crypto configuration.

  Temporary Workaround: Use an ACL with an ACE and the **log** keyword for the specific multicast group.

  Workaround: Disable Path MTU Discovery (PMTUD).

- CSCsg40391

  Symptoms: When a dot1x port is authenticated and assigned a VLAN by an AAA server and then the line card for the port is reset, the assigned VLAN becomes the configured access VLAN for the port. You can see this situation in the running configuration for the port.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reconfigure the access VLAN for the port to the old value.

  Further Problem Description: If, at a later time, you unconfigure dot1x on the port but do not unconfigure the access VLAN, the configuration for the assigned VLAN remains in place, causing the port to have access to whatever VLAN was previously assigned.

- CSCsg40425

  Symptoms: An Optical Services Module (OSM) may reset unexpectedly and generate the following error messages:

  ```
  %POSLC-3-SOP: TxSOP-0 SOP. (source=0x18, halt_minor0=0x4000)
  ```

  ```
  %CWANLC-3-FATAL: Fatal Management interrupt, gen_mgmt_intr_status 0x0,
  line_mgmt_intr_status 0x1, reloading
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsg41552

  Symptoms: A module does not come online after excessive fabric errors followed by a power-cycle of the module.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router. The symptom occurs because the Serial Control Protocol (SCP) fails to download. The following modules are affected:

- WS-X6704-10GE
- WS-X6748-GE-TX
- WS-X6724-SFP
- WS-X6748-SFP
- WS-X6708A-10GE

Workaround: Manually reset the power of the module by entering the **hw-module slot** *slot-number* **reset** command.

- CSCsg42246

  Symptoms: High CPU use may occur in the "IP Background" process, and the router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that is configured for RIP and that receives a RIP host route that is subsequently replaced by a route that is dynamically assigned to an interface. For example, this situation may occur on a PPP interface that has the **ip address negotiated** command enabled.

  Workaround: Use a route map to block the advertised route.

- CSCsg44555

  Symptoms: An MPLS TE tunnel with a third-party vendor headend, a Cisco midpoint, and a Cisco tailend may occasionally transition to the up/down state on the midpoint while still appearing in the up/up state on the headend and tailend. When this situation occurs, traffic may continue to flow on the tunnel even though the tunnel is in the up/down state at the midpoint or it may come to a halt.

  Conditions: This symptom is observed when the Cisco router that is the tailend for the MPLS TE tunnel uses a bandwidth or burst size that is not a multiple of 1 Kbps or 1 Kbyte and that rounds up the Resv burst size to the next higher multiple of 1 Kbps or 1 Kbyte.

  Workaround: Specify a tunnel bandwidth that is a multiple of 8 Kbps.

- CSCsg46087

  Symptoms: A packet with a size that is larger than 1460 bytes does not go through a GRE IPsec tunnel even when the IP MTU for the tunnel has a size that is larger than the size of the packet (for example, when the IP MTU is set to 1514 bytes).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series that are configured with an IPSEC-SPA-2G SPA when the following conditions are present:

  - Path MTU Discovery (PMTUD) is enabled.
  - The DF bit is set for the tunnel interface.

  Workaround: Disable PMTUD.

  First Alternate Workaround: Do not set the DF bit for the tunnel interface.

  Second Alternate Workaround: Use a small IP MTU for the tunnel.

  Further Problem Description: Enabling fragmentation on a large number of tunnels may cause some packet loss due to fragmentation timeouts.

- CSCsg47462

  Symptoms: A router that is configured with at least one multipoint GRE tunnel may crash with an address error.

Conditions: This symptom is observed when a T3 interface bounces while the CPU usage of the router is at 100 percent.

Workaround: There is no workaround.

- CSCsg51811

  Symptoms: When the OER BGP Inbound Optimization feature is configured and when route control is enforced, route control does not prepend autonomous systems or communities. Rather, router control prepends the same autonomous systems or communities to all external OER interfaces.

  Conditions: This symptom is observed on a Cisco router when OER manages inside prefixes that are either learned or configured.

  Workaround: There is no workaround.

- CSCsg60791

  Symptoms: The **show oer master appl** command may terminate prematurely, and the following error message is generated:

  Show buffer max size reached

  Conditions: This symptom is observed when there are more than 50 application traffic classes. The command displays only approximately the first 50 application traffic classes.

  Workaround: Based on the type of application traffic class that is configured, use one of the following commands to show the application traffic classes:

  – The output of the **show oer master appl access-list** *name* command shows all applications that are defined in the access list.

  – The output of the **show oer master appl tcp** command shows all applications that use TCP.

  – The output of the **show oer master appl udp** command shows all applications that use UDP.

  – The output of the **show oer master appl** *protocol-number* command shows all applications that use the protocol number that is defined in the *protocol-number* argument.

- CSCsg67551

  Symptoms: LDP sessions flap after a switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router and that is configured for EIGRP and BGP. Note that the symptom is platform-independent.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reload the router.

- CSCsg68740

  Symptoms: Fast Reroute (FRR) is not triggered when a cable is removed from a POS SPA or POS OSM, causing data loss of 3 to 4 seconds.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

  Further Problem Description: This symptom does not occur when a POS port adapter is installed in an Enhanced FlexWAN module.

- CSCsg68783

  Symptoms: The ATM SAR may hang on an ATM interface that is configured for AToM.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when you enter the **clear mpls traffic-eng auto-tunnel mesh** command.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ATM interface.

Further Problem Description: The symptom occurs because the ATM SAR receives a packet that is larger than the ATM cell size in the AToM mode of operation.

- CSCsg72398

  Symptoms: Traffic to a Cisco IOS SLB virtual server that is configured for UDP may be process-switched.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with multiple virtual servers.

  Workaround: Enter the **mls ip slb search wildcard rp** command.

- CSCsg73179

  Symptoms: After a change in the routing topology, a Bidirectional PIM Rendezvous Point is not updated correctly in the hardware tables, causing Bidirectional PIM multicast flows to be software-switched.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs only when the ACL that is used to statically configure the Rendezvous Point does not have any wildcard entries.

  Workaround: Reinstall the Rendezvous Point.

- CSCsg79810

  Symptoms: The MPLS MTU is overruled by the IP MTU on an ATM interface.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an MPLS core when the ATM interface has the **tag-switching mtu 1508** command and the **ip mtu 1500** command enabled. In this situation, packets that are larger than 1496 bytes are dropped.

  Workaround: There is no workaround.

- CSCsg85046

  Symptoms: A Cisco 7600 series with a SIP-600 crashes during the boot process.

  Conditions: This symptom is observed only when a 4-port OC-48c/STM-16 POS/DPT/RPR SPA (SPA-4XOC48POS/RPR) is installed in the SIP-600.

  Workaround: There is no workaround.

- CSCsg98612

  Symptoms: The **speed nonegotiate** command does not function for Gigabit Ethernet ports on a SIP-600.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2 or Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsg99996

  Symptoms: When an ERP timer event occurs for a particular endpoint, the endpoint may become stuck in a continuous loop.

  Conditions: This symptom is observed on a Cisco router that is configured for High Availability (HA) In-Service Software Upgrade (ISSU).

  Workaround: There is no workaround.

- CSCsh07037

  Symptoms: A “%SYS-2- CHUNKBADMAGIC” error mat occur on an OSM module and the module may restart.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when Weighted Random Early Detection (WRED) is configured with a maximum threshold of more than 2000 packets but without a queue limit.

  Workaround: Configure a proper queue limit for the class with the WRED configuration. For example, when the **random-detect precedence 3 32000 32000 1** command is configured, configure the queue limit by entering the **queue-limit 32768** command.

- CSCsh12760

  Symptoms: Invalid SPI messages are generated on a remote peer.

  Conditions: This symptom is observed when IPsec rekeying occurs on a Cisco 7600 series that has an IPsec VPN SPA (SPA-IPSEC-2G) and that is connected to a remote peer. The symptom is more likely to occur when there are duplicate SAs and/or dynamic crypto maps.

  Workaround: There is no workaround.

- CSCsh13291

  Symptoms: When a fatal CEF error occurs on a line card other than the RP, CEF becomes disabled on the RP and therefore on the router.

  Conditions: This symptom is observed on a Cisco router after at least one switchover has occurred since the router booted.

  Workaround: There is no workaround.

  Further Problem Description: Another issue can trigger the symptoms: When two 7600-SSC-400 line cards are present in a Cisco 7600 series, CEF on the active RP disables itself about 100 minutes after the router has booted if one or more switchovers have occurred during these 100 minutes.

- CSCsh13947

  Symptoms: A router that is processing certain MPLS forwarding updates may crash or hang because of a software configuration mismatch.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB but may also occur in other releases. The symptom occurs when EoMPLS or AToM is configured with many virtual circuits (VCs) and when LDP sessions go down because of extreme traffic loads or clearing of the LDP neighbors, causing the forwarding information to be modified.

  Workaround: There is no workaround.

- CSCsh22835

  Symptoms: After an RPR switchover occurs, a major error occurs on the newly active RP.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Reload the platform. If this not an option, there is no workaround.

- CSCsh26382

  Symptoms: IPsec SAs may be unexpectedly deleted.

  Conditions: This symptom is observed on a Cisco router when the transform set that is used to create IPsec tunnels is a combination of both AH and ESP protocols.

  Workaround: Do not use a combination of AH and ESP protocols for the transform set. Use either the AH protocol or use the ESP protocol.

- CSCsh42857

  Symptoms: After a TE tunnel has been reoptimized, AToM traffic may no longer pass through because the outgoing label and outgoing interface are not updated in the hardware.

  Conditions: This symptom is observed on a Cisco 7600 series that has AToM circuits configured over a TE tunnel that connects to a CE router.

  Temporary Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the interface that faces the CE router or configure and deconfigure the **xconnect** command on the interface that faces the CE router. Doing so re-establishes traffic forwarding until a new reoptimization occurs.

- CSCsh61393

  Symptoms: When the standby supervisor engine becomes active after an RPR+ switchover has occurred, the transmission of all traffic stops.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an EoMPLS environment. The symptom occurs because a VRF-VLAN with an explicit null label is not properly programmed on the SP and DFC after the standby supervisor engine has become active. This situation can be seen in the output of the following commands:

  On the RP:

  Enter the **show mls cef mpls detail labels** *value* command. For the *value* argument, enter the VRF-VLAN with the explicit null label.

  On the SP:

  – Enter the **show mls cef mpls detail labels** *value* command. For the *value* argument, enter the VRF-VLAN with the explicit null label.

  – Then, enter the **show mls cef adjacency entry** *index* command. For the *index* argument, enter the adjacency index shown in the output of the **show mls cef mpls detail labels** *value* command.

  Workaround: There is no workaround.

- CSCsh66675

  Symptoms: When Circuit Emulation circuits are configured in a very short period via a script and then an RPR+ switchover occurs, the interface of a Circuit Emulation over Packet (CEoP) SPA may shut down.

  Conditions: This symptom is observed rarely on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: After the RPR+ switchover has occurred, enter the **no shutdown** interface configuration command on the interface of the CEoP SPA.

- CSCsh66793

  Symptoms: After you have performed an OIR of a line card, the number of queues that correspond to QoS policies are smaller than before the OIR because not all queues are recreated.

  Conditions: This symptom is observed on a Cisco 7600 series that has a large number of Ethernet Virtual Circuit (EVC) instances on which QoS policies are configured and that are spread across several interfaces.

  Workaround: Perform another OIR of the line card.

- CSCuk60910

  Symptoms: A Cisco IOS router may detect a memory corruption and reload.

Conditions: An interface on the system must be configured for Van Jacobsen TCP header compression, using the **ip tcp header-compression** command, and connected to a third party system.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCee73956

  Symptoms: The Generalized TTL Security Mechanism (GTSM), formerly known as BGP TTL Security Hack (BTSH), checks the time-to-live (TTL) value of the packets at the application level, which is not efficient. Also, GTSM does not stop the establishment of a TCP connection for a packet with an invalid TTL value.

  Conditions: This symptom is observed on a Cisco platform that has the **neighbor** *neighbor-address* **security ttl hops** *hop-count* command configured in a BGP environment.

  Workaround: There is no workaround.

- CSCek12203

  Symptoms: When you enter the **copy ftp disk** command, the copy operation may fail and cannot be terminated, further **copy** commands may fail, and a TCP vty session for the purpose of troubleshooting the situation may fail and cannot be terminated.

  Conditions: These symptoms are observed on a Cisco platform when the FIN flag is set in the initial ESTAB message from a neighbor. You must reload the router to recover from the symptoms.

  Workaround: Do not enter the **copy ftp disk** command. Rather, enter the **copy tftp disk** command.

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

  Conditions: This symptom is seen under the following conditions:

  – The router must have RCP enabled.

  – The packet must come from the source address of the designated system configured to send RCP packets to the router.

  – The packet must have a specific data content.

  Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

- CSCsf33034

  Symptoms: The following error message and tracebacks are generated during the boot process:

  ```
  %TCP-2-INVALIDTCB: Invalid TCB pointer: 0x4704D088
   -Process= "IP Input", ipl= 0, pid= 122
   -Traceback= 409F00FC 409E4C50 407A032C 407D8EAC 4077FF38 407911D0 4078EC2C 4078EDE8
  4078F004
  ```

  Conditions: This symptom is observed on a Cisco platform when a TCP server is configured.

  Workaround: There is no workaround.

  Further Problem Description: A TCP control block that is already freed is referenced or accessed, causing the error message to be generated. This situation does not affect the proper functioning of the platform in any way.

Wide-Area Networking

- CSCeh64479

  Symptoms: A router reloads unexpectedly when an apparent Layer Two Forwarding (L2F) packet is received.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Virtual Private Dialup Network (VPDN). However, the symptom is not platform-specific.

  Workaround: There is no workaround.

- CSCek26657

  Symptoms: The following state mismatch error messages may be generated on the console of a standby RP:

  ```
  %IPV6-STDBY-4-IDB: Interface XXX state mismatch. IPv6 state is down, interface is up
  ```

  (Note that XXX represents the interface.)

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant RPs that function in SSO mode, and that is configured for IPv6, PPP, and IP header compression.

  Workaround: There is no workaround.

- CSCek31227

  Symptoms: A router may crash when a PPP access circuit flaps repeatedly.

  Conditions: This symptom is observed on a Cisco router that functions in a Virtual Private Dialup Network (VPDN).

  Workaround: There is no workaround.

- CSCek45604

  Symptoms: An OSM or FlexWAN module may crash when you apply an input QoS configuration to a Frame Relay interface in a particular sequence.

  Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

  1. You attach a policy to the main interface and you use the map class for inheritance.
  2. You remove the Frame Relay class from the interface and attach a flat policy to the main interface.

  Note that the symptom does not occur when you apply an output QoS configuration to a Frame Relay interface.

  Workaround: Do not apply an input QoS configuration to a Frame Relay interface.

- CSCir00712

  Symptoms: When a LAC receives fragmented data traffic over an L2TP tunnel, the IP layer reassembles the packets and routes them over the wrong interface instead of processing them locally.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T when fragmented L2TP data traffic is received on the LAC from the LNS over the L2TP tunnel. The symptom is release-independent.

  Workaround: There is no workaround.

- CSCsd21476

  Symptoms: A router crashes when you attempt to delete a Frame Relay-to-Ethernet connection.

Conditions: This symptom is observed when you first remove the Frame Relay interface via an OIR and then you attempt to delete the Frame Relay-to-Ethernet connection.

Workaround: Re-insert the Frame Relay interface before attempt to delete the Frame Relay-to-Ethernet connection.

- CSCsf03371

  Symptoms: A router may crash after more than 260,000 PPPoX sessions have flapped.

  Conditions: This symptom is observed on a Cisco router when the **aaa new-model** command is disabled.

  Workaround: Enter the **aaa new-model** command.

- CSCsf28443

  Symptoms: L2TP tunnels may not come up. When this situation occurs, a traceback is generated.

  Conditions: This symptom is observed on a Cisco router that has the **l2tp tunnel timeout no-session never** VPDN group configuration command enabled.

  Workaround: Do not configure the **never** keyword in the command. Rather, enter a value for the *seconds* argument.

- CSCsf28839

  Symptoms: When you change the encapsulation from Frame Relay to another type, a spurious memory access and tracebacks are generated.

  Conditions: This symptom is observed on a Cisco router that has the **encapsulation frame-relay** command enabled on a serial interface when you assign the serial interface to an MFR interface, which causes the Frame Relay encapsulation to be removed from the serial interface.

  Workaround: There is no workaround.

- CSCsg11708

  Symptoms: After An SSO switchover has occurred, punt adjacencies are installed for PPP, causing packets to be process-switched on the RP.

  Conditions: This symptom is observed on a Cisco 7600 series but may not be platform-specific.

  Workaround: Force the interface to reset by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCsg24778

  Symptoms: A router may crash because of a corrupted memory pointer.

  Conditions: This symptom is observed on a Cisco router that is configured for PPPoE Relay and VPDN.

  Workaround: There is no workaround.

- CSCsg35429

  Symptoms: Spurious access messages may be generated when you enter the **mpls bgp forwarding** command on a multilink interface.

  Conditions: This symptom is observed on a Cisco router that is configured for PPP.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA6

Cisco IOS Release 12.2(33)SRA6 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA6 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCek65222

  Symptoms: A non-parseable Ethernet configuration is nvgened for a VLAN.

  Conditions: This symptom is observed when you enter the **encap dot1q 1 native** command, and the command is rejected. When you enter the **encap dot1q 1** command, the command is accepted. However, in this situation, the output of the **show running-config** command shows that the **encap dot1q 1 native** command is present, which would have been rejected.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCse99493

  Symptoms: A router that is configured for NAT Overload may crash while performing dynamic translation from many ports to one port.

  Conditions: This symptom is observed after more than 5000 translations have been performed.

  Workaround: There is no workaround.

- CSCsg55591

  Symptoms: When there are link flaps in the network, various PE routers receive the following error message:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (1) received in update for prefix
  155:14344:10.150.3.22/32 from 10.2.2.1
  ```

  Or, a local label is not programmed into the forwarding table for a sourced BGP VPNv4 network.

  Conditions: These symptoms are observed when an iBGP path for a VPNv4 BGP network is present, and then a sourced path for the same route distinguisher (RD) and prefix is brought up.

  Workaround: Remove the iBGP path. Note that when the sourced path comes up first, the symptoms do not occur.

  Alternate Workaround: Use different RDs with the different PE routers. When the RD and prefix do not match exactly between the iBGP path and the sourced path, the symptoms do not occur.

- CSCsg97662

  Symptoms: When you enter the **no ip nat service skinny tcp port 2000** command, NAT is not disabled on port 2000. This situation causes NAT to be applied to SCCP packets, and causes the CPU usage to be very high.

  Conditions: This symptom is observed when an application is running on the port 2000.

  Workaround: There is no workaround.

  Further Problem Description: SCCP and NAT for voice are not supported in Cisco IOS Release 12.2 or a release that is based on Release 12.2. The **no ip nat service skinny tcp port 2000** command is not supported in these releases.

ISO CLNS

- CSCsj72039

  Symptoms: The prefix of a serial interface that is configured for PPP or HDLC and that functions as a passive interface for IS-IS may not be installed in the local IS-IS database.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)SXF6 but is not release-specific.

  Workaround: Remove and reconfigure the **passive-interface** command.

  First Alternate Workaround: Enter the **clear isis *** command.

  Second Alternate Workaround: Enter any command that triggers the generation of the local IS-IS database.

Miscellaneous

- CSCdz55178

  Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

  Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                          00000000011111111111222222222333^
                          12345678901234567890123456789012|
                                                           |
                                                        PROBLEM
                                                      (Variable Overflowed).
```

  Workaround: Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- CSCeb35205

  Symptoms: A Cisco router may reload when a subdirectory is created on an Advanced Technology Attachment (ATA) Flash disk.

  Conditions: This symptom is observed when the ATA Flash disk space that is allocated to the subdirectory contains data from previously deleted files.

  When a subdirectory is created or extended, it is given space on the ATA Flash disk. If this space contains zeros, the symptom does not occur. However, if the space was previously used, the space does contain data bytes from the previous file, and these data bytes may confuse the file system. This situation may cause the router to reload.

  Workaround: Do not create subdirectories on the ATA Flash disk.

- CSCek66590

  Symptoms: A router may crash when you enter the **show hw-module subslot** *slot/subslot* command.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a SPA services carrier (7600-SSC-400).

  Workaround: There is no workaround.

- CSCek68108

  Symptoms: A “INTSCHED: suspend” error message may be generated on a router that is configured with a SPA-IPSEC-2G, and the router may crash.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch an Cisco 7600 series router after you have removed the crypto map in crypto-connect mode.

  Workaround: There is no workaround.

- CSCsa96972

  Symptoms: A Dbus header error interrupt may occur during a recovery procedure on a DFC3, and the following error message is generated:

  ```
  %EARL_L3_ASIC-DFC5-3-INTR_WARN: EARL L3 ASIC: Non-fatal interrupt Packet
  Parser block interrupt
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when a recovery procedure occurs because of a transient problem in hardware forwarding.

  Workaround: There is no workaround. However, the error message indicates a harmless (non-fatal) error and does not have any impact on the traffic and proper functioning of the platform.

- CSCsb21941

  Symptoms: A supervisor engine may reset unexpectedly, and the following error messages may be generated:

  ```
  %PFREDUN-SP-7-KPA_WARN: RF KPA messages have not been heard for XXX seconds
  %OIR-SP-3-PWRCYCLE: Card in module 1, is being power-cycled (RF request)
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when “super jumbo” frames (greater than 10,000 bytes) are being used.

  Workaround: There is no workaround. The symptom can be mitigated by ensuring that all NICs on the domain are configured with a frame size that is smaller than 10,000 bytes.

- CSCsb74409

  Symptoms: A router may keep the vty lines busy after finishing a Telnet/Secure Shell (SSH) session from a client. When all vty lines are busy, no more Telnet/SSH sessions to the router are possible.

  Conditions: This symptom is observed on a Cisco router that is configured to allow SSH sessions to other devices.

  Workaround: Clear the SSH sessions that were initiated from the router to other devices.

- CSCsd70321

  Symptoms: Traffic stops flowing when you reset a line card and immediately afterwards an SSO switchover occurs.

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

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the line card.

- CSCsd85278

  Symptoms: A diagnostics test for bus connectivity on a SIP-400 fails.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the **vlan internal allocation policy ascending** command is enabled.

  Workaround: Remove the **vlan internal allocation policy ascending** command.

- CSCsf11353

  Symptoms: A FlexWAN, FlexWAN2, or SIP-200 may crash when you attach or remove service policies to or from virtual interfaces such as MLP or virtual-template interfaces or when these virtual interfaces flap.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsg09423

  Symptoms: When IPsec SAs flap, traffic loss may occur during the IPsec and IKE rekey.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when there is a large number of IKE and IPsec SAs (that is, more than 2000 IKE SAs and 4000 IPsec SAs) and when RSA signature authentication is configured.

  Workaround: Reduce the number of IKE and IPsec SAs.

- CSCsg18080

  Symptoms: A router that functions as a responder in an SNMP configuration may crash.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a SPA-IPSEC-2G after SNMP counters are retrieved for inbound traffic.

  Workaround: Do not use SNMP to obtain counters.

- CSCsg55315

  Symptoms: Packets may be duplicated or triplicated on interface “gig1/1” of a Supervisor Engine 2, Supervisor Engine 32, or Supervisor Engine 720.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with WAN line cards such as an Enhanced FlexWAN, SIP-200, SIP-400, or SIP-600 when SPAN is enabled and when interface “gig1/1” is used to connect to another platform.

  Workaround: Do not use interface “gig1/1” to connect to another platform. Rather, use another interface.

- CSCsg64327

  Symptoms: Tunnels may go down when continuous multicast traffic is processed in VRF mode.

  Conditions: This symptom is observed on a Cisco 6500 series switch and Cisco 7600 series router when the following conditions are present:

  – The initiator is configured in VRF mode and the responder is configured in crypto connect mode.
  – OSPF is configured for base connectivity and EIGRP is configured on the GRE tunnel.
  – There are four tunnels configured between the hub and spoke.
  – Multicast traffic is sent through all tunnels via the **ip igmp static-group** command.

  Initially, all tunnels are up and the traffic goes through fine as long as the traffic is not continuously. However, when traffic is sent continuously, all tunnels except for one go down one after another.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reload both the hub and the spoke. Note that clearing the (multicast and unicast) routes by shutting down and bringing up the tunnel interfaces on both sides, and clearing and re-establishing the crypto sessions does not resolve the symptom.

- CSCsg92950

  Symptoms: A software-forced reload may occur on a Cisco 7301.

  Conditions: This symptom is observed on a Cisco 7301 that terminates several thousand broadband subscribers. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsh46565

  Symptoms: When the configuration of the shape average is changed, the rate is not applied, which can be shown in the output of the **show policy interface** command and detected by a traffic analyzer.

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and GE-WAN subinterfaces that are configured with an HQoS (LLQ) output policy when the shape average is changed on all GE-WAN subinterfaces at the same time.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, delete the output policy and then reconfigure it on the GE-WAN subinterfaces.

- CSCsh61002

  Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a port-based EoMPLS interface (when Xconnect is configured on the main interface), forwarding stops on another L3 interface.

  Conditions: This symptom is observed on a Cisco 7600 series only when there is a short interval (about 30 seconds) between the **shutdown** and **no shutdown** commands.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the router.

  Further Problem Description: When you enter the **shutdown** command quickly followed by the **no shutdown** command on the port-based EoMPLS interface, a new internal VLAN is used. However, because of a software issue, an EoMPLS flag is set on the old VLAN, causing the router to process all packets that are received on the old VLAN as L2 packets. When a new L3 interface comes up and uses the old VLAN, the datapath fails because the router attempts to process these packets as L2 packets instead of L3 packet.

- CSCsi42769

  Symptoms: Tunnels are not set up or data traffic does not go through on a router that uses a VPN SPA card (SPA-IPSEC-2G).

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that uses a SPA-IPSEC-2G with certificates.

  Workaround: There is no workaround.

- CSCsi56793

  Symptoms: The following error messages and tracebacks may be generated on the console of a WAN line card that is installed in a Distributed Forwarding Cards (DFC):

  ```
  DFC1: PXF clients started, forwarding code operationalUnexpected call:
  c6k_pwr_get_system_power_sufficiency()

  DFC1: -Traceback= 4057162C 40B4770C 40B454A0 401EF56C 401EF5FC 4011760C
  40117838 401F089C 401F0888Unexpected call: sp_power_mgmt_led()

  DFC1: -Traceback= 40571F08 40B4771C 40B454A0 401EF56C 401EF5FC 4011760C
  40117838 401F089C 401F0888Unexpected call: sp_module_led()
  ```

```
DFC1: -Traceback= 40571F30 40B47808 40B454A0 401EF56C 401EF5FC 4011760C
40117838 401F089C 401F0888Unexpected call: sp_system_led()

DFC1: -Traceback= 40571F84 40B4783C 40B454A0 401EF56C 401EF5FC 4011760C
40117838 401F089C 401F0888
```

Conditions: This symptom is observed on a Cisco 7600 series when the WAN line card boots.

Workaround: There is no workaround. However, the error messages and tracebacks are harmless and do not impact the functionality of the router.

- CSCsi59267

  Symptoms: After you have reloaded the router, the Control Plane Policing feature does not function.

  Conditions: This symptom is observed on a Cisco 7600 series that has a policy attached to the control plane.

  Workaround: Remove the policy from the control plane and then re-attach it.

  Further Problem Description: When the symptom occurs, the output of the **show mls qos ip** command does not show that the control plane is programmed. Actually, there is no entry for the control plane policy in the output.

- CSCsi72758

  Symptoms: Clear inbound multicast traffic can not get to VPNSPA for processing.

  Conditions: This symptom occurs under the following conditions:

  – in crypto connect mode only

  – no encryption and decryption

  – multicast traffic is going through a “ifvlan”

  Workaround: There is no workaround.

- CSCsj01961

  Symptoms: A router may not boot and may generate an :INSUFFICIENT MEMORY” error message.

  Conditions: This symptom is observed on a Cisco 7600 series that has an RSP720 when the ifIndex table is corrupt, preventing SNMP from initializing because SNMP attempts to use the ifIndex table from NVRAM.

  Workaround: There is no workaround.

- CSCsj27811

  Symptoms: A supervisor engine may crash because of a low memory condition that is caused by an Ethernet Out of Band Channel (EOBC) buffer leak and a big buffer leak.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that runs Cisco IOS Release 12.2(18)SXF9 but could also affect a Cisco 7600 series router that runs Release 12.2SR.

  Workaround: There is no workaround.

- CSCsj35776

  Symptoms: Some PVCs may remain inactive after an ATM SPA has been reloaded.

  Conditions: This symptom is observed on a Cisco 7600 series when the ATM SPA is configured with OAM-managed PVCs and when these are many PVCs.

Workaround: Increase the *down-count* and *retry-frequency* OAM management arguments for the affected PVCs by using the **oam retry** command.

Alternate workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface with the affected PVCs.

- CSCsj36327

  Symptoms: A SPA-4XOC48POSRPR may not come up after a reload.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA3.

  Workaround: Enter the **hw-module module** *slot* **reset** command for the slot in which the affected SPA is installed.

- CSCsj36477

  Symptoms: When you enter the **shutdown** command on an interface of an OC-192 SPA, the FRR traffic loss may last about 120 ms.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-600 in which an OC-192 SPA is installed.

  Workaround: There is no workaround.

  Further Problem Description: When you physically remove the cable on the Cisco 7600 series, the FRR traffic loss may last only about 2-3 ms. Similarly, when you shut down the remote interface end, which is also a OC-192 SPA interface that is installed in a SIP-600 on a Cisco 12000 series, the FRR traffic loss may last only about 2-3 ms.

- CSCsj37071

  Symptoms: All E1 interfaces on a PA-MC-E3 port adapter may flap continuously even after the traffic has been stopped.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that have a PA-MC-E3 port adapter when you configure 16 or 128 channel groups on each time slot (that is, time slots 1-31) and then generate traffic just above line rate traffic through all the channel groups. Note that the symptom is not platform-specific.

  Workaround: Stop the traffic and reset the E3 controller of the PA-MC-E3 port adapter.

- CSCsj43677

  Symptoms: When you remove the standby supervisor engine, the active supervisor engine may crash and reload.

  Conditions: This symptom is observed on a Cisco 7600 series that has dual Supervisor Engine 720 modules that are configured for SSO.

  Workaround: There is no workaround.

- CSCsj47546

  Symptoms: When an interface of a POS SPA detects a Payload Label Mismatch-Path (PLM-P), it may generate a Remote Defect Indication-Path (RDI-P) to the far end. This is improper behavior.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SPA-2XOC3-POS, SPA-4XOC3-POS, SPA-1XOC12-POS, or SPA-1XOC48POS/RPR.

  Workaround: There is no workaround.

  Further Problem Description: Per the Bellcore GR-253 standard, RDI-P must not be transmitted to the far end when the interface detects PLM-P.

- CSCsj55865

  Symptoms: When you shut down an interface that is protected by FRR, a client API error may occur, and the following error message and a traceback may be generated:

  ```
  %LSD_CLIENT-3-CLIENTAPI: Client API error
  ```

  Conditions: This symptom is observed when an MLPS traffic engineering (TE) backup path is configured on the interface and when MPLS TE tunnels are not globally configured and enabled.

  Workaround: Configure and enable MPLS TE tunnels globally.

- CSCsj69176

  Symptoms: When you enter the **standby use-bia** command on an interface and when the HSRP status changes from active to standby on the interface or when HSRP is disabled on an interface that was previously in the active state, the MAC address of the interface is removed from the L2 table. This situation may disrupt L3 connectivity through the interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA, 12.2(33)SRA1, 12.2(33)SRA2, 12.2(33)SRA3, 12.2(33)SRA4, 12.2(33)SRB, or 12.2(33)SRB1.

  Workaround: To prevent the symptom from occurring, do not enter the **standby use-bia** command. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface to restore the MAC address.

  Further Problem Description: Cisco IOS Release 12.2(33)SRA is developed for and intended to run on Cisco 7600 series routers. We do not encourage you to run this release on Cisco Catalyst 6500 series switches. However, if you do run Cisco IOS Release 12.2(33)SRA, 12.2(33)SRA1, 12.2(33)SRA2, 12.2(33)SRA3, or 12.2(33)SRA4 on a Cisco Catalyst 6500 series switch, the symptom may occur.

- CSCsj76268

  Symptoms: When an MFR interface is configured to autosense LMI, the interface may not recover when the T1 links go down or when the interface is wedged.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and a Cisco 7600 series router that are configured with an OSM-12CT3/T1 Optical Services Module.

  Workaround: Configure the LMI type on both the DTE and the DCE. Also, entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the MFR interface may correct the symptom.

  Further Problem Description: Following are the debugs:

  ```
  lmi autosense on by default
  interface MFR1
  frame-relay intf-type dce

  Debug frame lmi
  MFR1(up): DCE LMI timeout
  MFR1: Invalid LMI type 1
  MFR1(down): DCE LMI timeout
  MFR1: Invalid LMI type 1
  MFR1: Invalid LMI type 1
  MFR1(down): DCE LMI timeout
  MFR1: Invalid LMI type 1
  ```

```
MFR1(down): DCE LMI timeout
MFR1: Invalid LMI type 1
MFR1: Invalid LMI type 2
MFR1(down): DCE LMI timeout
```

- CSCsj91961

  Symptoms: When you first create the channels for an E3 interface in a particular order on the active supervisor engine and then the standby supervisor engine is reloaded, the ifNumber objects on the active and standby supervisor engines do not match. This situation prevents proper forwarding on the E3 interface after a switchover.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an Enhanced FlexWAN.

  Workaround: Reload the router after you have configured the channels for the E3 interface.

- CSCsk08765

  Symptoms: When you add the first link to a multilink or MFR bundle, a bus error crash may occur, and the following error message is generated:

  TLB (load or instruction fetch) exception, CPU signal 10

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA, Release 12.2(33)SRB1, or Release 12.2SXF when you first have attached a policy map to the multilink or MFR interface and then have added the first link to the bundle.

  Workaround: First, add the required number of links to the multilink or MFR interface. Then, attach the service policy to the multilink or MFR interface.

- CSCsk14208

  Symptoms: A WAN line card or module that is configured for WCCP Redirection via the **ip wccp web-cache redirect {out | in}** interface configuration command may not redirect packets to the Cache Engine after an OIR has occurred or after the line card or module has been reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when WCCP redirection is applied to the interfaces that are configured on the WAN line card or module.

  Workaround: Remove and re-apply the WCCP Redirection configuration to the affected WAN interfaces by entering the **no ip wccp web-cache redirect {out | in}** interface configuration command followed by the **ip wccp web-cache redirect {out | in}** interface configuration command.

  Alternate Workaround: Delete and configure WCCP Redirection globally on the router by entering the **no ip wccp web-cache** router configuration command followed by the **ip wccp web-cache** router configuration command.

- CSCsk16974

  Symptoms: The following error message may be generated on a Supervisor Engine 2 or a line card that functions in bus mode:

  ```
  %PM_SCP-SP-2-LCP_FW_ERR_INFORM: Module 1 is experiencing the following error:
  Bus Asic #0 out of sync error
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router and may occur with a Supervisor Engine 2 or one of the following line cards:

  – 6516-GBIC

  – 6516-GE-TX

  - 6501-10GEX4
  - 6502-10GE
  - 6548-GE-TX
  - 6548-RJ-45
  - 6548-RJ-21
  - 6524-100FX-MM

  Workaround: There is no workaround.

  Further Problem Description: A large amount of traffic may causes the bus ASIC to be flow-controlled. This situation improperly triggers a patch that causes the out-of-sync behavior.

- CSCsk17205

  Symptoms: MFR LMI packets are consistently send through the serial interface that is associated with the MFR interface, instead of the MFR itself. You can verify this situation by enabling debugs:

  ```
  debug frame-relay lmi
   debug packet ----> CPU sensitive
  ```

  Because of this situation, when the LMI type is changed to another type, out- of-sequence problems may occur at the remote end.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with an Optical Services Module (OSM).

  Workaround: There is no workaround.

- CSCsk49151

  Symptoms: A policy map with MPLS EXP ingress marking attached to a non-EoMPLS VLAN is removed when the router is reloaded.

  Conditions: This symptom is observed on a Cisco 7600 series after you have reloaded the router.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, re-attach the policy map to the VLAN interface.

- CSCsk79031

  Symptoms: IP Internetworking may not function on a Supervisor Engine 720. For example, traffic may not pass from an EoMPLS VC on a Gigabit Ethernet interface to a serialATM interface.

  Conditions: This symptom is observed on a Cisco 7600 series when a packet is recirculated, for example, because a service policy is attached to the core-facing interface. The symptom is not related to the specific core- facing line card, but the workaround is.

  Workaround: Avoid recirculation of packet in direction from CE towards the core. For example, when service causes recirculation, service policy has to be removed from core interfaces.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA5

Cisco IOS Release 12.2(33)SRA5 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA5 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsi77983

  Symptoms: When NetFlow attempts to access a FIB source that is not present in the FIB, the router may crash.

  Conditions: This symptom is observed on a Cisco router that is configured with VLAN interfaces and virtual templates when a FIB source that is related to a virtual interface is not present in the FIB because of severe interface flaps.

  Workaround: There is no workaround.

- CSCsj44081

  Cisco IOS software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message when it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

  ```
  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

  Recommended Action: Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORR UPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

IP Routing Protocols

- CSCei93982

  Symptoms: A router that is configured for NAT may crash.

  Conditions: This symptom is observed when an application uses two well-known ports: one for the source and the other for the destination. After the outgoing translation is created, on return, when the previous source port is used as the destination, NAT may use an incorrect algorithm.

  For example, when a PPTP session is initiated to well-known port 1723 from source port 21 (FTP), then the outgoing packet creates a FTP translation. (Look at the source information when going from in to out). When the packet is returned, look again at the source information to see what kind of

packet is returned. In this situation, with source port 1723, NAT assumes that the packet is a PPTP packet, and then attempts to perform PPTP NAT operations on a data structure that NAT has built for a FT P packet, causing the router to crash.

Workaround: There is no workaround.

- CSCej20707

  Symptoms: The CPU usage may be high, and an IGP (OSPF or IS-IS) adjacency may drop when PIM sparse mode (PIM-SM) stress traffic is being processed.

  Conditions: This symptom is observed on a Cisco router that connects to a receiver and that has 60,000 (s,G) join messages. The symptom occurs when you enter the **show ip mroute count** command or when there is an abrupt increase in multicast groups.

  Workaround: Do not enter the **show ip mroute count** command. Rather, enter the **show ip mroute count terse** command. Increase multicast groups gradually to avoid high CPU usage. In addition, the following actions may also help to alleviate the symptoms:

  – Enter the **ip pim register-rate-limit** command on the first hop.

  – Enter the **ip pim fast-register-stop** on the PIM-RP.

  – Disable RP rate-limiting commands on the PIM-RP and first hop.

- CSCsb96034

  Symptoms: Routes redistributed from other routing protocols to BGP will be deleted and re-added after an NSF switchover, potentially causing traffic to go down for a long period of time.

  Conditions: This symptom may occur when the route is redistributed from other routing protocols (such as OSPF, ISIS, EIGRP) to BGP.

  Workaround: There is no workaround.

- CSCsd63038

  Symptoms: An MDT address-family session in a BGP environment may not come up between two PE routers. This situation prevents the tunnel interface from being shown in the output of the **show ip pim vrf** *vrf-name* **neighbor** command on one of the PE routers.

  Conditions: This symptom is observed on PE routers that are configured for Multicast VPN and that have the following commands enabled:

  address-family ipv4 mdt

  neighbor *neighbor-ip-address* **activate neighbor**

  neighbor *neighbor-ip-address* **send-community extended**

  Workaround: Reconfigure the **address-family ipv4 mdt** command in the BGP environment.

- CSCse92050

  Symptoms: A router may reload unexpectedly when a routing event causes multicast boundary to be configured on a Reverse Path Forwarding (RPF) interface.

  Conditions: This symptom is observed on a Cisco platforms that is configured for PIM.

  Workaround: Remove multicast boundary from the configuration.

- CSCsg55209

  Symptoms: When BGP updates are received, stale paths are not removed from the BGP table, causing the number of paths for a prefix to increase. When the number of BGP paths reaches the upper limit of 255 paths, the router resets.

Conditions: This symptom is observed on a Cisco router when the **neighbor soft-reconfiguration inbound** command is enabled for each BGP peer.

Workaround: Remove the **neighbor soft-reconfiguration inbound** command. A router that runs a Cisco IOS software image that has a route refresh capability, storing BGP updates is usually not necessary.

- CSCsh53926

  Symptoms: A router may crash because of a bus error in the OSPF process.

  Conditions: This symptom is observed on a Cisco router that is configured for incremental SPF (ISPF) and that functions in a network with MPLS TE tunnels.

  Workaround: Remove the ISPF configuration.

- CSCsi49948

  Symptoms: The local BGP MDT prefix may be missing.

  Conditions: This symptom is observed on a Cisco router that has the **mdt default** *group-address* command enabled under a VRF configuration and occurs after you have entered the **clear ip bgp *** command.

  Workaround: Disable and re-enable the **mdt default** *group-address* command.

- CSCsj25841

  Symptoms: A BGP router may not send the default route to its neighbor.

  Conditions: This symptom is observed when the **neighbor default-originate** command is conditionally configured with a route map and when the matching route is installed into the RIB by BGP itself.

  Workaround: There is no workaround.

ISO CLNS

- CSCsg40507

  Symptoms: BFD may not come up when an IP address on an interface is changed and when IS-IS is configured as the routing protocol.

  Conditions: This symptom is observed only when you first enter the **router isis** command and then enter the **bfd all-interfaces** command.

  Workaround: Unconfigure BFD, change the IP address, and then reconfigure BFD.

- CSCsi57971

  Symptoms: IS-IS may not advertise the prefix of a passive interface to the IS-IS database in a local router.

  Conditions: This symptom is observed on a Cisco router when you shut down an interface (for example, G9/1/1) of a 5-port GE SPA (SPA-5X1GE) that is installed in a SIP-600, replace the SPA-5X1GE with another card, and then enter the **no shutdown** interface configuration command on the interface at the same location (G9/1/1) on the new card. In this situation, the prefix for the interface (G9/1/1) is not advertised.

  Possible Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

Miscellaneous

- CSCek55987

  Symptoms: New Xconnect VCs do not function, causing packets that are sent from an OSM to be dropped. Note that packets that arrive on the OSM are not affected.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA4 when a VLAN-based EoMPLS is used with an uplink that is configured on a subinterface of an OSM and occurs only when you attach a service policy to the main interface of the OSM before you configure Xconnect.

  Workaround: Configure Xconnect before you attach the service policy to the main interface of the OSM. Note that the symptom does not occur in Release 12.2(33)SRA3 and Release 12.2SXF.

- CSCek65087

  Symptoms: A traceback may be generated on the supervisor engine when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a tunnel interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCek66164

  Symptoms: A router may hang briefly and then may crash when you enter any command of the following form:

  show ... | redirect rcp:....

  Conditions: This symptom is observed when Remote Copy Protocol (RCP) is used as the transfer protocol.

  Workaround: Use a transfer protocol other than RCP such as TFTP or FTP.

  Further Problem Description: RCP requires delivery of the total file size to the remote host before it delivers the file itself. The output of a **show** command is not an actual file on the file system nor is it completely accumulated before the transmission occurs, so the total file size is simply not available in a manner that is compatible with RCP requirements.

- CSCsb57042

  Symptoms: While running a health monitoring diagnostics test, the supervisor engine may crash because of an illegal memory access and generate a “%SYS-SP-3-OVERRUN” error message.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that run Cisco IOS Release 12.2(18)SXF4 and on a Cisco 7600 series router that runs Cisco IOS Release 12.2(33)SRA3. The symptom may also affect other releases. The symptom occurs when the firmware of the module that is being tested reports more errors than an SCP message can carry, causing the health monitoring test to access unauthorized memory outside the SCP message.

  Workaround Enter the **no diagnostic monitor module** *module-num* **test** *test-id* command for the affected module.

- CSCsb79306

  Symptoms: Setting the cbeDot1dTpVlanAgingFromGlobal from “false” to “true” may cause the standby supervisor engine to reload unexpectedly.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have redundant Supervisor Engine 720 modules that function in SSO mode when the following sequence of events occurs:

1. USe the CLI to configure a VLAN, for example, VLAN 50:
2. SNMP creates an entry cbeDot1dTpVlanAgingFromGlobal.50 with the value set to “true”.
3. Manually set the value for cbeDot1dTpVlanAgingFromGlobal.50 from “true” to “false”.
4. USe the CLI to delete VLAN 50.
5. When you initiate a mibwalk for cbeDot1dTpVlanAgingFromGlobal, the entry for VLAN 50 is still present.
6. Manually set the value for cbeDot1dTpVlanAgingFromGlobal.50 from “false” to “true”.

This last event causes the standby supervisor engine to reload unexpectedly.

Workaround: Do not use or limit the use of cbeDot1dTpVlanAgingFromGlobal.

- CSCsc89932

  Symptoms: A switch or router may crash when you enter the **show diagnostic sanity** command.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsc95875

  Symptoms: After multiple SSO switchovers occur on a Cisco 7600 series, an OSM or FlexWAN module may be reset by the switch processor because of a keepalive or SCP failure.

  The same symptom may occur while toggling hardware switching by entering the **no mls switching** command followed by the **no mls switching** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR and that has a non-fabric-enabled LAN card in its chassis.

  Workaround: There is no workaround.

- CSCsd31503

  Symptoms: Some protocol packets such as OSPF, EIGRP, MPLS LDP, BGP, and IS-IS may be dropped at the Route Processor (RP) because SPD classifies them as lower-priority packets.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when there are a number of routing protocols running with a very large topology and when rapid topology changes or changes in link states occur, causing more traffic to be processed by the RP.

  Workaround: Increase the priority of the protocol packets by entering the configuration stated below, in which 0 indicates a lower priority and 7 indicates a higher priority and in which the following levels are used for packet classification:

  – 0-1, indicating that the packet is to be dropped
  – 2-4, indicating that as a last resort the packet is to be dropped
  – 5-7, indicating that the packet should be the last one to be dropped.

  Priority level 5-7 is best suitable for protocol packets.

```
Router(config)#mls qos protocol ospf precedence 6
 Marking will work on the packet which comes from untrusted port
```

```
Router(config)#mls qos protocol ?
  isis
  eigrp
  ldp
  ospf
  rip
  bgp
  ospfv3
  bgpv2
  ripng
  neigh-discover
  wlccp
  arp

Router(config)#mls qos protocol eig
Router(config)#mls qos protocol eigrp ?
  pass-through  pass-through keyword
  police        police keyword
  precedence    change ip-precedence(used to map the dscp to cos value)
Router(config)#mls qos protocol eigrp pr Router(config)#mls qos protocol eigrp
precedence 6  Marking will work on the packet which comes from untrusted port
```

- CSCsf23115

  Symptoms: After the fan tray has failed, the system can not determine if the fan tray is an original fan (FAN1) or high-speed fan (FAN2).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that hare configured with a Supervisor Engine 720.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur on a Cisco Catalyst 6504-E or Cisco Catalyst 6509 NEB that are configured with an E-FAN.

- CSCsg00252

  Symptoms: A Cisco 7600 series may generate the following error message:

  ```
  MSC-RPDF ASSERTION FAILED 0
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for multicast traffic when the replication mode is changed.

  Workaround: There is no workaround.

- CSCsg41552

  Symptoms: A module does not come online after excessive fabric errors followed by a power-cycle of the module.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router. The symptom occurs because the Serial Control Protocol (SCP) fails to download. The following modules are affected:

  – WS-X6704-10GE

  – WS-X6748-GE-TX

  – WS-X6724-SFP

- WS-X6748-SFP
- WS-X6708A-10GE

Workaround: Manually reset the power of the module by entering the **hw-module slot** *slot-number* **reset** command.

- CSCsg47039

  Symptoms: After a Fast Reroute (FRR) event and multiple failure situations have occurred, any of the following line cards or port adapters may crash:

  - SIP-600
  - 2-port Ethernet Services line card (7600-ES20-10G)
  - 20-port Ethernet Services line card (7600-ES20-GE)

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for MPLS Traffic Engineering Fast Reroute--Link Protection when the line card or port adapter is processing incoming traffic from the MPLS core and when the following sequence of events occurs:

  - You remove the protected TE tunnel configuration from the protected interface.
  - You add back the protected TE tunnel configuration to the same interface.
  - You clear the fault that caused the FRR event.

  The crash occurs after OSPF and LDP are negotiated through the protected interface.

  Workaround: After the FRR event has occurred, do not remove the protected TE tunnel configuration from the protected interface.

- CSCsg70474

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsh25976

  Symptoms: There are two symptoms:

  1. 1) The threshold of the fan-fail sensor of the power supply may not be updated correctly, and the following error message may be generated:

     power-supply incompatible with fan: N/A

     The value should not be “N/A” but “OK”.

2. 2) The threshold of the fan-fail sensor of the power supply may get be added when power supply is detected. For example, information about the fan-fail sensor of the power supply may not be shown in the output of the **show environment alarm thresholds power-supply** command.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

Workaround: Initiate a Stateful Switchover (SSO). After the SSO, the symptom no longer occurs.

- CSCsh89826

  Symptoms: When a QoS service policy is applied to a serial interface, the rate that is provided to the default queue may drop to unexpectedly low values.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(31)SRA1 with a SPA-4XCT3/DS0 that in installed in a SIP-200. The following is an example of a configuration in which the symptom occurs:

```
class-map match-all MGCP
  match ip precedence 4
class-map match-all RTP
  match ip precedence 5

policy-map TEST1
  class RTP
    priority percent 88
  class MGCP
    bandwidth percent 10

     interface Serial2/0/0/17:0
      ip address 10.1.0.13 255.255.255.252
      encapsulation ppp
      load-interval 30
      service-policy output TEST1
```

  In this configuration, when there are eight G.711 calls and an FTP file is sent, the throughput is around 30 Kbps of application data for the FTP file. Considering the output service policy and the fact that the priority class does not consume the bandwidth, this throughput rate is very low. Moreover, after a few minutes of operation, the throughput rate drops to about 2 Kbps even though the rate that is provided in the priority queue has not changed. When the traffic is removed from the priority queue, the default queue continues to serve traffic at the reduced rate of only a few Kbps even though the full T1 line is now available.

  Workaround: Remove the service policy from the interface to enable the data traffic to resume flowing at a normal rate.

- CSCsi41791

  Symptoms: A buffer memory leak may cause a SPA-IPSEC-2G to crash. When this situation occurs, the following error messages are generated in the logs:

```
SPA_IPSEC-3-PWRCYCLE: SPA (<slot/subslot>) is being power-cycled (Module not
responding to keep-alive polling)
SPA_OIR-3-RECOVERY_RELOAD: subslot <slot/subslot>: Attempting recovery by reloading
SPA
ACE-6-INFO: SPA-IPSEC-2G[<slot/subslot>]: Crypto Engine X going DOWN
```

Conditions: This symptom is observed rarely on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when GRE fragments are reassembled by the SPA-IPSEC-2G and when the length of the IP packet after GRE decapsulation is more than 9126 bytes.

Workaround: To prevent the symptom from occurring, proactively reload the SPA-IPSEC-2G outside of business hours by entering the **hw-module subslot** *slot*/*subslot* **reload** command.

- CSCsi46469

  Symptoms: The CBQoSMIB may generate inaccurate results: a manual snmpwalk of the CBQoSMIB may fail with errors that indicate “OID not increasing.”

  Conditions: This symptom is observed on a Cisco 7609 that runs Cisco IOS Release 12.2(33)SRA2 and that is configured for QoS.

  Workaround: There is no workaround.

- CSCsi49520

  Symptoms: A medium buffer leak may occur on an MSFC.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that function as a PE router after an SSO has occurred.

  Workaround: There is no workaround.

- CSCsi52209

  Symptoms: A SIP-600 may crash, and the following error message may be generated:

  ```
  %PXF-DFC1-2-FAULT: T0 OHB Exception: SLIP FIFO full WARNING: PXF Exception:
  mac_xid=0x40000 ***
  PXF OHB SLIP FIFO Full %SIP600-DFC1-2-UNRECOVERABLE_FAILURE: SIP-600 Unrecoverable
  Failure
  ```

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

  Workaround: There is no workaround.

- CSCsi60004

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)

  – Media Gateway Control Protocol (MGCP)

  – Signaling protocols H.323, H.254

  – Real-time Transport Protocol (RTP)

  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsi69350

  Symptoms: The RP on the standby supervisor engine may crash during the boot process when you upgrade the ROMmon of the RP on the standby supervisor from the active supervisor engine.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have redundant Supervisor Engine 720 modules that function in RPR mode when you upgrade the ROMmon of the RP on the standby supervisor from the active supervisor engine by entering the **upgrade rom-monitor slot** *slot-num* **rp file** *filename* command.

Workaround: There is no workaround.

- CSCsi75566

  Symptoms: Packets may be dropped on a Fast ReRouting (FRR) backup tunnel.

  Conditions: This symptom is observed on a Cisco router when the primary MPLS TE tunnel is protected by a backup tunnel and when the protected tunnel interface is a subinterface that goes administratively down.

  Workaround: There is no workaround.

  Further Problem Description: Process-switched traffic (such as traffic that originates from the router itself or a ping with a record option) is not impacted.

- CSCsi86396

  Symptoms: Two subinterfaces may have the same CEF interface index.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when the following configuration sequence occurs:

  1. Create subinterface 1, 2, and 3.
  2. Delete subinterface 1.
  3. Create subinterface 4.
  4. Enable subinterface 1.

  In this situation, subinterface 1 and 4 may have the same CEF IDB.

  Workaround: There is no workaround. You must reload the platform to clear the symptoms.

- CSCsi89136

  Symptoms: When you remove and re-add a working VRF instance, the IP connectivity to VRF sites may break.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2, that functions as a PE router and a Layer 3 switch, and that connects to another PE router that has VRF instances.

  Workaround: There is no workaround.

- CSCsi98993

  Symptoms: When you attempt an FPD downgrade on an ATM SPA, an error message similar to the following may be generated, and the SPA may be disabled:

  ```
  %FPD_MGMT-3-FPD_UPGRADE_FAILED: I/O FPGA (FPD ID=1) image upgrade for SPA- 4XOC3-ATM
  card in subslot 3/0 has FAILED.
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an SPA-2XOC3-ATM, SPA-4XOC3-ATM, SPA-1XOC12-ATM, or SPA-1XOC48-ATM.

  With an SPA-2XOC3-ATM, SPA-4XOC3-ATM or SPA-1XOC12-ATM, the symptom occurs when the hardware version is newer than version 1.0 and when the downgrade FPD image version is older than version 1.26.

  With an SPA-1XOC48-ATM, the symptom occurs when the hardware version is newer than version 1.0 and when the downgrade FPD image version is older than version 0.15.

Workaround: There is no workaround to downgrade the FPD for these cases, but the symptom does not actually corrupt the FPD image on the SPA. You can bring up SPA again by entering the **hw-module subslot** *slot-number/subslot -number* **reload** command.

- CSCsj37398

  Symptoms: A CoS value may be incorrectly changed.

  Conditions: This symptom is observed on a cisco 7600 series when a register is not initialized properly, causing traffic to be marked to a random CoS value.

  Workaround: There is no workaround.

- CSCsj59997

  Symptoms: When a VTI is created, traffic that is generated by the Route Processor such as a ping and routing protocol hello messages may be dropped at the interface level.

  The output of the **show interface tunnel** *number* command shows the output drops:

```
router#sh int tu 1 | i drop
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 26
router#
```

  The output of the **show ip traffic** command shows that the number of “encapsulation failed” increases:

```
router#sh ip traff | i Drop
  Drop:  26 encapsulation failed, 0 unresolved, 0 no adjacency
router#
```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a SPA-IPSEC-2G when both of the following conditions are present:

  – The tunnel destination is not directly connected to the switch or router.

  – Proxy ARP is not enabled on the next-hop router to the tunnel destination.

  Workaround: Create a dummy ARP entry for each VTI tunnel destination, as in the following example:

```
arp <tunnel destination ip> 1111.1111.1111 arpa.
```

- CSCuk61396

  Symptoms: WCCP service redirection may not work. In particular, packets that are rejected by a third-party vendor appliance device and are returned to the router for normal forwarding may be discarded.

  Conditions: This symptom is observed on a Cisco router when NAT or Cisco IOS Firewall features are enabled on the same interfaces that have WCCP enabled.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCsi70727

  Symptoms: A fragment size may be incorrect for Link Fragmentation and Interleaving (LFI) over Frame Relay.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink PPP (MLP) over Frame Relay when a script tests LFI over Frame Relay by looking for a fragment size in the output of the **show ppp multilink interface** *number* command.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA4

Cisco IOS Release 12.2(33)SRA4 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA4 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCdy11174

  Symptoms: Some object of the ciscoFlashCopyTable and ciscoFlashMiscOpTable cannot be read after row creation.

  Conditions: This symptom is observed for any newly created rows in these tables.

  Workaround: Objects will become readable immediately after being set. Additionally, rows can still be activated in these tables even if all objects cannot be read. Any objects that cannot be read contain their MIB-defined default value.

- CSCeh85133

  Symptoms: A memory leak may occur when an SNMP trap is sent to a VRF destination. The output of the **show processes memory** command shows that the memory that is held by the process that creates the trap increases, and eventually causes a MALLOC failure. When this situation occurs, you must reload the platform.

  Conditions: This symptom is platform-independent and occurs in a configuration in which at least one VRF destination has the **snmp-server host** command enabled.

  Workaround: Ensure that no VRF is associated with the **snmp-server host** command.

- CSCsc09336

  Symptoms: When you enter the **show memory detailed** command, memory leaks in the process that this command is applied to.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured for Cisco IOS Software Modularity.

  Workaround: There is no workaround.

- CSCsd23056

  Symptoms: Reverse Telnet may not function.

  Conditions: This symptom is observed when AAA authentication is enabled for the asynchronous line over which you attempt to establish a reverse Telnet connection. The AAA authentication prompt takes the console output as input for the AAA authentication process, causing a login failure for reverse Telnet.

  Workaround: There is no workaround.

- CSCse80032

  Symptoms: An SNMP Manager that uses SNMPv3 may not resynchronize the timer for the SNMP engine after the router has been reloaded.

  Conditions: This symptom is observed on Cisco Catalyst 6000 series switch and Cisco 7600 series router that have been reloaded and occurs because a parameter is incorrectly set in the REPORT message, causing a mediation device to register an SNMP timeout instead of a reload.

Workaround: You may be able to restart the SNMP Manager to force the timer for the SNMP engine to resynchronize. Note, however, that doing so causes a 100-percent outage for all wiretaps that are served by the SNMP Manager. If you cannot restart the SNMP Manager, there is no workaround.

EXEC and Configuration Parser

- CSCsd32923

  Symptoms: A router may unexpectedly reload with a bus error when you enter a command while the command buffer is full of white space.

  Conditions: This symptom is observed when you enter a partial command and when the tab key is used while the command buffer is full.

  Workaround: There is no workaround.

IBM Connectivity

- CSCse17611

  Symptoms: When DLSw Ethernet Redundancy is configured, circuits may be established through the wrong switch.

  Conditions: This symptom is observed in the following configuration:

  – Clients are connecting to MAC A.

  – Mapping statements are configured so that “Switch 1” has a mapping of MAC A = MAC A and “Switch 2” has a mapping of MAC B = MAC A.

  The output of the **show dlsw transparent map** command shows that “Switch 1” has the active mapping and that “Switch 2” has the passive mapping. All circuits should be established on “Switch 1”, but instead they are established on “Switch 2”.

  The outputs of the **show dlsw trans neighbor** and **show dlsw trans map** commands show correct information, but the output of the **show dlsw cir cache** command shows state “negative” on “Switch 1” and state “positive” on “Switch 2”.

  Workaround: There is no workaround. Note that all circuits are up and running, but they just go through the wrong router.

Interfaces and Bridging

- CSCsd94687

  Symptoms: The output of the **show vlans** *vlanID* shows the wrong counters. The counters do not match the SNMP counters.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: Use only the SNMP counters.

IP Routing Protocols

- CSCed84633

  Symptoms: The *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command do not function.

Conditions: This symptom is observed on a Cisco platform that integrates the fix for caveat CSCea59206. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCea59206. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: There is no workaround.

Further Problem Description: The fix for CSCed84633 re-enables the *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command for both VRF interfaces and non-VRF interfaces.

- CSCei29944

  Symptoms: A CE router that has L2TP tunnels in an MPLS VPN environment with about 1000 VRFs may crash and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x50766038
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)S and that functions as a CE router when BGP neighbors are unconfigured via the **no neighbor** *ip-address* command while the **show ip bgp summary** command is entered from the Aux console. The symptom is not release-specific and may also affect other releases.

  Workaround: There is no workaround.

- CSCsd99760

  Symptoms: The routing table is not updated with an IP route for a prefix for a properly connected routed interface even though the CEF table shows a receive entry for the same prefix at both the RP and the SP.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when the following conditions occur:

  1. The IP routing process iprouting.iosproc is restarted.
  2. You change a switch virtual interface (SVI) port to a routed port.
  3. You configure the port with the same IP address as the address that was associated with the SVI port.
  4. You make the port active by entering the **no shutdown** command.

  In this situation, the routing table is not updated with the IP route for the prefix for the new routed port.

  Workaround: Restart the IP routing process iprouting.iosproc once more.

- CSCse05031

  Symptoms: The **neighbor default-originate** command does not function properly when the **route map** keyword and *map-name* argument are defined.

  Conditions: This symptom is observed when the target route that is specified in the route map is added or removed from the routing table after the BGP session has already been established.

  Workaround: Clear and re-establish the BGP neighbor.

- CSCse41484

  Symptoms: A DMVPN hub receives a few unencrypted GRE packets from a spoke during the negotiation of an IPsec security association (SA).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for NHRP and that have an IPsec VPN SPA that functions as a spoke in a DMVPN topology.

Workaround: There is no workaround.

- CSCsf99057

  Symptoms: The OSPF Stub Router Advertisement feature may stop functioning after an RPR+ or SSO switchover has occurred, and the newly active RP does not originate router LSAs with infinity metric as it should do when the **max-metric router-lsa on-startup** router configuration command is enabled.

  Conditions: This symptom is observed on a Cisco router that has dual RPs that function in RPR+ or SSO mode when NSF is not enabled on the router and when the standby RP is in the "Standby-Hot" state.

  Workaround: Do not configure RPR+ or SSO. Rather, configure RPR. If this is not an option, there is no workaround.

- CSCsg43140

  Symptoms: A router may crash during the boot process and return to ROMmon.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that has VPNs configured.

  Workaround: There is no workaround.

ISO CLNS

- CSCse34050

  Symptoms: IS-IS may not advertise a passive interface when it should do so, or IS-IS may advertise a passive interface when it should not do so.

  Conditions: This symptom is observed on a Cisco router when IS-IS misinterprets an interface "shutdown" event as an UP event.

  Workaround: Enable IS-IS on the interface by entering the **ip router isis** command and then make the interface passive by entering the **no ip router isis** command followed by the **passive-interface** *interface-type interface-number* command.

- CSCsf26043

  Symptoms: IS-IS protocol packets may not be classified as high-priority. When this situation occurs during stress conditions and when the IS-IS protocol packets are mixed with other packets, the IS-IS protocol packets may be dropped because of their low-priority.

  Conditions: This symptom is observed on a Cisco platform that is configured for Selective Packet Discard (SPD).

  Workaround: Ensure that DSCP rewrite is enabled and then enter the following command:

  ```
  mls qos protocol isis precedence 6
  ```

Miscellaneous

- CSCeb05456

  Symptoms: A Cisco platform may reset its RP when two simultaneous **write memory** commands from two different vty connections are executed, and messages similar to the following may appear in the crashinfo file:

  ```
  validblock_diagnose, code = 10
  ```

  ```
  current memory block, bp = 0x48FCC7D8,
  memory pool type is Processor
  data check, ptr = 0x48FCC808
  ```

  ```
  next memory block, bp = 0x491AC060,
  memory pool type is Processor
  data check, ptr = 0x491AC090
  ```

  ```
  previous memory block, bp = 0x48FCBBE8,
  memory pool type is Processor
  data check, ptr = 0x48FCBC18
  ```

  The symptom is intermittent and is related to the way NVRAM is accessed.

  Conditions: This symptom is observed on a Catalyst 6000 series Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXD but is platform- and release-independent.

  Workaround: Set the boot configuration to non-NVRAM media such as a disk or bootflash by entering the following commands:

  ```
  boot config disk0:
  filename
  nvbypass
  ```

- CSCeb21064

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCeg02918

  Symptoms: A Cisco router that is configured with an HTTP authentication proxy may reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs a crypto image of Cisco IOS Release 12.3(9) or Release 12.3(10). Note that the symptom is not release-specific.

Workaround: Disable the HTTP authentication proxy. If this is not an option, there is no workaround.

- CSCeh18195

  Symptoms: Packets that flow to VPNv4 destinations may be dropped for up to one second when the next-hop router clears its IS-IS overload bit after having been rebooted.

  Conditions: This symptom is observed in a MPLS-TE network with one-hop TE tunnels.

  Workaround: There is no workaround.

- CSCeh86935

  Symptoms: As a user of a router, you cannot authenticate or authorize via a TACACS+ server. A TCP SYN that is sent from the router to port 49 of the TACACS+ server carries an incorrect source IP address. Instead of the address that is specified in the **ip tacacs source-interface** *subinterface-name* command, the router uses the default address for login authentication and exec authorization. The nondefault source interface is correctly used for command authorization.

  Conditions: This symptom is observed on a Cisco router that is configured to use a nondefault source interface to connect to a TACACS+ server when there is at least one authentication or authorization method list configured to use one more TACACS+ servers and when the following command sequence is enabled:

  ```
  aaa new-model
  tacacs-server host host-ip-address
  tacacs-server key key
  ip tacacs source-interface subinterface-name
  ```

  Workaround: Remove the **ip tacacs source-interface** *subinterface-name* command.

  Further Problem Description: Protocols other than TACACS+ that use TCP and that are implemented via the sockets library may also use an incorrect source address when they are configured to use a nondefault source interface or address. This situation may cause problems, depending on the configuration of the router, the routing tables, and the configuration of the outside client or server with which the other protocol communicates. In Cisco IOS software images, most services that use TCP, including BGP, are not implemented via sockets but, instead, use a proprietary interface for the TCP protocol, and are not affected.

  Some older versions of TACACS+ do not use sockets. In a Cisco IOS software image with such an older TACACS+ version, TACACS+ is not affected but other services may still be affected.

  Workaround for protocols other than TACACS+: Remove the configuration that specifies a source interface or source address from the router.

- CSCei52830

  Symptoms: A router or switch may not properly function when you enter a message-of-the-day (MOTD) through the **banner motd** *d message d* command because the *d message d* argument of the command may not be synchronized to the standby RP.

  Conditions: This symptom is observed on Cisco router or switch that is configured for SSO.

  Workaround: Do not enter the **banner motd** *d message d* command.

- CSCej08637

  Symptoms: When you run the Entity-MIB on a redundant system, the standby supervisor engine may reset. When you enter the **show environment status** command on the standby supervisor engine, the module information is not shown, nor are inline power sensors on the VDB shown.

  Conditions: These symptoms are observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured for SSO.

Workaround: There is no workaround.

- CSCej21698

  Symptoms: A switch or router that is configured for multicast may generate the following error message when stress traffic is sent:

  ```
  %EARL_L2_ASIC-DFC8-4-SRCH_ENG_FAIL: EARL L2 ASIC Search Engine has failed: ios-base
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that functions under stress.

  Workaround: There's no workaround.

- CSCek35417

  Symptoms: When the ROMmon of an RP on a Supervisor Engine 720 resets or reboots or when the platform resets or reboots, the ROMmon may not load the runtime image because of a corrupted NVRAM. When this situation occurs, the following error message is generated:

  ```
  "Warning: Rommon NVRAM area is corrupted. Initialize the area to default values
  Cat6k-Sup720/RP platform with 1048576 Kbytes of main memory"
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have a Supervisor Engine 720 on which the NVRAM is installed on a flash device.

  Workaround: Erase the ROMmon in the NVRAM and set the ROMmon confreg utility to 0x2102, as in the following example:

  ```
  rommon 1 > priv
  rommon 2 > nvram_erase

  Enter in hex value the start address [0x0]:  0xbe000000
  Enter in hex value the test size or length in bytes [0x0]:  0x20000

  rommon 3 > confreg 0x2102
  rommon 4 > reset
  ```

- CSCek47574

  Symptoms: When you enter a **traceroute** command to check the route to an interface that has MPLS enabled, the first hop may be dropped. After the first hop, the **traceroute** command completes normally. Furthermore, for each **traceroute** command, three input errors occur on the MPLS interface.

  Conditions: These symptoms are observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2 and that is configured with a SIP-400 in which an OC-48 SPA is installed. The symptom occur when the MPLS interface receives packets while the time-to-live (TTL) is set to "0" or "1". The MPLS interface drops these packets.

  Workaround: There is no workaround. However, the symptom does not affect the functionality of the router.

  Further Problem Description: Although the symptom is observed with the **traceroute** command, the packets drops could occur with any application when the TTL is set to "0" or "1".

- CSCek63611

  Symptoms: IPSec SA rekey operations may fail with an IPSec VPN SPA (SPA-IPSEC-2G).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router for SAs that are established after the SPA-IPSEC-2G has been reloaded.

  Workaround: There is no workaround.

- CSCek66277

  Symptoms: When you run the TestAclDeny diagnostic test, the output of the **show diagnostic content module** *num* command, with the *num* representing the active supervisor engine, shows the test as "N" to denote non-disruptive. This situation is shown in the following example:

  ```
  18) TestAclDeny --------------------> M**N****A*** 000 00:00:05.00 n/a
  ```

  In reality, the TestAclDeny diagnostic test for the active supervisor engine is a disruptive test because the test may cause traffic forwarding issues and flapping of the first uplink port.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Do not run the TestAclDeny diagnostic test.

  Further Problem Description: The fix for this caveat sets the flag to "D" to denote disruptive.

- CSCek67100

  Symptoms: A crashdump may not be saved when a SSC-400 crashes.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCek67701

  Symptoms: When an exception occurs on an IPSec VPN SPA (SPA-IPSEC-2G) there is insufficient time to save the crashdump file before the SPA-IPSEC-2G is automatically reset.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables the SPA-IPSEC-2G to save the crashinfo file. In turn, the crashinfo file enables you to find the cause of the exception.

- CSCek70058

  Symptoms: An Optical Services Module (OSM) may crash because of a memory corruption.

  Conditions: This symptom is observed when you apply a QoS configuration with WRED.

  Workaround: There is no workaround.

- CSCir00786

  Symptoms: When you attempt to update the startup configuration from a file but the **boot** commands are incorrect or you are unauthorized to enter the **boot** commands, a boot configuration error message should be displayed, but this does not occur.

  Conditions: This symptom is observed on a Cisco router after the startup configuration has been updated by SNMP.

  Workaround: Perform the following tasks:

  1. Copy the startup configuration to the running configuration.
  2. Copy the running configuration to the startup configuration.
  3. Verify manually that the **boot** commands are indeed correct and use the CLI to update the startup configuration.

- CSCsb45696

  Symptoms: A platform may reload in response to malformed 802.1x EAP traffic.

Conditions: This symptom is observed on a Cisco Catalyst 3750 that runs Cisco IOS Release 12.2(25)SEC. However, the symptom is both platform- and release-independent.

Workaround: There is no workaround.

- CSCsb54378

  Symptoms: A router may reload due to software forced crash.

  Conditions: This problem has been observed when initiating a Secure Shell (SSH) session from the router or when copying a file to/from the router via SCP.

  Workaround: Do not initiate SSH or SCP sessions from the router.

  Further Problem Description: This was observed on a Cisco 2811 router that was running Cisco IOS Release 12.4(4)T. Note that the symptom is not platform- or release-specific.

  Prior to the crash, the router logs a series of %SYS-3-CPUHOG messages and will eventually crash with %SYS-2-WATCHDOG. See the following example:

  ```
  %SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs
  (1426/5),process = Virtual Exec.
  -Traceback= 0x41DC8E2C 0x41DC9098 0x41BAA6E0 0x41BA6990 0x41B96B4C 0x41BA6768
  0x41BA7490 0x41BA7750
  0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8
  0x41834200
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Virtual Exec.
  -Traceback= 0x41A23CC8 0x41BAA3D8 0x41BA6A08 0x41B96B4C 0x41BA6768 0x41BA7490
  0x41BA7750 0x41BAC854
  0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8 0x41834200
  0x418341E4
  %Software-forced reload
  ```

- CSCsb61381

  Symptoms: A router or switch that has an ATA file system may crash when the **dir** *all-filesystems* command is executed.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router. The symptom may occur when a network management tool such as CiscoWorks periodically backs up or restores the vlan.dat file along with the configuration of the system while other periodic scripts execute the **dir** *all-filesystems* command.

  Workaround: Prevent applications such as CiscoWorks from accessing the vlan.dat file.

- CSCsb64767

  Symptoms: When a layer 2 EtherChannel is load-balancing multicast traffic on multiple member ports of a local switch or router, one port may not transmit multicast packets but may drop them. When this situation occurs, the OutMcastPkts counter for this port does not increase.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when an OIR is performed on a line card of the remote switch or router, causing the local port that is a member of the EtherChannel to change its state to link down and then to link up.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on affected member port of the local switch or router. Doing so re-enables multicast forwarding.

- CSCsb66799

  Symptoms: After a router has been reloaded, an URL match statement unexpectedly may be removed from the configuration.

  Conditions: This symptom is observed when the **match protocol http url** *url-string* command is enabled. After the router has been reloaded, this command has disappeared from the configuration.

  Workaround: There is no workaround.

- CSCsb79031

  Symptoms: A Cisco Catalyst 6500 series switch or Cisco 7600 series router may crash when you enter the **clear counters** command.

  Conditions: This symptom is observed when a communication problem occurs with one of the CSMs. Internal communication problems can be reported through an ICC, IPC, or SCP error message such as the following ICC-4-HEARTBEAT message:

  ```
  %ICC-4-HEARTBEAT: Card 6 failed to respond to heartbeat.
  ```

  Workaround: Do not enter the **clear counters** command when an ICC-4-HEARTBEAT message is generated for an CSM.

- CSCsc09892

  Symptoms: A spurious memory access may occur on a supervisor engine.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for SNMP and QoS.

  Workaround: There is no workaround.

- CSCsc19259

  The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

  The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml.

- CSCsc33990

  Symptoms: A supervisor engine may unexpectedly reset when the TestSPRPInbandPing as part of the Cisco Generic Online Diagnostics (GOLD) fails for 10 consecutive times.

  The following syslog error messages are typically generated right before the supervisor engine resets, and can also be found in the crashinfo files:

  ```
  %CONST_DIAG-SP-3-HM_TEST_FAIL: Module <slot#> TestSPRPInbandPing consecutive failure
  count:5
  %CONST_DIAG-SP-6-HM_TEST_INFO: CPU util(5sec): SP=10% RP=0% Traffic=0%
  netint_thr_active[0], Tx_Rate[4412], Rx_Rate[0]
  %CONST_DIAG-SP-3-HM_TEST_FAIL: Module <slot#> TestSPRPInbandPing consecutive failure
  count:10
  ```

```
%CONST_DIAG-SP-6-HM_TEST_INFO: CPU util(5sec): SP=10% RP=0% Traffic=0%
netint_thr_active[0], Tx_Rate[4652], Rx_Rate[0]
%CONST_DIAG-SP-2-HM_SUP_CRSH: Supervisor crashed due to unrecoverable errors, Reason:
Failed TestSPRPInbandPing
```

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that run an integrated Cisco IOS software image. The trigger for the symptom may be possible corruption in TCAM entries that are used to perform the TestSPRPInbandPing.

Workaround: Enter the **no diagnostic crash** global configuration command to disable exceptions that are being triggered by failed diagnostic monitoring. However, you should do this with discretion because it may also prevent the system from taking proactive measure to mitigate problems that could impact user traffic.

Further Information: The fix for this caveat is more of an enhancement because it only prevents the system from being over-aggressive in taking exceptions when the TestSPRPInbandPing fails under specific conditions. Therefore, the fix for this caveat does not address all triggers that may cause the TestSPRPInbandPing to fail. Please consult Cisco TAC for further assistance if you experience the same problem after upgrading to a Cisco IOS software image that contains the fix for this caveat.

- CSCsc46105

  Symptoms: The type of service (ToS) value from a Cisco SSL Module (SSLM) for back-end encryption is not carried over but is stripped off.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when the **tos carryover** command is enabled on the SSLM and when the **mls qos** command is enabled in Native IOS. The symptom does not occur when the **mls qos** command is not enabled, nor does it occur for encryption in the direction of the clients.

  Workaround: Disable the **mls qos** command in Native IOS.

- CSCsc56766

  Symptoms: When channel members of an EtherChannel are located on different forwarding engines and when one channel goes down, traffic may be disturbed for six seconds or longer and a control protocol may be adversely affected. The duration of the traffic disturbance depends on the number of VLANs.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch but may also occur on a Cisco 7600 series router.

  Workaround: Place all members of the EtherChannel on the same forwarding engine.

  Alternate Workaround: Limit the number of VLANs on the trunk.

- CSCsc71245

  Symptoms: A router that is connected to several VPN clients may unexpectedly reload because of a CPUHOG condition in the crypto IKMP process followed by a watchdog timeout.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router and occurs about every about 24 hours, which is equal to the IKE lifetime.

  Workaround: There is no workaround.

- CSCsd17641

  Symptoms: A hierarchical service policy may not be attached to a subinterface, and no error message is generated, as if the configuration is ignored. Entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the subinterface or deleting the subinterface does not have any effect.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2 and that is configured with subinterfaces on a SPA-2X1GE that is installed in a SIP-400.

Workaround: Do not use a hierarchical service policy.

Further Problem Description: Debugs of the SIP-400 show that for the subinterfaces that works fine, the SIP-400 received the commands from MQC. For the subinterfaces that do not work, the SIP-400 did not receive any commands to program the queues.

- CSCsd28214

  Symptoms: A Cisco router may crash because of a watch dog timeout while running the RIP routing protocol.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3(19) when an interface changes state at the exact same time that a RIP route that was learned on this interface is being replaced with a better metric redistributed route. For example, when RIP has learned the 192.168.1.0 network from Fast Ethernet 1/0 interface and then RIP learns the 192.168.1.0 network from a redistributed protocol that has a better metric, the RIP route is removed. However, when during this time the Fast Ethernet 1/0 interface goes down, the router may crash because of a watch dog timeout. Note that the symptom may also affect other releases.

  Workaround: There is no workaround.

- CSCsd70948

  Symptoms: After an SSO switchover occurs, the supervisor engine stops receiving BPDUs and CDPs. You must reload the platform to enable the platform to receive CDP and BPDUs.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when rate-limiting of layer 2 BPDUs is enabled through the **mls rate-limit layer2 pdu** command.

  Workaround: Disable rate-limiting of layer 2 BPDUs by entering the **no mls rate-limit layer2 pdu** command.

- CSCsd71047

  Symptoms: When the MAC address of a local-source address in a NAT configuration is changed, for example because of a failover between NICs, the corresponding NetFlow entry is not updated, causing return traffic to continue to be send to the old MAC address. In turn, this situation causes traffic to be dropped at the destination or to be send to an incorrect interface until the NetFlow entry times out or is cleared.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when either static NAT or dynamic NAT is configured.

  Workaround: Clear the corresponding NetFlow entry by entering the **clear mls netflow ip destination** *ip-address* command.

- CSCsd77751

  Symptoms: A router may sends empty or blank syslog messages. For example, this situation may occur after the following error messages have been generated:

  ```
  %SYS-3-LOGGER_FLUSHING, %OIR-SP-STDBY-6-CONSOLE, %SYS-SP-STDBY-3-LOGGER_FLUSHED,
  %PFREDUN-SP-STDBY-6-ACTIVE ...
  ```

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

  Workaround: There is no workaround.

- CSCsd80632

  Symptoms: A change to the 64-bit high capacity (HC) input traffic counter of a main interface does not equal the sum of the changes for the HC input traffic counters of its subinterfaces.

  Conditions: This symptom is observed on a Cisco router that is configured for SNMP when the main interface is configured for Frame Relay.

  Workaround: There is no workaround.

- CSCsd81275

  Symptoms: When a standby supervisor engine or standby RP comes up, the following error message may be generated:

  ```
  %PFINIT-SP-1-CONFIG_SYNC_FAIL: Sync'ing the private configuration to the standby
  Router FAILED, the file may be already locked by a command like: show config.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for ISSU.

  Workaround: There is no workaround.

- CSCsd81407

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)

  – Media Gateway Control Protocol (MGCP)

  – Signaling protocols H.323, H.254

  – Real-time Transport Protocol (RTP)

  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsd88401

  Symptoms: Incoming packets may be dropped at the GE-WAN port 2 on an OSM-2+4GE-WAN+. In addition, the output of the **show platform hardware gt48520 counters** command shows that "mac_rx_error" errors for the OSM-2+4GE-WAN+ are increasing.

  Conditions: This symptom is observed on a Cisco 7600 series that processes IPv4 TCP and UDP packets with a random data pattern on an OSM-2+4GE-WAN+ with hardware revision 2.4 or lower. Note that the symptom occurs only on GE-WAN port 2, not on the other ports.

  Workaround: There is no workaround.

  Further Problem Description: Both upgrade the Cisco IOS software image to an image that integrates the fix for caveat CSCsd88401 and change the hardware revision of the OSM-2+4GE-WAN+ to 2.5.

- CSCsd88636

  Symptoms: Continuous CPUHOGs may occur during the "ATM OAM Input" process, locking the console for a long time.

Conditions: This symptom is observed on the MSFC of a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA and that has an ATM interface with several VCs that are configured for Single Cell Relay (VC Mode). These VCs are configured on a PA-A3-OC3 or PA-A6-OC3 port adapter that is installed in an enhanced FlexWAN module. The symptom occurs after the peer router that is connected to the ATM interface (and on which the PVPs are configured) is reloaded.

Note that the symptom is not platform- or release-dependent.

Workaround: When the console is less busy, shut down the ATM interface on the peer router. The CPUHOGs may stop after some time. If this is not an option, there is no workaround.

- CSCsd94127

  Symptoms: An egress CoS is unexpectedly rewritten by the Internet Printing Protocol (IPP) on the ingress side.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when multicast traffic is routed over an ingress trunk interface on which the **mls qos trust cos** interface configuration command is enabled.

  Note that the symptom occurs only for routed multicast traffic. The symptom does not occur for other traffic such as layer 2 multicast and layer 2/layer 3 unicast traffic.

  Workaround: There is no workaround.

- CSCsd95575

  Symptoms: A switch or router crashes because of a TEMPALARM message on the SP.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have a Supervisor Engine 720 router and occurs only with an automated script, often when the script runs the **clear ip route *** command.

  Workaround: There is no workaround.

- CSCsd98390

  Symptoms: A WS-X6148A-45AF module may not boot when you power-cycle the platform. The output of the **show module** shows the module status as “unknown.” In addition, one or more modules may lose their configuration.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with eight or more modules.

  Workaround: Do not power-cycle the platform but enter the **reload** command.

- CSCse12154

  Symptoms: A router may crash because of a bus error when you enter the **copy scp** command to copy a configuration.

  Conditions: This symptom is observed on a Cisco router that is configured for SSH.

  Workaround: Do not use SCP. Rather, use Remote Copy Protocol (RCP) or use a TFTP transfer.

- CSCse24889

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t
ip ssh version 1 end
```

Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

```
10.1.1.0/24 is a trusted network that
is permitted access to the router, all
other access is denied
```

```
access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any
```

```
line vty 0 4
access-class 99 in
end
```

Further Problem Description:

For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapte r09186a0080716ec2.html

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

http://www.cisco.com/warp/public/707/ssh.shtml

- CSCse37587

  Symptoms: When DHCP snooping is enabled in conjunction with VRF, DHCP clients do not receive a DHCP IP address.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that function as a DHCP server.

  Workaround: There is no workaround.

- CSCse40423

  Symptoms: A tunnel interface cannot ping the other end of an IP tunnel.

  Conditions: This symptom is observed when ATM is configured and when the tunnel interface is up.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the tunnel interface.

- CSCse49388

  Symptoms: On a physical interface or subinterface on which a tunnel is configured and that encrypts or decrypts traffic, when you shut down and bring up the physical interface or subinterface multiple times, MAC entries for all VLANs that support the tunnel may be removed.

  When this situation occurs, when the “RMac reference” counter reaches 1, and when you shut down the physical interface or subinterface for the last time, packets are prevented from traversing the tunnel.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with either a Supervisor Engine 32 or a Supervisor Engine 720 and with a SIP-400 in which an IPsec VPN SPA is installed.

Workaround: To prevent the symptom from occurring, do not shut down and bring up the physical interface or subinterface that supports the IPsec tunnel. When the symptom has occurred, reload the SIP-400 to reset the “RMac reference” counter to the original value.

Further Problem Description: To see if the symptom has occurred, check the “RMac reference” counter as follows:

```
# remote login switch
sp# test mls net debug task 1 stat
...
Netflow RMac List:
0013.5f21.9100[14] <<-- where [n] is the reference count, in this case 14.
Tunnel Interface(s):
...
sp#
```

You can check the counter each time after you have shut down and brought up the physical interface or subinterface. If, after every iteration, the reference count keeps decrementing towards 0, it means the symptom has occurred. A flapping link does not cause this problem. The “RMac reference” counter decreases each time that you shut down the physical interface or subinterface, perform and OIR of the SPA, or reset the SPA.

- CSCse56501

  Symptoms: When two sockets are bound to the same port, the first File Descriptor always receives the requests.

  Conditions: This symptom is observed on a Cisco router when two sockets such as one IPv4 socket and one IPv6 socket are connected to the same UDP port.

  Workaround: Use different UDP ports for different sockets.

- CSCse56921

  Symptoms: A platform that is configured for GPRS Tunneling Protocol (GTP) Server Load Balancing (SLB) may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when the same International Mobile Subscriber Identity (IMSI) is sent in two or more Packet Data Protocol (PDP) requests to different virtual servers and occurs when the sticky table entries time-out.

  Workaround: There is no workaround.

- CSCse69713

  Symptoms: When all cache engines in a WCCP service group are inactive, the traffic is handled by the software; the traffic is CEF-switched by the software instead of FIB-switched in the hardware.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Remove and re-enter the **ip wccp webcache** command.

- CSCse97422

  Symptoms: When you enter the **show tech** command with long a regular expression, the platform may crash during the display of the command output. For example, this situation may occur when you enter the following command:

  ```
  show tech |  e (0.00%  0.00%  0.00%|cmd_sts|0  0|ast clearing|packets input|packets
  output|SESs|LMI enq|cast queue|Last input|OAM cells input|reliability 255)
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 720.

Workaround: Do not use a long regular expression when you enter the **show tech** command.

- CSCsf03566

  Symptoms: On a router that functions as an EzVPN server, a software-forced crash may occur because of memory corruption.

  Conditions: This symptom is observed on a Cisco 7600 series router that runs Cisco IOS Release 12.2(18)SXF when Extended Authentication (Xauth) is enabled while the crypto session is brought down. The symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCsf07232

  Symptoms: Tcl standard I/O operations such as a **puts** command may not display text on the terminal line under which the Tcl code is running. The text may be displayed on the terminal line that was the first one to connect (for example, vty0) or may not be displayed anywhere. Both print to standard output (STDOUT) and standard error (STDERR) streams are affected.

  Conditions: This symptom is observed on a Cisco router when more than one user is logged into a device, when one user enters Tcl Shell mode via the **tclsh** command, and then a second user enters Tcl Shell mode.

  Workaround: Ensure that only one user is connected to the device when Tcl standard I/O operations are run. If this is not an option, there is no workaround.

  Further Problem Description: When Tcl standard I/O operations are run on vty0 with only one user logged in, the text is displayed correctly.

- CSCsf14994

  Symptoms: A ping may not go through an MLP interface that is configured on a channelized T1/E1 SPA, channelized T3 SPA, or channelized STM-1 SPA.

  Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

  1. You remove a multilink interface by entering the **no interface multilink** *multilink-bundle-number* command without first removing the member links from the bundle.
  2. You recreate the same multilink interface.
  3. You configure the multilink bundle by adding links from a different SPA that is installed in the same SIP.

  Workaround: First remove the **multilink-group** command from the member link configuration before you enter the **no interface multilink** *multilink-bundle-number* command.

- CSCsf31458

  Symptoms: The entPhysicalIndex object of the ENTITY-MIB may not remain the same after an SSO switchover has occurred on a Supervisor Engine 32.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsf97682

  Symptoms: An E3/T3 interface that is located on a SPA in a SIP-200 does not come up. The controller is active, but the line-protocol remains down. Even with a physical loop, the E3/T3 interface does not enter the UP/UP (looped) state.

Conditions: This symptom is observed on a Cisco 7600 series that has a SUP720-3BXL supervisor engine that runs Cisco IOS Release 12.2(33)SRA2 or Release 12.2(33)SRA3. For the symptom to occur, the diagnostics must be minimal or complete.

Workaround: Configure bypass for the diagnostics by entering the **diagnostic bootup level bypass** command. Then, reset the SIP-200 by entering the **hw-module module** *slot-number* **reset** command or reload the SPA by entering the **hw-module subslot** *slot/subslot* **reload** command.

Further Problem Description: The symptom does not occur in Release 12.2(33)SRB and Release 12.2(33)SRA1.

- CSCsf98345

  Symptoms: An MPLS LDP peer on a default VRF resets when a VRF interface goes down.

  Conditions: This symptom is observed on a Cisco router when the VRF interface is configured with a subnetwork address that overlaps with the default router ID.

  Workaround: Reconfigure the VRF interface address so it does not overlap with the default router ID.

- CSCsg02241

  Symptoms: Incorrect NAT translation may occur for one or more faulty Multilayer Switching (MLS) flows. You can recognize a faulty MLS flow in the output of the **show mls netflow ip** command. If any two MLS flows show the same adjacency, one of the MLS flows is faulty.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for NAT and occurs regardless of whether or not a Supervisor Engine 32 or Supervisor Engine 720 is configured for central or distributed forwarding.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(18)SXF8 and later releases.

- CSCsg02605

  Symptoms: After a packet buffer parity error has occurred on one port of a group of 12 ports, an Ethernet module does not go through the rapid reboot process but rather reboots regularly, which takes about 40 seconds.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and affects the following modules when these are configured for to reset as a corrective action after an error has occurred:

  – WS-X6348-RJ-45
  – WS-X6348-RJ-21V
  – WS-X6248-RJ-45
  – WS-X6248-TEL
  – WS-X6148-RJ-45
  – WS-X6148-RJ-21

  Workaround: There is no workaround.

- CSCsg03483

  Symptoms: When you attempt to create a new VRF, the following error message may be generated:

  ```
  %FIB-SP-STDBY-4-FIBCBLK: Missing cef table for tableid 2 during route update XDR event
  SLOT 2:
  %FIB-4-FIBCBLK: Missing cef table for tableid 2 during route update XDR event
  %FIB-SP-4-FIBCBLK: Missing cef table for tableid 2 during route update XDR event
  ```

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA1 but may be platform- and release-independent.

Workaround: There is no workaround.

- CSCsg03739

  Symptoms: A memory leak may occur in the “Crypto IKMP” process.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an IPSec VPN SPA (SPA-IPSEC-2G).

  Workaround: There is no workaround.

- CSCsg08200

  Symptoms: The bootup diagnostics for a line card may detect a major failure after an RPR switchover has occurred, and these line cards reset repeatedly and eventually power-down.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs only with a Supervisor Engine 720 that is configured with a PFC3BXL (WS-SUP720-3BXL) or with a DFC3BXL-equipped module.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur after an SSO or RPR+ switchover has occurred.

- CSCsg10075

  Symptoms: When you enter the **show policy-map interface** command, the platform may hang at the --More-- prompt.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router but may also affect other platforms.

  Workaround: There is no workaround.

- CSCsg16425

  Symptoms: The output of the **show ip slb reals** command displays very large connection values (conns) for some real servers.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for Cisco IOS Server Load Balancing (IOS SLB) with inter-firewall routing enabled via the **ip slb route inter-firewall** command. The symptom occurs only when the inter-firewall connections switch from one firewall real to other firewall real in the firewall farm.

  Workaround: Remove and reconfigure the real server that is part of the server farm or firewall farm.

  Further Problem Description: When the connection value for a real server becomes very large, the server may enter the “MAXCONNS” state. When this situation occurs, you can no longer clear the connections counter by entering the **clear ip slb counters** or **clear ip slb connections** command.

- CSCsg19208

  Symptoms: When you reload a PE router, the standby RP crashes.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router in an MPLS configuration with TE tunnels and per-VRF-aggregate labels.

  Workaround: There is no workaround.

- CSCsg21429

  Symptoms: The interface of an OSM-1OC48-POS-SI+ module may flap after you have entered the **redundancy force-switchover** command.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with redundant Supervisor Engine 720-3BXL modules that function in RPR+ mode.

Workaround: Repeat the **redundancy force-switchover** command several times.

- CSCsg24609

  Symptoms: A MIB walk on the CISCO-L2-CONTROL-MIB occurs very slowly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that do not have the **mac-address-table limit vlan** *vlan* command enabled.

  Workaround: Enter the **mac-address-table limit vlan** *vlan* command.

- CSCsg35506

  Symptoms: After a Gigabit Ethernet (GE) interface has flapped, a mismatch may occur on a port channel, preventing the GE interface from joining the port channel. This situation occurs when the default flow control operational mode on the GE interface is unexpectedly changed from “off/off” to “on” after the GE interface has flapped.

  If the symptom occurs for the first interface of a group of interfaces that is supposed to join the port channel, none of the interfaces in the group can join the port channel, degrading the bandwidth and possibly causing severe packet drops on the channel.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router, and affects the following modules:

  – Supervisor Engines 1 and 1a
  – Supervisor Engine 2
  – WS-X6408-GBIC
  – WS-X6416-GBIC
  – WS-X6516-GBIC and WS-X6516A-GBIC

  Note that the symptom does not occur with the WS-X6724-SFP and the WS-X6748-GE-TX.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected GE interface.

  Further Problem Description:

  – Any operation that causes flow control negotiation triggers the symptom. For example. problem, entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command, resetting the module, performing an OIR, an RPR switchover, and so on.
  – The symptom tends to occur when many ports are brought up simultaneously.

- CSCsg37484

  Symptoms: A router may reload because of a bus error in a crypto map and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x4284A878
  ```

  Conditions: This symptom is observed on a Cisco router that has an IPSec crypto map.

  Workaround: There is no workaround.

- CSCsg40425

  Symptoms: An Optical Services Module (OSM) may reset unexpectedly and generate the following error messages:

  ```
  %POSLC-3-SOP: TxSOP-0 SOP. (source=0x18, halt_minor0=0x4000)
  %CWANLC-3-FATAL: Fatal Management interrupt, gen_mgmt_intr_status 0x0,
  line_mgmt_intr_status 0x1, reloading
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsg40567

  Symptoms: Malformed SSL packets may cause a router to leak multiple memory blocks.

  Conditions: This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

  Workaround: Disable the **ip http secure server** command.

- CSCsg42246

  Symptoms: High CPU use may occur in the “IP Background” process, and the router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that is configured for RIP and that receives a RIP host route that is subsequently replaced by a route that is dynamically assigned to an interface. For example, this situation may occur on a PPP interface that has the **ip address negotiated** command enabled.

  Workaround: Use a route map to block the advertised route.

- CSCsg43284

  Symptoms: A VPN tunnel may fail to establish a proper connection to a Cisco Catalyst 6500 series switch or Cisco 7600 series router because fragmented ISAKMP packet are dropped by the IPSec VPN Services Module (SPA-IPSEC-2G).

  Conditions: This symptom may occur for many reasons, including the following:

  – The peer sends too many different proposals.

  – The certificate that is used by the peer is too large, for example, because the key is too large, the issuer-name is long, the subject-name is long, the are many CDPs, and so on.

  Workaround: In some circumstances, when the peer is an EzVPN client router that runs Cisco IOS Release 12.4T, changing the Cisco IOS software image to Release 12.4 may reduce the size of the proposals.

  When the certificate of the peer is too large, reduce the size of the RSA key, and/or remove or reduce long fields in the certificate.

  Further Problem Description: When the symptom occurs, a packet capture of all traffic that is received by and sent to the switch or router shows the following:

  – The fragmented ISAKMP packets that are sent to the switch or router.

  – The response (several seconds or up to one minute later) of the switch or router with the following ICMP packet:

    ```
    Type: 11 (Time-to-live exceeded)
    Code: 1 (Fragment reassembly time exceeded)
    ```

- CSCsg47462

  Symptoms: A router that is configured with at least one multipoint GRE tunnel may crash with an address error.

Conditions: This symptom is observed when a T3 interface bounces while the CPU usage of the router is at 100 percent.

Workaround: There is no workaround.

- CSCsg61773

  Symptoms: Egress multicast forwarding may not function when an outgoing interface (OIF) flaps very quickly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when Multicast MultiLayer Switching (MMLS) is configured (MMLS is configured by default).

  Workaround: There is no workaround.

  Further Problem Description: When an interface flaps very quickly, the module mask may not be allocated for the interface, causing the egress multicast functionality to be affected. In this situation, the interface may not function properly as an OIF.

- CSCsg69646

  Symptoms: An IPSec VPN SPA (SPA-IPSEC-2G) may stop forwarding traffic over GRE tunnels that are configured with tunnel protection.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs on a rare intermittent basis when the CPU processing load of the RP is high, for example, when there is a large number of crypto certificates being processed.

  Workaround: There is no workaround.

- CSCsg73179

  Symptoms: After a change in the routing topology, a Bidirectional PIM Rendezvous Point is not updated correctly in the hardware tables, causing Bidirectional PIM multicast flows to be software-switched.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs only when the ACL that is used to statically configure the Rendezvous Point does not have any wildcard entries.

  Workaround: Reinstall the Rendezvous Point.

- CSCsg79810

  Symptoms: The MPLS MTU is overruled by the IP MTU on an ATM interface.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an MPLS core when the ATM interface has the **tag-switching mtu 1508** command and the **ip mtu 1500** command enabled. In this situation, packets that are larger than 1496 bytes are dropped.

  Workaround: There is no workaround.

- CSCsg90190

  Symptoms: Without the enforcement of a voice daughterboard connector rating, the number of IP phones that can be powered up may exceed the number that the voice daughterboard can handle, that is, the available allocated inline power can exceed the VDB connector rating.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsg99914

  Symptoms: A SIP-200 may reset unexpectedly because of a keepalive failure when there is a lot of IPC backplane traffic and when Ethernet Out of Band Channel (EOBC) traffic drops occur because of a low queue size at the EOBC level.

  Conditions: This symptom is observed on a Cisco 7600 series that functions with a scaled configuration when a major and sudden topology change causes many IPC messages on the backplane.

  Workaround: There is no workaround.

- CSCsh01749

  Symptoms: The **mls qos marking ignore port-trust** command may not function.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch or Cisco 7600 series router that has a Supervisor Engine 32 or Supervisor Engine 720. When you enter the **mls qos marking ignore port-trust** command for an interface that is configured with several subinterfaces, each with a service policy, the service policies are supposed to match a unique ingress CoS value and change the corresponding egress MPLS EXP value for transfer across an MPLS cloud. However, after you have entered the **mls qos marking ignore port-trust** command, all egress EXP values show up as 0 because the command has no effect.

  Workaround: There is no workaround.

- CSCsh07037

  Symptoms: A “%SYS-2- CHUNKBADMAGIC” error mat occur on an OSM module and the module may restart.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when Weighted Random Early Detection (WRED) is configured with a maximum threshold of more than 2000 packets but without a queue limit.

  Workaround: Configure a proper queue limit for the class with the WRED configuration. For example, when the **random-detect precedence 3 32000 32000 1** command is configured, configure the queue limit by entering the **queue-limit 32768** command.

- CSCsh11498

  Symptoms: When you boot a switch or router with two SPA-IPSEC-2G SPAs in the same Services SPA Carrier (7600-SSC-400), one of the SPAs does not come up. When you attempt to boot the switch or router again, both SPAs come up properly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsh13947

  Symptoms: A router that is processing certain MPLS forwarding updates may crash or hang because of a software configuration mismatch.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB but may also occur in other releases. The symptom occurs when EoMPLS or AToM is configured with many virtual circuits (VCs) and when LDP sessions go down because of extreme traffic loads or clearing of the LDP neighbors, causing the forwarding information to be modified.

  Workaround: There is no workaround.

- CSCsh17979

  Symptoms: When inline power ports can not be powered on, a command may be rejected with the following error message:

  ```
  Command rejected: there's not enough system power to be allocated to Fa1/47, or the
  maximum power the backplane of this chassis can support has reached the limit.
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a module with a voice daughtercard.

  Workaround: There is no workaround.

- CSCsh20354

  Symptom 1: A third-party vendor VPN client may not be able to establish a VPN tunnel to a Cisco router. When you enable the **debug crypto isakmp** command on the Cisco router, the output shows the following:

  ```
  ISAKMP:(0:4:HW:2):No IP address pool defined for ISAKMP!
  ISAKMP:(0:4:HW:2):deleting SA reason "Fail to allocate ip address" state (R)
  CONF_ADDR     (peer x.x.x.x)
  ```

  Symptom 2: Although a third-party vendor VPN client can establish a VPN tunnel to a Cisco router, the client receives only an IP address but no DNS configuration, split-tunnel information, or other data during the mode configuration phase. In this situation, the debug output does not show any errors.

  Conditions: Both of these symptoms are observed only when a third-party vendor VPN client connects to a Cisco router that functions as a VPN server.

  Workaround: There are no workarounds.

- CSCsh22835

  Symptoms: After an RPR switchover occurs, a major error occurs on the newly active RP.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Reload the platform. If this not an option, there is no workaround.

- CSCsh23981

  Symptoms: During an HA switchover while IPC traffic is sent between the standby RP and standby SP, the newly active RP may crash.

  Conditions: This symptom is observed on Cisco Catalyst 6000 series switches and Cisco 7600 series routers. For Cisco Catalyst 6000 series switches, the symptom occurs in Release 12.2SX and Release 12.2SXF, in which ISSU is not supported. For Cisco 7600 series router, the symptom occurs in Release 12.2(33)SRB, in which ISSU is supported.

  Workaround: There is no workaround.

- CSCsh29863

  Symptoms: On an RPR switchover, the new active crashes during bootup diagnostics.

  Conditions: This symptom occurs when bad SFPs are plugged into the SFP- capable ports. Bad SFP means incompatible/unsupported/faulty SFP.

  Workaround: Remove incompatible/unsupported/faulty SFPs from the SFP port(s) and plug in a good one if needed.

- CSCsh31287

  Symptoms: The source MAC address for multicast on a tunnel that is accelerated by a crypto engine may remain zero.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an IPSec VPN Services Module (SPA-IPSEC-2G).

Workaround: There is no workaround.

- CSCsh31306

  Symptoms: Output drops occurs on a T1 serial interface. These drops are shown in the output of the **show interface serial** command but are not shown at the QoS level, that is, the output of the **show policy-map interface** command does not indicate any drops.

  When this situation occurs, the output of the **show controller** command for the serial interface at the VIP or FlexWAN level shows “pascb.tx_polling_high” with any value other than 2.

  Conditions: The symptoms is observed on a Cisco 7500 series (with a VIP) and Cisco 7600 series (with a FlexWAN module) that have a serial interface that is configured for fair-queueing.

  Workaround: Remove and then reconfigure fair-queueing so that “pascb.tx_polling_high” is set to the correct value of 2.

- CSCsh33770

  Symptoms: An IPSec VPN SPA (SPA-IPSEC-2G) may not come up during the boot process, that is, it remains in the “Initializing” state. The output of the **show crypto eli** command shows the following information:

  ```
  Hardware Encryption : INACTIVE
  Number of hardware crypto engines = 1
  CryptoEngine SPA-IPSEC-2G[6/0] details: state = Initializing
  Capability      :
  IPSEC: DES, 3DES, AES, RSA
  IKE-Session   :     0 active, 16383 max, 0 failed
  DH            :     0 active,  9999 max, 0 failed
  IPSec-Session  :      0 active, 65534 max, 0 failed
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that run Cisco IOS Release 12.2SRA.

  Workaround: There is no workaround.

- CSCsh51688

  Symptoms: A Cisco 7600 series may crash unexpectedly because of a bus error on the Switch Processor (SP). The following error message may be generated prior to the crash:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x40B450D4
  ```

  Conditions: This symptom is observed on a Cisco 7600 series and the trigger is currently not known.

  Workaround: There is no workaround.

- CSCsh54325

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: When frames require PXF punting to the RP (or SP), PPP LCP frames may not be forwarded to the RP (or SP), causing link negotiation to fail. Or, HDLC keepalives may not be forwarded to the RP (or SP), causing the link to remain down.

  Condition 1: These symptoms are observed on a Cisco Catalyst 6503, Cisco Catalyst 6503-E, and Cisco 7604 that are configured with a SIP-600 in which a POS SPA is installed and occurs when the supervisor engine resides in slot 1 or slot 2 of the chassis.

  Workaround 1: There is no workaround.

  Symptom 2: When frames require PXF punting to the RP (or SP), CFM PDUs may not be properly forwarded to the RP (or RP).

Condition 2: This symptom is observed on a Cisco 7604 that is configured with a SIP-600 or Ethernet Services line card (ES20) and occurs when the supervisor engine resides in slot 1 or slot 2 of the chassis.

Workaround 2: There is no workaround.

- CSCsh56121

  Symptoms: After you have reloaded a Cisco 7600 series that has redundant supervisor engines, or after you have forced a redundancy switchover, the RSA key on the standby supervisor engine may be lost.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the RSA key.

- CSCsh61946

  Symptoms: After an SSO switchover has occurred, the second of two 6000 W DC power supplies in the chassis is shut down.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 router when both power supplies are powered on before the SSO switchover occurs.

  Workaround: There is no workaround.

- CSCsh65322

  Symptoms: A Cisco 7600 series with an Enhanced FlexWAN in which a PA-A3-OC3SMI port adapter is installed may drop packets steadily from the ATM interface. This situation may be verified under the “Total output drops” in the output of the **show interfaces atm** command.

  Conditions: This symptom is observed when the router is configured for PPPoA connections. There is no correlation between the packet drops on the interface and any particular ATM PVCs or virtual-access interfaces. The symptom may also occur on other platforms that are configured with a PA-A3-OC3SMI port adapter.

  Workaround: There is no workaround.

  Further Problem Description: note that the symptom does not occur with a FlexWAN.

- CSCsh76923

  Symptoms: A Cisco Catalyst 6500 series switch may crash because of memory corruption or a bus error.

  Conditions: This symptom is observed when NAT is configured. The symptom may also affect a Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsh83559

  Symptoms: A Cisco Catalyst 6000 series switch may leak memory in the IP Input task in the Cisco IOS-BASE process. The memory is leaked in a small amount per packet that is process switched over a VRF on the switch. Non-VRF traffic is not affected.

  Conditions: This symptom is seen on a Cisco Catalyst 6000 series switch that is running Cisco IOS Modularity. This can only happen if there are VRFs configured on the switch.

  Workaround: Do not use VRFs.

- CSCsh94940

  Symptoms: An active supervisor engine may crash because of memory corruption in the SP processor pool, and the following error message may be generated:

  ```
  %SYS-SP-3-BADFREEMAGIC: Corrupt free block at [...] (magic [...])
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 32 when a periodic SNMP query is made to the L2 MAC table. Because of a race condition, freed memory may be written by another thread, causing memory corruption.

  Note that the symptom does not occur with a Supervisor Engine 1 and Supervisor Engine 2.

  Workaround: Disable the SNMP query to the L2 MAC table.

- CSCsi01151

  Symptoms: When IPSec SA rekeys, an SPI deletion error may occur, causing one peer to use the outbound SA that has been deleted by the other peer.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with an IPSec VPN Services Module (SPA-IPSEC-2G). The symptom occurs when both the Cisco platform and its peer rekey at the same time, preventing the Cisco platform from deleting the old SPI, causing multiple SPIs to be generated on the Cisco platform, and causing the Cisco platform to use the wrong SPI to encrypt the packets.

  Workaround: Clear the tunnel.

- CSCsi01422

  Symptoms: Frame Relay traffic shaping in a configuration with a child policy and hierarchical QoS does not function. Traffic does not respond to BECN or FECN marking.

  Conditions: This symptom is observed on a Cisco 7600 series when a service policy is configured under a Frame Relay map class. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsi02033

  Symptoms: On a PE router, a subinterface on which an EoMPLS VC is configured may stop forwarding traffic from the backbone to a CE router. Traffic that is sent from the PE router to the CE router goes through fine. Traffic forwarding from the backbone is affected.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA3 or an earlier release and that functions as a PE router. The symptom occurs when you configure a new subinterface and an IP address on a Gigabit Ethernet (GE) interface that is installed in a SIP-400 and that connects to a remote CE router. In this situation, another subinterface (on the same GE interface) that is configured for EoMPLS no longer functions for traffic that is forwarded from the backbone to the CE router.

  Workaround: Remove and reconfigure Xconnect on the affected subinterface.

  Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the physical interface on which the affected subinterface is configured.

- CSCsi02778

  Symptoms: When the MPLS Traffic Engineering (TE)-Fast Reroute (FRR) Link and Node Protection feature is enabled, VPLS traffic does not flow from end-to-end after it has been rerouted to single-hop backup tunnel.

Conditions: This symptom is observed on a Cisco 7600 series when the primary tunnel is a multihop tunnel with implicit-null as the next-hop label and when the backup tunnel is single-hop tunnel. After traffic has been rerouted to the backup tunnel, VCs do come up and the egress path for VPLS VCs is shown correctly as the backup tunnel. However, the traffic does not reach the egress PE router.

Workaround: There is no workaround.

Further Problem Description: From the egress line card, enter the following **show** commands to collect information to further debug this issue:

- Enter the **show platform atom ether-vc** command to identify the egress index of the VPLS VC.
- Enter the **show platform mpls imposition-table details** command to look at the egress information.

After traffic has been rerouted to the backup tunnel, the egress label operation is incorrectly programmed to forward the original primary TE label on the label stack.

- CSCsi06759

  Symptoms: When you run the **snmpwalk** command, the ifIndex for the subinterfaces of a SIP-200 is not retrieved although the output of a **show** command does show the ifIndex. When you run the **snmpwalk** command, the following error message and a possible traceback are generated:

  ```
  %SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe regn with SNMP IM by driver having ifIndex
  <index> and ifDescr <description>
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router after you have replaced a FlexWAN module with a SIP-200.

  Workaround: There is no workaround.

- CSCsi10219

  Symptoms: A SIP-200 may crash, and a SIP heartbeat failure message may be generated on the console of the RP.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-200 that is configured for hardware-based MLP and cRTP and in which a SPA-8XCHT1/E1, SPA-1XCHSTM1/OC3, SPA-2XCT3/DS0, or SPA-4XCT3/DS0 is installed. The symptom occurs when RTP traffic is processed on the MLP bundle.

  Workaround: Do not configure hardware-based MLP. Rather, when cRTP is required, configure software-based MLP.

- CSCsi14145

  Symptoms: The runt counter is updated with runt frames with CRC errors while runt frames with proper CRCs are ignored.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when packets with a size smaller than 64 bytes are received. The output of the **show interface** command accounts only for packets as runt frames that are smaller than 64 bytes and that have CRC errors. Thus, statistics are lost.

  Workaround: There is no workaround.

  Further Problem Description: According to the 802.3 specifics and information on the IEEE website, the definition of runt frames is:

  Runts: Frames that are smaller than the minimum frame size for IEEE-802.3 standard frames. Runt frames typically are caused by collision fragments and are propagated through the network. If the number of runt frames exceeds the number of collisions, there is a problem with a transmitting device.

- CSCsi71285

  Symptoms: SNMP walk of VLAN statistics or executing the **show vlan counters** CLI command causes indefinite console wait or CPUHOG.

  Conditions: This defect is seen only in Cisco IOS Release 12.2SRA images.

  Workaround: VLAN statistics are collected from cached entries instead of collecting real time statistics, which was causing indefinite wait on IPC calls.

  Further Problem Description: Both SNMP queries and CLI commands will block while retrieving nonrouted VLAN counters. An SNMP query on any of the ifTable counters for a nonrouted VLAN interface will block the SNMP Agent indefinitely. This causes the SNMP AGENT queue to fill up and start dropping SNMP packets. This problem in turn prevents the Network Management application from accessing any other MIB objects not related to the nonrouted VLANs. Restarting the SNMP agent clears the thread, but as soon as another objects related to nonrouted VLAN is accessed, the SNMP agent will block again.

- CSCuk61773

  Symptoms: CPU spikes may occur on a router that is configured for Web Cache Communication Protocol (WCCP) earlier than Release 4.0.7.

  Conditions: This symptom is observed on a Cisco 7600 series when WCCP is in communication with a Cisco Wide Area Application Services (WAAS) appliance. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCek12203

  Symptoms: When you enter the **copy ftp disk** command, the copy operation may fail and cannot be terminated, further **copy** commands may fail, and a TCP vty session for the purpose of troubleshooting the situation may fail and cannot be terminated.

  Conditions: These symptoms are observed on a Cisco platform when the FIN flag is set in the initial ESTAB message from a neighbor. You must reload the router to recover from the symptoms.

  Workaround: Do not enter the **copy ftp disk** command. Rather, enter the **copy tftp disk** command.

- CSCsg39837

  Symptoms: HTTP errors may occur while accessing a Win2003 Web Server.

  Conditions: This symptom is observed on a voice gateway that runs Cisco IOS Release 12.4(6)T when a Win2003 HTTP web server is accessed under a heavy load and when the voice gateway has the **ip http client connection persistent** command disabled. Note that the symptom may also affect other releases.

  Workaround: There are two possible workarounds:

  1. Switch to a Win2000 HTTP web server.
  2. On a Win2003 server, set “TcpTimedWaitDelay” to the minimum (30 seconds). This does not totally eliminate but will reduce the occurrences of dropped TCP SYN requests from the Cisco IOS router.

Wide-Area Networking

- CSCek49202

  Symptoms: When an attempt to move an interface from one multilink group to another fails because of platform-specific limitations, the interface is left in an invalid state. The **multilink-group** command still appears in the interface configuration, but the interface does not appear in the output of **show ppp multilink** command.

  Conditions: This symptom may occur on platforms that support distributed implementations of multilink (such as the Cisco 7500 series, Cisco 7600 series, Cisco 10000 series, and Cisco 12000 series routers) when the platform does not allow the interface to be added to a multilink group for some reason, for example, because of resource constraints.

  Workaround: Enter the **no multilink-group** command to remove the interface from its current multilink group before adding it to a new one.

- CSCsd72854

  Symptoms: When IS-IS is configured on an MLP interface of a 6-port channelized T3 Engine 0 line card, the line card may fail to come up because PPP fails to negotiate OSICP on the MLP interface.

  Conditions: This symptom is observed on a Cisco 12000 series router after you have reloaded the router. Note that the symptom may also occur on other platforms and in other releases.

  Workaround: Increase the PPP timeout retry interval to 10 seconds by entering the **ppp timeout retry 10** command on the interface. (The default timeout retry interval is 2 seconds).

Resolved Caveats—Cisco IOS Release 12.2(33)SRA3

Cisco IOS Release 12.2(33)SRA3 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA3 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsb89847

  Symptoms: Source and destination Border Gateway Protocol (BGP) autonomous system (AS) information may not be properly updated.

  Conditions: This symptom is observed on a Cisco router that is configured for MSDP and NetFlow.

  Workaround: There is no workaround.

- CSCse08044

  Symptoms: A Cisco router may generate export packets in which the first flow record contains incorrect data such as incorrect IP addresses.

  Conditions: This symptom is observed on a Cisco router that is configured for NetFlow and NetFlow Data Export.

  Workaround: Disable NetFlow.

- 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. Is this not an option, there is no workaround.

Interfaces and Bridging

- CSCek43732

  Symptoms: All packets are dropped from a 1-port OC-3/STM-1 POS port adapter (PA-POS-1OC3) or 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) that is configured for CBWFQ.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1. However, the symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsd40136

  Symptoms: POS interfaces may remain in the up/down state after the router is upgraded to another Cisco IOS software image.

  Conditions: This symptom has been observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router but may also affect other platforms such as the Cisco 7500 series router.

  Workaround: Reload the FlexWAN or VIP in which the POS port adapter is installed.

IP Routing Protocols

- CSCsd15749

  Symptoms: Prefixes that are tagged with Site of Origin (SoO) values may not be filtered at the border.

  Conditions: This symptom is observed when SoO values are configured for a peer group. The peer group members may not correctly filter the prefixes that are based on the SoO value at the border.

  Workaround: BGP supports Dynamic Update peer groups, which ensure that packing is as efficient as possible for all neighbors regardless of whether or not they are peer-group members.

  Peer groups simplify configurations, but peer-templates provide a much more flexible solution to simplify the configuration than peer groups.

  If the SoO configuration is applied directly to the neighbor or to a template, the symptom does not occur. Using templates to simplify the configuration is a better solution and Dynamic Update peer groups ensure efficiency.

- CSCsd73245

  Symptoms: Many “IPRT-3-PATHIDX” error messages are generated by the “BGP Router” process when you increase the prefixes in a VRF.

  Conditions: This symptom is observed on a Cisco router that is configured for loadbalancing and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

- CSCsf20947

  Symptoms: A default route that is defined by the **neighbor default-originate** command may be ignored by the BGP neighbor.

  Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the default route to be relearned.

Workaround: Manually clear the BGP neighbor to enable the router to correctly relearn the default route.

- CSCsh61119

  Symptoms: ARP may be refreshed excessively on the default interface, causing high CPU usage in the "Collection Process."

  Conditions: This symptom is observed on a Cisco router that has point-to-point interfaces that have non-/32 interface addresses or secondary addresses and that constantly come up or go down.

  Workaround: There is no workaround.

ISO CLNS

- CSCse40346

  Symptoms: Tracebacks may be generated when you configure IS-IS and LDP features, for example, when you enter the **no ip router isis** *area-tag* command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)SY but may also occur in other releases.

  Workaround: There is no workaround.

Miscellaneous

- CSCed36177

  Symptoms: A software-forced crash may occur on the RP in a Cisco Catalyst 6500 series switch or Cisco 7600 series router.

  Conditions: This symptom is observed only with a tunnel configuration and may occur with either crypto or non-crypto images.

  Workaround: There is no workaround.

- CSCek42751

  Symptoms: The running configuration may not be accessible after you have copied a small file to the running configuration.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system after you have rebooted the router.

  Workaround: Reboot the router once more.

- CSCek47814

  Symptoms: A ping between two CE routers may fail after you have reloaded the CE router on the Ethernet side.

  Conditions: This symptom is observed in an AToM configuration when one CE router is configured for PPP and the other CE router is configured for Ethernet. The symptom occurs because of a MAC address learning failure.

  Workaround: Reconfigure VLAN over MPLS on the corresponding Ethernet interface of the adjacent PE router.

- CSCek60775

  Symptoms: A router that has Virtual Tunnel Interfaces (VTIs) may crash.

Conditions: This symptom is observed when two VTIs are configured with the same IP address and when the inside VRF (IVRF) of one VTI is the same as the Front Door VRF (FVRF) for the other VTI.

Workaround: There is no workaround. The configuration that is stated in the Conditions is not considered a valid configuration.

- CSCek61974

  Symptoms: You may be able to configure a minimum receive interval as short as 1 ms, which may cause problems on the router.

  Conditions: This symptom is observed on a Cisco router that supports Bidirectional Forwarding Detection (BFD). Note that a minimum receive interval shorter than 50 ms is not supported in Cisco IOS software images.

  Workaround: Configure a minimum receive interval of 50 ms or longer.

- CSCek65022

  Symptoms: A 7600-SSC-400 may crash on bootup.

  Conditions: This symptom is observed when the Cisco IPsec VPN Shared Port Adapter (SPA-IPSEC-2G) is booting up.

  Workaround: There is no workaround.

- CSCek66294

  Symptoms: TCP MSS adjusts feature works only on the ingress direction. The feature should work on both ingress and egress directions.

  Conditions: This symptom has been observed when the TCP MSS adjusts feature is configured.

  Workaround: There is no workaround.

- CSCek68218

  Symptoms: A SIP-600 may crash when the **diagnostic bootup level** command is enabled.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SIP-600 in which a 16-port Gigabit Ethernet GBIC (WS-X6516-GBIC) is installed.

  Workaround: Bypass the diagnostic test by entering the **no diagnostic bootup level** command.

- CSCin74155

  Symptoms: A router that functions under a heavy load with SSHv2 clients may crash if any of the SSH clients are terminated.

  Conditions: This symptom is observed when the following conditions are present:

  – The CPU utilization above 70 percent.

  – There are continuous sweep pings from two far-end routers that have the **debug ip packet** command enabled to create continuous logs for the SSH clients.

  – The **no logging console** command is configured.

  – A connection is made from a couple of SSHv2 clients, you enable the **terminal monitor** command, and you terminate the SSHv2 clients while continuous messages are being generated.

  – The TCP window size is reduced.

  Workaround: Avoid using SSHv2 when the router is very stressed.

- CSCsb89043

  Symptoms: The following error message and traceback are generated when an RP switchover occurs:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x603D9154 reading 0x4C
  -Traceback= 603D9154 603DA078 603DA0C0 603DA65C 603DA740 603DA8AC 603DA9AC 603C92F4
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for HA.

  Workaround: There is no workaround. However, the symptoms do not affect the performance of the router or the processing of traffic.

- CSCsc60249

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)

  – Media Gateway Control Protocol (MGCP)

  – Signaling protocols H.323, H.254

  – Real-time Transport Protocol (RTP)

  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

  Workaround: There is no workaround.

- CSCsd29469

  Symptoms: SNMP polls hang at a specific point, after which there is no response for a long time. Then, SNMP polling works fine for a while until it hangs again at a specific point.

  When SNMP becomes unresponsive, the following error message may be generated, and SNMP queries may time-out at the application:

  ```
  %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
  ```

  Conditions: These symptoms are observed under the following conditions:

  – After a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF2 have been polled for a while.

  – After the CISCO-ENHANCED-MEMORY-POOL-MIB is polled on a Cisco 7600 series router that has a Supervisor Engine 720 that runs Cisco IOS Release 12.2(33)SRA.

Workaround: Exclude the CISCO-ENHANCED-MEMORY-POOL-MIB from the SNMP view. Enter the following commands to exclude the CISCO-ENHANCED-MEMORY-POOL-MIB:

```
snmp-server view public-view iso included
snmp-server view public-view ciscoMemoryPoolMIB excluded
snmp-server view public-view ciscoEnhancedMemPoolMIB excluded
snmp-server community public view public-view RO
```

This view should be applied to all community strings that might be used to poll these MIB modules. If views are already applied to a community string then the one above and the existing view should be merged.

If SNMPv3 is in use then this view should be applied to any SNMPv3 groups configured as well.

There is no need to reboot the platform. The symptom should resolve itself within a few minutes. If you must immediately clear the symptom, enter the following two commands (use one of the SNMP server community string commands that are actually configured on the router instead of the ones that are mentioned in the example below, which are based on the information that is presented above):

Disable SNMP and stop the processes:

```
no snmp-server
```

Re-enable SNMP and restore the SNMP configuration:

```
snmp-server community public view public-view RO
```

Further Problem Description: When you enable the **debug snmp packet** command, you can see that the SNMP poll requests are not being acknowledged. However, the output of the **show snmp counters** command shows about the same number of SNMP requests as the number of outputs, even though these outputs were never processed and sent.

- CSCsd40211

  Symptoms: After you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface, ARP may be delayed. After 5 to 30 minutes, ARP finally appears for the interface in the MAC address table of the switch processor.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXD4 or Release 12.2(18)SXE4 and that is configured for NetFlow. The symptom may also affect other releases such as Release 12.2SR.

  Workaround: There is no workaround.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  – Cisco IOS, documented as Cisco bug ID CSCsd85587

  – Cisco IOS XR, documented as Cisco bug ID CSCsg41084

  – Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999

- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM)

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

- CSCse09498

  Symptoms: When you enter the **no shutdown** interface configuration command on an auto-template interface during deployment, some tunnels may be in the up/down state, and the tunnel mode may be GRE instead of the configured tunnel mode of MPLS.

  Conditions: This symptom is observed on a Cisco router with about 70 primary MPLS TE tunnels. The symptom occurs when you first enter the **no interface auto-template** command, then you enter the **tunnel mode mpls traffic-eng** command, and finally you paste the template back.

  Workaround: Reload the router.

  Alternate Workaround: Create an automesh in the following sequence:

```
conf t
access-list 60 permit 10.0.7.3
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12

interface Auto-Template1
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination access-list 60
tunnel mode mpls traffic-eng

........
access-list 60 permit 10.0.7.3
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12
```

- CSCse11794

  Symptoms: A SIP-200 or SIP-400 may crash when you configure 12,000 bridged VCs along with a service policy on an ATM SPA that is installed in the SIP.

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

Workaround: There is no workaround. To prevent the symptom from occurring, do not configure more than 1000 bridged VCs when there is also a service policy.

- CSCse17175

  Symptoms: The line protocol may go down on some of the serial interfaces of a 1-port multichannel STM-1 single mode port adapter.

  Conditions: This symptom is observed on a Cisco router when the maximum number of channel groups (256) is configured on the port adapter.

  Workaround: There is no workaround.

- CSCse26682

  Symptoms: When you enter the **no ipv6 unicast-routing** command followed by the **ipv6 unicast-routing** command, prefixes may be missing from the IPv6 CEF table on a line card. This situation may cause traffic loss.

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

  Workaround: Although you can enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command for every interface that is configured for IPv6, doing so is inefficient. It is more efficient and less disruptive to enter the **clear cef table ipv6** command.

- CSCse68138

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  – Session Initiation Protocol (SIP)

  – Media Gateway Control Protocol (MGCP)

  – Signaling protocols H.323, H.254

  – Real-time Transport Protocol (RTP)

  – Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCse83031

  Symptoms: A memory leak may occur when you remove an Xconnect configuration from a router, which can be verified by enabling the **show memory debug** command.

  Conditions: This symptom is observed when you configure Xconnect with the Exchange Fabric Protocol (EFP) and then remove the Xconnect configuration.

  Workaround: There is no workaround.

- CSCse84226

  Symptoms: When a VC is down, the output of the **show connection** command on the local side shows that the VC is up, even though the output of the **show mpls l2 vc detail** command shows that the VC is down. The output of the **show connection** command on the remote side shows that the VC is down.

  Conditions: This symptom is observed on a Cisco router that is configured for AToM when the MTU mismatches the Virtual Private Wire Service (VPWS) circuit.

  Workaround: There is no workaround.

- CSCse90586

  Symptoms: A Cisco 7600 series that has a large number of OSPF tunnels with VRFs may run out of memory, many MALLOC failures may occur, and the router may reload because of a "Corrupted Program Counter" error. The crash traceback that is generated is invalid.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA, that is configured for OSPF, and that has 500 tunnels with a VRF configuration.

  Workaround: Reduce the number of tunnels and VRFs in the configuration.

- CSCsf19418

  Symptoms: A router may reload unexpectedly when you enter the **show mpls ldp graceful-restart** command.

  Conditions: This symptom is observed when either of the following conditions are present:

  – When the command output has a "Down Neighbor Database" entry that expires by reaching the reconnect timeout limit while the command output is generating the neighbor address list.

  – When the command output is paged at the "--More--" string within the context of displaying addresses.

  Workaround: Do not enter the **show mpls ldp graceful-restart** command when a graceful-restart database entry is about to expire. When the command output is paged at the "--More--" string within the context of displaying addresses and when the Down Neighbor Database entry may have expired, type the letter "Q" to abort any further output of addresses.

- CSCsg02554

  Symptoms: On a Cisco Catalyst 6500 series or Cisco 7600 series router that has two Optical Services Modules (OSMs) that are configured for APS, a switchover to the protect channel may result in a 30-second traffic loss.

  Conditions: This symptom is observed when the L2 protocol is configured for Frame Relay.

  Workaround: Disable keepalive on the Frame Relay link, or lower the keepalive interval.

- CSCsg29498

  Symptoms: A router may reload when you enter the **show monitor event-trace adjacency all** command.

  Conditions: This symptom is observed when you enter the command after a route to a destination changes from multiple paths to a single path.

  Workaround: There is no workaround.

- CSCsg37435

  Symptoms: The output of the **show snmp mib ifmib ifindex** command does not show the SNMP Interface Index identification numbers (ifIndex values) for 802.1Q VLAN subinterfaces.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router after you have performed an OIR of a Gigabit Ethernet module.

Workaround: Reload the platform.

- CSCsg44555

  Symptoms: An MPLS TE tunnel with a third-party vendor headend, a Cisco midpoint, and a Cisco tailend may occasionally transition to the up/down state on the midpoint while still appearing in the up/up state on the headend and tailend. When this situation occurs, traffic may continue to flow on the tunnel even though the tunnel is in the up/down state at the midpoint or it may come to a halt.

  Conditions: This symptom is observed when the Cisco router that is the tailend for the MPLS TE tunnel uses a bandwidth or burst size that is not a multiple of 1 Kbps or 1 Kbyte and that rounds up the Resv burst size to the next higher multiple of 1 Kbps or 1 Kbyte.

  Workaround: Specify a tunnel bandwidth that is a multiple of 8 Kbps.

- CSCsg58587

  Symptoms: The “ifHCOutUcastPkts” SNMP output counters for VLANs are incorrect because they count the data twice:

  ```
  interfaces.ifTable.ifEntry.ifOutUcastPkts.xxx : Counter: <=== counted twice
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutUcastPkts.xxx : Counter64: <=== counted twice
  ```

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

  Workaround: There is no workaround.

  Further Problem Description: Note that the “ifHCInUcastPkts” SNMP input counters function fine and provide correct data.

- CSCsg68740

  Symptoms: Fast Reroute (FRR) is not triggered when a cable is removed from a POS SPA or POS OSM, causing data loss of 3 to 4 seconds.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

  Further Problem Description: This symptom does not occur when a POS port adapter is installed in an Enhanced FlexWAN module.

- CSCsg68783

  Symptoms: The ATM SAR may hang on an ATM interface that is configured for AToM.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when you enter the **clear mpls traffic-eng auto-tunnel mesh** command.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ATM interface.

  Further Problem Description: The symptom occurs because the ATM SAR receives a packet that is larger than the ATM cell size in the AToM mode of operation.

- CSCsg98612

  Symptoms: The **speed nonegotiate** command does not function for Gigabit Ethernet ports on a SIP-600.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2 or Release 12.2(33)SRB.

Workaround: There is no workaround.

- CSCsh42857

  Symptoms: After TE tunnel reoptimization, the AToM traffic is not passing anymore due to a stale outgoing label and interface in the hardware.

  Conditions: This symptom has been observed with AToM circuits going over a TE tunnel.

  Workaround: Enter the **shutdown** command and the **no shutdown** command on the CE facing interface or configure and deconfigure the **xconnect** command on the CE facing interface will reestablish the traffic forwarding until a new reoptimization occurs.

TCP/IP Host-Mode Services

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

  Conditions: This symptom is seen under the following conditions:

  – The router must have RCP enabled.

  – The packet must come from the source address of the designated system configured to send RCP packets to the router.

  – The packet must have a specific data content.

  Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

- CSCsf33034

  Symptoms: The following error message and tracebacks are generated during the boot process:

```
%TCP-2-INVALIDTCB: Invalid TCB pointer: 0x4704D088
 -Process= "IP Input", ipl= 0, pid= 122
 -Traceback= 409F00FC 409E4C50 407A032C 407D8EAC 4077FF38 407911D0 4078EC2C 4078EDE8
4078F004
```

  Conditions: This symptom is observed on a Cisco platform when a TCP server is configured.

  Workaround: There is no workaround.

  Further Problem Description: A TCP control block that is already freed is referenced or accessed, causing the error message to be generated. This situation does not affect the proper functioning of the platform in any way.

Wide-Area Networking

- CSCek45604

  Symptoms: An OSM or FlexWAN module may crash when you apply an input QoS configuration to a Frame Relay interface in a particular sequence.

  Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

  1. You attach a policy to the main interface and you use the map class for inheritance.
  2. You remove the Frame Relay class from the interface and attach a flat policy to the main interface.

  Note that the symptom does not occur when you apply an output QoS configuration to a Frame Relay interface.

Workaround: Do not apply an input QoS configuration to a Frame Relay interface.

- CSCsg35429

  Symptoms: Spurious access messages may be generated when you enter the **mpls bgp forwarding** command on a multilink interface.

  Conditions: This symptom is observed on a Cisco router that is configured for PPP.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA2

Cisco IOS Release 12.2(33)SRA2 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA2 but may be open in previous Cisco IOS releases.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

IP Routing Protocols

- CSCsa87034

  Symptoms: When you attempt to clear the routing table, the neighbor is brought down instead.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 unicast *** or **clear bgp ipv6 unicast *** command, causing respectively the IPv4 neighbor or IPv6 neighbor to be brought down.

  Workaround: There is no workaround.

- CSCsb86987

  Symptoms: A Cisco router may generate tracebacks or may crash when multicast performs an RPF lookup into the BGP table.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and multicast.

  Workaround: There is no workaround.

- CSCse04220

  Symptoms: The BGP table version remains stuck at 1, and the router may crash.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 uni *** command for IPv4 or the **clear bgp ipv6 uni *** command for IPv6. The symptom may also occur when you enter the **clear bgp nsap uni *** command for a network service access point (NSAP) address family.

  Workaround: Enter the **clear ip bgp *** command to clear the sessions, purge the BGP table, and prevent the router from crashing.

Miscellaneous

- CSCek37222

  Symptoms: Packets are not classified when a service policy is configured with random-detect in the class default.

  Conditions: This symptom is observed on a Cisco 7600 series when the service policy is attached to a Frame Relay interface on an OSM-CT3 line card or OSM-8OC3-POS module. Note that the symptom does not occur when the service policy is attached to a Frame Relay PVC.

  Workaround: There is no workaround.

- CSCek47059

  Symptoms: IPv6 packets may be accounted as MPLS packets in the output of the **show interface accounting** command.

  Conditions: This symptom is observed on a Cisco 7600 series when IPv6 addresses are configured on interfaces of an Optical Services Module (OSM) and when IPv6 traffic or a ping is processed.

  Workaround: There is no workaround.

- CSCek47506

  Symptoms: NetFlow Data Export (NDE) stops functioning unexpectedly, a memory allocation failure (MALLOCFAIL) occurs, hardware-switching becomes disabled, and, finally, the Distributed Forwarding Card (DFC) is reset.

  When an SSO switchover occurs and when the DFC has a high NetFlow TCAM utilization, the DFC stops functioning immediately and is eventually reset.

  Conditions: These symptoms are observed on a Cisco 7600 series when NDE is enabled, especially NDE version 8 or NDE version 9.

  Workaround: There is no workaround.

  Further Problem Description: When NDE stops functioning, the export packets continue to be generated and are queued, waiting to be sent. These packets use up the memory and cause the DFC to run out of memory because the memory pool becomes too fragmented.

- CSCek50720

  Symptoms: A router does not report the cause of an error when an ATM SPA does not boot because of a delay-locked loops (DLL) centering failure during SAR initialization.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXF and that has an ATM SPA that is installed in a SIP-400. The symptom may also affect other releases.

  Workaround: There is no workaround.

- CSCek52892

  Symptoms: An enhanced FlexWAN module or other line card may crash.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for MPLS and OAM.

  Workaround: There is no workaround.

- CSCek54572

  Symptoms: A switch or router may crash when you configure and unconfigure 500 IPSec VTI tunnels two or three times. The symptom does not occur when you configure and unconfigure the tunnels only once.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series.

Workaround: After you have configured the tunnels, wait for the tunnels to come up before you unconfigure the tunnels.

- CSCsb40304

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  – Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  – Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  – Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd43211

  Symptoms: A SIP-200 may crash when it has a channelized SPA that has a multilink bundle, an LFI configuration, and more than two links in the bundle.

  Conditions: This symptom is observed on a Cisco 7600 series when an SSO or RPR+ switchover occurs while traffic is processed near the line rate, that is, at about 75 percent of the line rate.

  Workaround: There is no workaround.

- CSCsd75273

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  – Processing ClientHello messages, documented as Cisco bug ID CSCsb12598

  – Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304

  – Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCse03277

  Symptoms: When a tunnel is removed and reconfigured, the tunnel interface may not come up.

  Conditions: This symptom is observed on a Cisco router that has a tunnel that is configured on a Virtual Tunnel Interface (VTI).

  Workaround: Shut down the tunnel before you unconfigure the IP address of the tunnel interface, disable the VTI tunnel mode, or remove the VTI tunnel itself.

- CSCse12195

  Symptoms: Connected ports on a Cisco Catalyst 6000 series or Cisco 7600 series may transition from the up state to the down state with no apparent cause.

  Conditions: This symptom is observed on a 16-port Gigabit Ethernet GBIC line card (WS-X6816-GBIC) when the following two conditions are met:

  – A 1000Base-T GBIC is inserted after the WS-X6816-GBIC has been powered up.

  – Port 1 is enabled, not connected, and set to auto-negotiate.

  Workaround: Disable auto-negotiation on port 1 by entering the **speed nonegotiate** command.

  First Alternate Workaround: Remove all 1000Base-T GBICs that are in use, reset the WS-X6816-GBIC, and refrain from using 1000Base-T GBICs.

  Second Alternate Workaround: Disable port 1.

- CSCse22153

  Symptoms: The following error messages may be generated on the console of the standby RP when MPLS TE tunnels are deleted and then added while the standby RP reloads.

  ```
  %IDBINDEX_SYNC-STDBY-3-IDBINDEX_ENTRY_LOOKUP: Cannot find IDB index table
  entry: "", 0
  ```

  ```
  %COMMON_FIB-STDBY-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface for Tunnel5
  with illegal if_number: -1
  ```

  Conditions: This symptom is observed in an MPLS network that has multiple TE tunnels.

  Workaround: Do not delete and add MPLS TE tunnels while the standby RP reloads.

- CSCse41480

  Symptoms: The CoS VLAN priority may be changed and become corrupted when MPLS packets are sent over an EoMPLS tunnel on Cisco 7600 series even when the **mls qos trust cos** command is enabled on the ingress interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXE2 or Release 12.2(18)SXF4 but may also affect other releases that run on the Cisco 7600 series. The symptom occurs only when packets with Ethertype 8847 and 8848 are processed on the ingress interface, causing an incorrect MPLS EXP bit to be assigned on the ingress interface.

  Note that the symptom does not occur when the payload is IP (Ethertype 0800) or any other Ethertype.

  Workaround: There is no workaround. (However, see the Further Problem Description.)

  Further Problem Description: The fix for this caveat does not resolve the underlying hardware issue but, as a workaround, it does allow you to configure an ingress marking policy on the EoMPLS interface, to match on the incoming MPLS EXP bit values (that is, value 0 through 7), and to set the marking to the same value.

- CSCse52951

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

- CSCse59865

  Symptoms: The “ifDescr” for dot1q encapsulation on the interface of a 1-port 10 Gigabit Ethernet SPA may be truncated and may cause the “ifDescr” to be incorrect or the router to crash.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SRA.

  Workaround: There is no workaround.

- CSCse62462

  Symptoms: When a GRE tunnel is routed over an MPLS cloud, process-switched packets that are destined for the remote end of the GRE tunnel are sent unlabeled.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S when the router functions as a PE router that has a GRE tunnel configured within a VRF that is sourced from another VRF.

Workaround: There is no workaround.

- CSCse67650

  Symptoms: Non-IP packets may be dropped from an egress interface when a QoS service policy with WRED is applied. Dropped packets may include ARP and MPLS LDP packets. If the router is booted with this configuration, the router may be unable to perform L2 address resolution for IP and fail to establish MPLS neighbor relationships.

  Conditions: This symptom is observed on a Cisco 7600 series when a QoS service policy with WRED is applied to an interface on a SIP-600.

  Workaround: Remove WRED from any QoS policies that are applied on SIP-600 interfaces.

- CSCse74713

  Symptoms: Pings may fail across a link on an ATM SPA that is configured for MLP, LFI, and VRF forwarding and that is installed in a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: Reload the router and reapply the VRF configuration to the virtual template.

  Further Problem Description: The symptom does not occur in Release 12.2.18SXF4 and earlier releases.

- CSCse75429

  Symptoms: An LDP neighbor does not come up when the MPLS LDP Graceful Restart feature is enabled.

  Conditions: This symptom is observed when the forwarding state holding timer of the MPLS LDP Graceful Restart feature is configured to a value that is less than 120 seconds, causing the LDP session to be brought down.

  Workaround: Configure the forwarding state holding timer to a value that is greater than or equal to 120 seconds.

- CSCse77427

  Symptoms: The throughput performance may be adversely affected on a Cisco 7600 series that has a SIP-600 in which a 1-port 10 Gigabit Ethernet SPA or 10-port Gigabit Ethernet SPA is installed that is configured for Hierarchical Virtual Private LAN Service (H-VPLS) with traffic engineering (TE) tunnels.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when the 1-port 10 Gigabit Ethernet SPA or 10-port Gigabit Ethernet SPA processes incoming packets at 50 percent of the line rate and has the TE tunnels disabled after they were previously enabled for the incoming traffic.

  Workaround: There is no workaround.

- CSCse77768

  Symptoms: MAC addresses may not be learned when traffic is switched from Multipoint Bridging (MPB) to Virtual Private LAN Services (VPLS).

  Conditions: This symptom is observed on a Cisco 7600 series when traffic is switched from a customer-facing interface that is configured for MPB on a SIP-400 to a core-facing interface that is configured for VPLS and EoMPLS on a SIP-200, SIP-600, enhanced 4-port Gigabit Ethernet OSM, or FlexWAN2.

  Workaround: There is no workaround.

- CSCse91675

  Symptoms: The RP may generate a RX FIFO FULL error message for a SPA, followed by a VC_CONFIG error message, and subsequently all interfaces on all SPAs that are processing traffic may go down.

  Symptoms: This symptom is observed on a Cisco 7600 series that is configured with MLP or MFR bundles on a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3), 2-port channelized T3/DS0 SPA (SPA-2XCT3/DS0), or 4-port channelized T3/DS0 SPA (SPA-4XCT3/DS0) when traffic exceeds about 350 kpps on these bundles.

  Workaround: After the symptom has occurred, reload the affected SPAs or the SIPs in which the affected SPAs are installed. There is no workaround to prevent the symptom from occurring. Therefore, configure the MLP or MFR bundles in such a manner that the 350 kpps threshold is not exceeded.

- CSCse94388

  Symptoms: A SIP-200 that is configured with distributed Multilink Point-to-Point (dMLP) bundles and that has some of the bundles interleaved may crash.

  Conditions: This symptom is observed when you send traffic at line rate through all of the bundles.

  Workaround: There is no workaround.

- CSCse95146

  Symptoms: A Supervisor Engine 720 with a cross-module EtherChannel duplicates all packets that enter or leave the cross-module EtherChannel on the same physical port.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series or Cisco 7600 series that has a Supervisor Engine 720 and an Enhanced FlexWAN module when the supervisor engine functions in bus mode and has a cross-module EtherChannel.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when you remove the cross-module EtherChannel or the Enhanced FlexWAN module.

- CSCse95888

  Symptoms: The bandwidth of an interface on a Fast Ethernet (FE) SPA changes unexpectedly when the interface on the other side is shut down and brought back up, or the other around, brought up and then shut down.

  Conditions: This symptom is observed on a Cisco router such as a Cisco 7600 series or Cisco 12000 series that is configured with an FE SPA.

  Workaround: Use the **bandwidth** command to configure the appropriate bandwidth.

- CSCse98354

  Symptoms: The interfaces of the SPAs on a SIP-200 may enter the up/down state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXF5 but may also occur in Release 12.2(33)SR.

  Workaround: There is no workaround.

- CSCsf04301

  Symptoms: All multicast data packets on ATM multipoint interfaces may be dropped, regardless of the number of VCs that are configured under a single multipoint interface. When this situation occurs, control plane packets still pass so that routing protocol adjacencies do come up and PIM neighbors are formed.

Conditions: This symptom is observed on a Cisco 7600 series that has an ATM SPA.

Workaround: There is no workaround.

Further Problem Description: The ATM OSM is able to direct multicast packets to a single VC that is configured on a multipoint interface.

- CSCsf05390

  Symptoms: A Cisco 7600 series that has a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3) may generate several CPUHOG messages and may crash.

  Conditions: This symptom is observed when you create the 258th channel group on the SPA-1XCHSTM1/OC3 and then delete one of the channel groups.

  Workaround: There is no workaround.

- CSCsf11098

  Symptoms: When you insert a 2-port Gigabit Ethernet SPA (SPA-2X1GE-V2) in a SIP-400 on a Cisco 7600 series, the following error messages may be generated:

  ```
  %FPD_MGMT-3-MAJOR_VER_MISMATCH: Major image version mismatch detected with GE I/O
  FPGA (FPD ID=1) for SPA-2X1GE-V2 card in subslot 5/2. Image will need to be upgraded
  from version 0.5 to at least a minimum version of 1.10. Current HW version = 0.21.

  %FPD_MGMT-5-UPGRADE_ATTEMPT: Attempting to automatically upgrade the FPD image (s)
  for SPA-2X1GE-V2 card in subslot 5/2. Use 'show upgrade fpd progress' command to view
  the upgrade progress ...

  %FPD_MGMT-3-PKG_FILE_SEARCH_FAILED: FPD image package (c7600-fpd-pkg.122-
  33.SRA.pkg) cannot be found in system's flash card or disk to do FPD upgrade.

  %FPD_MGMT-3-CARD_DISABLED: SPA-2X1GE-V2 card in subslot 5/2 is being disabled because
  of an incompatible FPD image
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA or Release 12.2(3)SRA1 and occurs because the SPA-2X1GE-V2 is not supported in Release 12.2(33)SRA and its rebuilds.

  Workaround: Do not insert a SPA-2X1GE-V2 in a Cisco 7600 series that runs Release 12.2(33)SRA or one of its rebuilds.

- CSCsf14018

  Symptoms: A router may crash when a large number of VRFs such as 150 or more are unconfigured.

  Conditions: This symptom is observed when the deletion process suspends while deleting a VRF and when another process that is triggered by the timer deletes the same VRF. When the suspended process resumes, the process attempts to free the already freed memory that belonged to the already deleted VRF. This situation causes the router to crash.

  Workaround: There is no workaround.

- CSCsf19575

  Symptoms: A Cisco 7600 series that has an IPsec SPA with mGRE tunnels that function in VRF mode may crash.

  Conditions: This symptom is observed when you enter the **crypto engine slot** *slot/subslot* **inside** command on the mGRE interface.

  Workaround: There is no workaround.

- CSCsf20194

  Symptoms: When you perform an OIR of a SIP-200, the SIP-200 may crash.

  Conditions: This symptom is observed when the same policy map is attached to both the ingress and egress side of an interface on the SIP-200.

Workaround: There is no workaround.

- CSCsf25712

  Symptoms: A line card such as a SIP-200 may crash when the line card on the other side or SPAs in the line card on the other side are reloaded.

  Conditions: This symptom is observed on a router that has a highly scaled configuration (for example, a configuration that is used for mobile users) with priority traffic and non-priority traffic running at line rate.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs because of memory corruption.

- CSCsf27085

  Symptoms: A SIP-200 may crash when a class with a priority is removed from a service policy while traffic is being processed.

  Conditions: This symptom is observed when the class that is being removed is the last class at a layer in the service policy.

  Workaround: There is no workaround.

- CSCsg04681

  Symptoms: Traffic from an MPLS cloud to a tunnel interface within a VRF may stop when the tunnel interface is moved from the supervisor engine to a SPA.

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

  Workaround: First shut down the tunnel interface, then move the tunnel interface to the SPA, and then bring up the tunnel interface.

- CSCsg17500

  Symptoms: OSPFv3 neighbors or adjacencies are not formed across MLP and MFR links.

  Conditions: This symptom is observed on a Cisco 7600 series for MLP and MFR configurations on a FlexWAN module that is configured for OSPFv3.

  Workaround: There is no workaround.

- CSCsg24278

  Symptoms: After a Supervisor Engine 32 has been powered-on or reloaded, it may enter a state in which it responds very slowly. For example, the response time to a ping from a directly-connected host is very high such as in the order of hundreds of milliseconds as opposed to under a few milliseconds in a normal state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA1.

  Workaround: There is no workaround.

- CSCsg32195

  Symptoms: Line cards that are equipped with a Distributed Forwarding Card 3A (DFC3A) should be powered down because they are not supported in Cisco IOS Release 12.2(33)SRA, but they are still powered up.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: There is no workaround.

- CSCsg35439

  Symptoms: After a switch or router boots up, OSPF neighbors continue to flap. This situation occurs because, even though the switch or router correctly sends and receives OSPF hello packets at every interval, it incorrectly detects that the neighbors are down.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series that has a Supervisor Engine 32 and that runs Cisco IOS Release 12.2(18)SXF6 and on a Cisco 7600 series that has a Supervisor Engine 32 and that runs Release 12.2(18)SXF6 or Release 12.2(33)SRA1.

  Workaround: There is no workaround.

- CSCsg38930

  Symptoms: IP fragments may not be forwarded over an GRE tunnel when the tunnel is configured to go through an IPSEC-SPA-2G. These IP fragments may be dropped.

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and an IPSEC-SPA-2G, and that runs Cisco IOS Release 12.2(18)SXF5 when the tunnel is configured in the following manner:

  – Path MTU Discovery (PMTUD) is enabled.

  – IPsec tunnel protection is enabled.

  – The **crypto engine slot** *slot/subslot* **inside** command is enabled.

  The symptom may also affect other releases.

  The output of the **show crypto vlan** command shows the VLAN that is associated with the crypto configuration.

  Temporary Workaround: Use an ACL with an ACE and the **log** keyword for the specific multicast group.

  Workaround: Disable Path MTU Discovery (PMTUD).

- CSCsg46087

  Symptoms: A packet with a size that is larger than 1460 bytes does not go through a GRE IPsec tunnel even when the IP MTU for the tunnel has a size that is larger than the size of the packet (for example, when the IP MTU is set to 1514 bytes).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series that are configured with an IPSEC-SPA-2G SPA when the following conditions are present:

  – Path MTU Discovery (PMTUD) is enabled.

  – The DF bit is set for the tunnel interface.

  Workaround: Disable PMTUD.

  First Alternate Workaround: Do not set the DF bit for the tunnel interface.

  Second Alternate Workaround: Use a small IP MTU for the tunnel.

  Further Problem Description: Enabling fragmentation on a large number of tunnels may cause some packet loss due to fragmentation timeouts.

- CSCsg46761

  Symptoms: A Cisco 7600 series may reload, causing a temporary service outage.

  Conditions: This symptom is observed when the following conditions are present:

  – The router contains a SIP-600.

  – The SIP-600 contains a Shared Port Adapter (SPA).

  - One or more of the plugholes in the SPA do not contain Small Form Factor Pluggable (SFP) modules.
  - You enter the **show interface transceiver** command at the router console.

  Workaround: Do not enter the **show interface transceiver** command unless all plugholes in all SPAs in the SIP-600 contain SFP modules.

- CSCsg85046

  Symptoms: A Cisco 7600 series with a SIP-600 crashes during the boot process.

  Conditions: This symptom is observed only when a 4-port OC-48c/STM-16 POS/DPT/RPR SPA (SPA-4XOC48POS/RPR) is installed in the SIP-600.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA1

Cisco IOS Release 12.2(33)SRA1 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA1 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCek38025

  Symptoms: A Multicast Distribution Tree (MDT) update does not reach a remote PE router.

  Conditions: This symptom is observed when some of the routers in the network core send MDT addresses in the form of VPNv4 extended community attributes and other routers in the network core send MDT addresses in the MDT SAFI format.

  Workaround: Configure all routers in the network core to use only one form of MDT implementation (that is, configure either the VPNv4 extended community format or the MDT SAFI format).

- CSCek45564

  Symptoms: A router crashes because of memory corruption when you bring up Gigabit Ethernet links and BGP neighbor adjacencies, and an error message is generated, indicating that a block overrun and rezone corruption have occurred.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series that are configured for BGP.

  Workaround: There is no workaround.

- CSCsd98168

  Symptoms: A router may reload unexpectedly when you enable the BGP Support for TCP Path MTU Discovery per Session feature in session-template configuration mode.

  Conditions: This symptom is observed on a Cisco router when there are no BGP neighbors configured.

  Workaround: On a router has no BGP neighbors, do not enable the BGP Support for TCP Path MTU Discovery per Session feature in session-template configuration mode, nor enter the **no transport path-mtu-discovery** command session-template configuration mode.

Miscellaneous

- CSCek31437

  Symptoms: A WS-6516-GE-TX module may not power up, and the following error message may be generated:

  ```
  C6KPWR-SP-4-UNSUPPORTED: unsupported module in slot <slot-no>, power not allowed:
  Module not at an appropriate hardware revision level.
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with a Supervisor Engine 32 that runs Cisco IOS Release 12.2SR or Release 12.2SX.

  Workaround: There is no workaround.

- CSCek35061

  Symptoms: A router may crash when you disassociate a VRF from an MPLS interface.

  Conditions: This symptom is observed on a Cisco router that is configured for L2TP when you enter the **no ip vrf forwarding** *vrf-name* command.

  Workaround: There is no workaround.

- CSCek45862

  Symptoms: Packets are not classified according to the value of the *mpls-exp-value* argument in the **set mpls experimental imposition** *mpls-exp-value* command.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a 6PE router when packets are processed via a SIP-200.

  Workaround: There is no workaround.

- CSCek47083

  Symptoms: In a blade-to-blade configuration, when the encryption cards are reloaded at the same time, there are less GRE SAs at the active blade than that there are at the standby blade, causing traffic loss for the GREs that are missing from the active blade.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a blade-to-blade redundancy configuration and that has 500 GRE over IPsec tunnels.

  Workaround: Do not reload both encryption cards at the same time. First reload one encryption card and wait until it has come up. Then, reload the other encryption card.

- CSCek47205

  Symptoms: A Cisco 7600 series may crash when a blade-to-blade switchover occurs.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.3(33)SRA, that has an IPSec VPN SPA, and that has the **crypto engine mode vrf** command enabled.

  Workaround: There is no workaround.

- CSCek48618

  Symptoms: A Cisco 7600 series may generate the following error message in the console log:

  ```
  %FPD_MGMT-4-UPGRADE_EXIT: Unexpected exit of FPD image upgrade operation for
  7600-SSC-400 card in slot 4.
  ```

After this error message, the following error messages are generated, indicating that the 7600-SSC-400 is unable to boot:

```
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%CWAN_RP-3-BOOTFAIL: The WAN module in slot 4/0 failed to boot
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
%CWAN_RP-3-BOOTFAIL: The WAN module in slot 4/0 failed to boot
%CWAN_RP-3-RESET_FAIL: The WAN module in slot 4 failed even after several resets
```

Workaround: Contact Cisco TAC for a workaround that prevents an RMA of the 7600-SSC-400.

- CSCsc38127

  Symptoms: The standby supervisor engine may crash when an interface has a stateful inspection policy or when the **ip nbar protocol-discovery** command is enabled.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series or Cisco 7600 series that run a native Cisco IOS software image.

  Workaround: There is no workaround.

- CSCsd39344

  Symptoms: When MPLS cell-relay or ATM cell-switched traffic enters an OC-48 ATM SPA that is installed in a SIP-400, the performance is limited to 64.5 percent of the OC-48 line rate (which is about 1.5 Gb/s).

  Conditions: This symptom is observed on a Cisco 7600 series and occurs only for MPLS cell-relay or ATM cell-switched traffic.

  Workaround: Avoid sending MPLS cell-relay or ATM cell-switched traffic above 64.5 percent of the OC-48 line rate to the OC-48 ATM SPA.

  Note that the performance for two-cell traffic or traffic with larger packets (that is, non-cell switched traffic) is not impacted and full line rate is supported in these cases.

- CSCsd96511

  Symptoms: When a hardware interface goes down, for example because the interface is shut down, the cable is disconnected, or an uplink on a supervisor engine goes from the active state to the standby state, packets in the egress direction are bridged in the software for later processing. When

there is a high traffic rate, this situation may cause CPU congestion until the routing table is updated in the hardware. This type of traffic (that is, traffic that is bridged for later processing) cannot be rate-limited.

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

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat causes the packets to be denied and dropped instead of being bridged in the software.

- CSCse00135

  Symptoms: When MLPoMPLS is configured, a VC comes up but, the first few ping packets from one CE router to another CE router on the far end do not go through.

  Conditions: This symptom is observed in a configuration with Cisco 7600 series routers that functions as CE and PE routers.

  Workaround: There is no workaround. Note that the connectivity recovers after a few pings.

- CSCse05336

  Symptoms: A subinterface of an OSM-2+4GE-WAN+ that is passing traffic may drop some packets when you create a new subinterface or delete an existing subinterface on the same physical interface as the subinterface that is passing traffic.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF3. The symptom may also affect Release 12.2(33)SRA.

  Workaround: There is no workaround.

- CSCse14269

  Symptoms: The encapsulation and decapsulation counters in the output of the **show crypto ipsec sa stats** command are inaccurate because they are not updated correctly during a rekey.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an IPsec VPN SPA.

  Workaround: Do no set the IPsec SA lifetime to prevent rekeying of the IPsec SA.

- CSCse19351

  Symptoms: On a Cisco 7600 series that has an IPsec VPN SPA, traffic may not pass through an IPsec tunnel when the destination is reached through a front-door VRF (FVRF).

  The symptom typically occurs in the following configuration:

```
interface Tunnel105
 ip vrf forwarding black
 ip address 10.0.0.1 255.0.0.0
 tunnel source 10.0.1.1
 tunnel destination 10.0.0.2
 tunnel vrf temp2044
 tunnel protection ipsec profile ipsec_black_105
 crypto engine slot 3/0 inside
```

  Conditions: This symptom is observed when the internal VRF table ID that is associated with a FVRF is greater than 1024.

In the example above (in the Symptoms section), the internal VRF table ID that must be confirmed is “temp2044”; enter the **show ip vrf detail temp2044** command to identify the internal VRF table ID.

Workaround: Limit the number of VRFs that are defined on the router to less than 1024.

- CSCse20150

  Symptoms: A SPA may cause an RX FIFO FULL error message to be generated on the RP. When this occurs, a VC_CONFIG error message is generated, and subsequently all interfaces on all SPAs that are switching traffic go down.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for MLP or MFR when traffic with 46-byte size packets exceeds about 350 kpps on the MLP or MFR bundles.

  Workaround: When the symptom has occurred, reload the SIP with the affected SPA. To prevent the symptom from occurring, ensure that traffic does not exceed about 350 kpps on the MLP or MFR bundles. If this is not an option, there is no preventive workaround.

  Further Problem Description: The following is an example configuration in which the symptom occurs:

  Consider 110 bundles with 6 members with 4 DS0 interfaces, so each bundle has 1.5 Mbps of bandwidth. When you send an IP packet of 46 bytes, the maximum traffic that will flow through the SIP is as follows:

  ```
  110 Bundles * (1536kbps * 1000bits) / (8 * (46bytes + 13bytes)) = 357965 pps (rounded
  to about 350 kpps)
  ```

- CSCse20340

  Symptoms: Upon recovery from a microcode reload on a line card or a router bootup, the controller state for a serial interface of a 2-port or 4-port T3/E3 SPA may remain in the “down” state.

  Conditions: This symptom is observed on a Cisco 7600 series and Cisco 12000 series.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected serial interface to enable the interface to enter the “up” state.

- CSCse30293

  Symptoms: A ping may not go through an IPsec tunnel on a Cisco 7600 series after you have copied a configuration from a disk device to the running configuration.

  Conditions: This symptom is observed on a Cisco 7600 series system that has an IPsec VPN SPA on which tunnels with tunnel protection are configured.

  When the symptom occurs, the encryption and decryption counters in the output of the **show crypto ipsec sa** command for the affected IPsec tunnel do still increment, but a ping to the tunnel IP address does not go through. The output of the **show interface tunnel** *number* shows the tunnel interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected tunnel interface.

- CSCse34615

  Symptoms: A RADIUS virtual server drops RADIUS accounting on and off packets, instead of forwarding the packets to the real servers. The client never receives response packets for the RADIUS accounting on and off packets that were sent.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series.

  Workaround: There is no workaround.

- CSCse35278

  Symptoms: A Cisco 7600 series with an IPSec VPN Services Module or IPSec VPN SPA may incorrectly drop IPSec NAT Traversal (NAT-T) transit packets that are transported via UDP port 4500.

  Conditions: This symptom is observed on a Cisco 7600 series that terminates IPSec tunnels on an IPSec VPN Services Module or IPSec VPN SPA when the NAT-T packets must traverse the crypto VLAN.

  Workaround: There is no workaround.

- CSCse35319

  Symptoms: The IP MTU is not properly applied to the payload.

  Conditions: This symptom is observed when the IP MTU is configured on a Virtual Tunnel Interface (VTI).

  Workaround: There is no workaround.

- CSCse35622

  Symptoms: Routed packets are dropped from VLANs that are configured for split horizon.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SIP-400 when two or more VLANS are configured for split horizon and when a layer-3 packet is routed from one VLAN with a split horizon configuration to another VLAN with a split horizon configuration.

  Workaround: Do not configure split horizon, which is a bridge-domain option, on an interface or subinterface when layer-3 traffic may be routed from another bridge domain that is configured with split horizon. Note that this workaround disables the split horizon feature for bridging, which is its normal use.

  Further Problem Description: The symptom occurs on a SIP-400 because the line card microcode does not distinguish between layer-2 switched packets and layer-3 routed packets on bridged interfaces when split horizon is configured. Both cases result in dropped packets, which is correct for layer-2 switched packets but not for layer-3 routed packets.

- CSCse47732

  Symptoms: RFC 1407 and RFC 2496 are not supported on a 1-port channelized STM1/OC3 SPA.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when SNMP queries are performed for CISCO-DS3-MIB objects.

  Workaround: There is no workaround.

- CSCse50009

  Symptoms: The supervisor engine of a Cisco 7600 series may generate the following error message:

  ```
  %COMMON_FIB-SP-3-FIBXDRINV: Invalid XDR format. FIB entry XDR has bogus routecount
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for IPv6 when you configure a PortChannel.

  Workaround: There is no workaround.

- CSCse50607

  Symptoms: Periods of high latency may occur on a Multilink PPP interface, and finally the interface may lock up.

  Conditions: This symptom is observed on a Cisco 7600 series when the Multilink PPP interface is configured on a SPA-8XCHT1/E1 that is installed in a SIP-200.

Workaround: Configure multilink interfaces on another line card that does not require insertion in a SIP.

Alternate Workaround: Configure IP load balancing by using two separate E1 links (that is, do not use multilink interfaces).

- CSCse57865

  Symptoms: An ICMP unreachable message from an IPsec VPN SPA does not have the correct MTU size. The MTU value is too conservative and causes an unexpected fragmentation behavior for traffic within a specific packet-size range.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when traffic is sent that has the DF bit set and that must be fragmented after the IPsec encryption.

  Workaround: There is no workaround.

- CSCse73539

  Symptoms: A Supervisor Engine 720 may crash because the EOBC channel is jammed when you insert a second Supervisor Engine 720 in the chassis.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series.

  Workaround: There is no workaround.

- CSCse76036

  Symptoms: In an MPLS TE FRR configuration, a point of local repair (PLR) router may insert an MPLS label that has a value of 3 (that is, an implicit null label) into the outgoing label stack. This situation prevents traffic from being forwarded.

  Conditions: This symptom is observed on a Cisco 7600 series when the primary TE tunnel is a one-hop tunnel that is configured for implicit null labels and LDP. For an MPLS L3VPN prefix, the outgoing packets have a label stack of “3, ldp label, vpn label.” The correct label stack in this case should be “ldp label, vpn label.”

  Workaround: Configure the one-hop primary TE tunnel for explicit-null labels as the outgoing labels.

- CSCsf04112

  Symptoms: On a Cisco 7600 router, the MAC address of one or more interfaces may change unexpectedly when the ifPhysAddress object of the IF-MIB is accessed by SNMP. This situation prevents the router from receiving packets when an ARP entry that contains the MAC address of the router is refreshed.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: To prevent the symptom from occurring, configure static ARP on the devices that must be able to send packets to the router. After the symptom has occurred, reload the router to clear the condition.

- CSCsf13513

  Symptoms: Packets are dropped because of decryption errors.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with an SPA-IPSEC-2G and occurs when incoming NAT-T packets result in an error. This situation causes incorrect information to be sent with the next packet, and, in turn, causes a decryption error.

  Workaround: There is no workaround.

Further Problem Description: The symptom occurs intermittently, and the platform may recover automatically.

Wide-Area Networking

- CSCek26657

  Symptoms: The following state mismatch error messages may be generated on the console of a standby RP:

  ```
  %IPV6-STDBY-4-IDB: Interface XXX state mismatch. IPv6 state is down, interface is up
  ```

  (Note that XXX represents the interface.)

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant RPs that function in SSO mode, and that is configured for IPv6, PPP, and IP header compression.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SRA

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRA. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRA. This section describes only severity 1, severity 2, and select severity 3 caveats.

IP Routing Protocols

- CSCsb86987

  Symptoms: A Cisco router may generate tracebacks or may crash when multicast performs an RPF lookup into the BGP table.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and multicast.

  Workaround: There is no workaround.

- CSCsc58030

  Symptoms: When a local PE router receives remote VPNv4 routes, the following error messages may be generated.

  ```
  %IPRT-3-PATHIDX: Bad path pointer of 0 for 201.1.10.0, 2 max
  -Process= "BGP Router", ipl= 0, pid= 414
  ```

  Conditions: This symptom is observed on a Cisco router that functions as a PE router with 200 VRFs and about 50,000 VPNv4 routes.

  Workaround: There is no workaround.

- CSCsc79722

  Symptoms: eBGP sessions between a PE router and a CE router may go down after an SSO switchover has occurred.

  Conditions: This symptom is observed after an SSO switchover has occurred on a PE router when the BGP sessions are all set and when all routes in the BGP VPNv4 table have been checked. When you sent traffic from a CE router to the PE router, the BGP sessions may go down after 3 or 4 minutes.

  Workaround: Stop the traffic to enable the eBGP sessions to come up again. Then, resume the traffic.

- CSCsd98168

  Symptoms: A router may reload unexpectedly when you enable the BGP Support for TCP Path MTU Discovery per Session feature in session-template configuration mode.

  Conditions: This symptom is observed on a Cisco router when there are no BGP neighbors configured.

  Workaround: On a router has no BGP neighbors, do not enable the BGP Support for TCP Path MTU Discovery per Session feature in session-template configuration mode, nor enter the **no transport path-mtu-discovery** command session-template configuration mode.

- CSCse28676

  Symptoms: The following error message may be generated continuously on a PE router, preventing an OSPF neighbor to enter the "Full" state because OSPF packets are dropped:

  ```
  %OSPF-4-BADLENGTH: Invalid length in OSPF packet type x
  ```

  Conditions: This symptom is observed on a Cisco platform that functions as a PE router when the following configuration is present:

  – The OSPF Sham-Link Support for MPLS VPN feature is enabled.

  – The value of the MPLS MTU is smaller than the default MPLS MTU for the connection between the PE router and a P router that functions as the OSPF neighbor.

  Workaround: Configure the default MPLS MTU for the connection between the PE router and the P router.

- CSCse35654

  Symptoms: IPv6 multicast streams may become stuck in the registering state.

  Conditions: This symptom is observed on a Cisco router that has a large number of IPv6 multicast streams.

  Workaround: There is no workaround.

Miscellaneous

- CSCek36924

  Symptoms: Traffic on tunnel interfaces may be punted to the RP.

  Conditions: This symptom is observed on a Cisco 7600 series when you delete and re-create tunnel interfaces. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCek43849

  Symptoms: Traffic on a 4-port Gigabit Ethernet WAN Optical Services Module (OSM-2+4GE-WAN+) may be interrupted.

  Conditions: This symptom is observed on a Cisco 7600 series after you have reloaded the router and when the OSM-2+4GE-WAN+ has an egress HQoS policy. The symptom occurs because the queues on the line card are not created.

  Workaround: Remove and re-apply the policy map on the GE interfaces of the OSM-2+4GE-WAN+.

- CSCek45604

  Symptoms: An OSM or FlexWAN module may crash when you apply an input QoS configuration to a Frame Relay interface in a particular sequence.

Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

1. You attach a policy to the main interface and you use the map class for inheritance.
2. You remove the Frame Relay class from the interface and attach a flat policy to the main interface.

Note that the symptom does not occur when you apply an output QoS configuration to a Frame Relay interface.

Workaround: Do not apply an input QoS configuration to a Frame Relay interface.

- CSCsd39344

  Symptoms: When MPLS cell-relay or ATM cell-switched traffic enters an OC-48 ATM SPA that is installed in a SIP-400, the performance is limited to 64.5 percent of the OC-48 line rate (which is about 1.5 Gb/s).

  Conditions: This symptom is observed on a Cisco 7600 series and occurs only for MPLS cell-relay or ATM cell-switched traffic.

  Workaround: Avoid sending MPLS cell-relay or ATM cell-switched traffic above 64.5 percent of the OC-48 line rate to the OC-48 ATM SPA.

  Note that the performance for two-cell traffic or traffic with larger packets (that is, non-cell switched traffic) is not impacted and full line rate is supported in these cases.

- CSCsd73577

  Symptoms: When the active supervisor engine is reloaded during an SSO switchover, the following error message may be generated:

  ```
  %MDT-4-RD_CONFLICT: MDT entry 10:30:(2.2.2.2,0.0.0.0) received an update for RD 11:30
  ```

  Conditions: This symptom is observed on a Cisco platform that is configured for Multicast VPN.

  Workaround: There is no workaround.

- CSCsd88478

  Symptoms: Memory fragmentation and memory allocation (Malloc) failures may occur on AToM edge or core line cards after a few SSO switchovers have occurred under stress traffic conditions.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR and that has AToM configured when there are several thousand EoMPLS and FRoMPLS or ATMoMPLS VCs configured.

  Workaround: Reload the affected line cards.

- CSCsd99417

  Symptoms: An FRR failover may fail when the primary path for a TE tunnel that is protected by FRR is shut down before the tunnel has completely recovered from a previous FRR failover.

  Conditions: This symptom is observed on a Cisco 7600 series when the primary path fails before the tunnel has reoptimized completely to its primary path. This situation is considered a double failure case and is not supported. The output of the **show mpls traffic-eng fast-reroute database** command shows whether or not the primary tunnel has recovered completely: the FRR database entry should be in the “ready” state for the FRR failover to be successful.

  Workaround: To prevent the symptom from occurring, ensure that the primary path for the TE tunnel that is protected by FRR is not shut down while the tunnel is recovering from a previous FRR failover. When the symptom has occurred, toggle the primary tunnel interface to recover from the failure.

- CSCse19299

  Symptoms: Some packet drops may occur during SA negotiation between two spokes. The expected behavior is that during SA negotiation between the spokes, the traffic should flow through spoke-to-hub tunnels. Note that when the spoke-to-spoke SA is up, traffic flows fine without any packet drops.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCse22894

  Symptoms: A traceback and the following error message are generated during the initial boot process:

  ```
  PM-SP-STDBY-3-INTERNALERROR: Port Manager Internal Software Error
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with two Supervisor Engine 720 processors that run in SSO mode.

  Workaround: There is no workaround.

- CSCse24715

  Symptoms: When Multicast Listener Discovery (MLD) leave messages are sent for 500 or more subinterfaces, traffic continues to be forwarded to some of these subinterfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that sends MLD leave messages via one physical connection to 500 or more subinterfaces. The symptom occurs because some OIFs through which the MLD leave messages are sent are not deleted.

  Workaround: There is no workaround to prevent the symptom from occurring. To recover from the symptom, clear the MFIB entry through which the traffic is forwarded.

  Further Problem Description: This caveat occurs because of a timing issue.

- CSCse31859

  Symptoms: The **monitor session** *session* **destination interface** *type*/*slot*/*port* command does not function.

  Conditions: This symptom is observed on a Cisco 7600 series after you have configured a Remote SPAN (RSPAN) VLAN.

  Workaround: There is no workaround.

- CSCse34025

  Symptoms: When you scale a router with the maximum number (65,536) of dynamic MAC entries, one or two dynamic MAC entries are dropped after a few seconds. You can verify this situation in the output of the **show mac-address-table count** command.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a basic configuration.

  Workaround: There is no workaround.

- CSCse34697

  Symptoms: When you configure a crypto map and enter the **reverse-route remote-peer** command, the reverse route that is injected by IPsec when the IPsec tunnel comes up may point to an incorrect interface.

Conditions: This symptom is observed when the following occurs:

1. You apply a crypto map to one interface (A).
2. You apply a crypto map to a second interface (B).
3. You remove the crypto map from the second interface (B).

In this situation, when the IPsec tunnel comes up, IPsec points to the second interface (B) instead of the first interface (A).

Workaround: To ensure that the reverse route points to the correct interface, re-apply the crypto map to the first interface (A).

- CSCse35319

  Symptoms: The IP MTU is not properly applied to the payload.

  Conditions: This symptom is observed when the IP MTU is configured on a Virtual Tunnel Interface (VTI).

  Workaround: There is no workaround.

- CSCse35457

  Symptoms: A SPA-8XCTE1 may generate the following error messages during its boot process:

  ```
  %INTR_MGR-3-INTR: SPA-8XCHT1/E1[1/2] [SPA FPGA] IPC RX Parity Error
  %INTR_MGR-3-BURST: SPA-8XCHT1/E1[1/2] [SPA FPGA] IPC TX Parity Error [100]
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that has a SPA-8XCTE1 installed in a SIP-200 and occurs during the boot process of the SPA-8XCTE1.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur after the SPA has properly booted.

- CSCse35825

  Symptoms: An IPsec VPN SPA may become stuck in the “Initializing” state.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are reloaded with the maximum number of VLANS allocated.

  Workaround: Delete some VLANs or IPsec tunnels to enable the IPsec VPN SPA to enter the “Active” state.

  Further Problem Description: When the symptom occurs, the output of the **show platform hardware capacity | i VLAN** command shows “0 free” VLAN resources:

  ```
  VLANs: 4094 total, 1005 VTP, 0 extended, 3089 internal, 0 free
  ```

  When the platform reloads, the startup configuration allocates all VLANs. While the IPsec VPN SPA boots, there are no VLANs available for the control messaging of the IPsec VPN SPA, causing the IPsec VPN SPA to become stuck in the “Initializing” state.

- CSCse37684

  Symptoms: When an SSO switchover occurs after the STP mode has been changed, some tracebacks may be generated on the newly active supervisor engine.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with two supervisor engines that run in SSO mode.

  Workaround: There is no workaround. However, the tracebacks appear for only about a second and should not affect any functionality of the router.

- CSCse38650

  Symptoms: A router that functions as a BGP Route Reflector in an multicast VPN environment may displays error messages and may eventually crash.

  Conditions: This symptom is observed when the router receives multicast updates and attempts to send multicast updates in which it sets itself as the next hop.

  Workaround: There is no workaround.

- CSCse50009

  Symptoms: The supervisor engine of a Cisco 7600 series may generate the following error message:

  ```
  %COMMON_FIB-SP-3-FIBXDRINV: Invalid XDR format. FIB entry XDR has bogus routecount
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for IPv6 when you configure a PortChannel.

  Workaround: There is no workaround.

- CSCse53249

  Symptoms: A router may crash during the configuration of PIM, specifically when you enter the **ip pim send-rp-announce** command for a tunnel.

  Conditions: This condition is observed on a Cisco router when the following conditions are present:

  – A large number (125 or a higher number) of tunnels is configured.

  – The **ip pim sparse-dense-mode** command is enabled on a VLAN interface.

  – You enter the **ip pim send-rp-announce** *interface-type interface-number* **scope** *ttl-value* command for each tunnel.

  Workaround: Perform the following steps:

  1. Remove the **ip pim sparse-dense-mode** command from the VLAN interface.
  2. Do not enter the **ip pim send-rp-announce** command. Rather, manually configure a rendezvous point (RP) for each scope.

- CSCsg09423

  Symptoms: When IPsec SAs flap, traffic loss may occur during the IPsec and IKE rekey.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when there is a large number of IKE and IPsec SAs (that is, more than 2000 IKE SAs and 4000 IPsec SAs) and when RSA signature authentication is configured.

  Workaround: Reduce the number of IKE and IPsec SAs.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SRA. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsd75273

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

- CSCse52951

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page*:

  http://www.cisco.com/warp/public/108/index.shtml

- *Troubleshooting Bus Error Exceptions*:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

- *Why Does My Router Lose Its Configuration During Reboot?*:

  http://www.cisco.com/warp/public/63/lose_config_6201.html

- *Troubleshooting Router Hangs*:

  http://www.cisco.com/warp/public/63/why_hang.html

- *Troubleshooting Memory Problems*:

  http://www.cisco.com/warp/public/63/mallocfail.shtml

- *Troubleshooting High CPU Utilization on Cisco Routers*:

  http://www.cisco.com/warp/public/63/highcpu.html

- *Troubleshooting Router Crashes*:

  http://www.cisco.com/warp/public/122/crashes_router_troubleshooting.shtml

- *Using CAR During DOS Attacks*:

  http://www.cisco.com/warp/public/63/car_rate_limit_icmp.html

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2SR. These documents consist of hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, feature modules, and other documents.

Documentation is available online on Cisco.com.

Use these release notes with the following resources:

Release-Specific Documents

This section provides information about release-specific documents.

Cisco IOS Release 12.2SR

The following documents are specific to Cisco IOS Release 12.2SR and are located at http://www.cisco.com/univercd/home/index.htm:

- New Feature Documentation for Cisco IOS Release 12.2SR

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/index.htm
- Command Reference for Cisco IOS Release 12.2SR

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

Note For Cisco IOS Release 12.2(33)SRA and later releases of Release 12.2SR, all commands that are supported on the Cisco 7600 series are documented in the *Command Reference for Cisco IOS Release 12.2SR*. The *Cisco 7600 Series Router Cisco IOS Command Reference* is still available in Release 12.2(33)SRA but will not be updated for later releases of Release 12.2SR. We recommend that you start using the *Command Reference for Cisco IOS Release 12.2SR*.

Cisco IOS Release 12.2

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2**

- Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**

- Caveats for Cisco IOS Release 12.2 (Parts 5 through 8)

  As a supplement to the caveats listed in the "Caveats" section in these release notes, see the *Cross-Platform Release Notes for Cisco IOS Release 12.2*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2.

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2**

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 click **Support: Tools & Resources: Bug Toolkit** (which is listed under Troubleshooting). Another option is to 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.)

Cisco IOS Release 12.2S

The following documents are specific to Cisco IOS Release 12.2S and are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2S*

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Release Notes**

- New Feature Documentation

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**: **Feature Guides**

On http://www.cisco.com/univercd/home/index.htm at

Cisco IOS Software: **Release 12.2**: **New Feature Documentation**: **Cisco IOS Release 12.2 S**: **New Feature Documentation**

- Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **New Feature Documentation**: **Cisco IOS Release 12.2 S**: **System Messages for 12.2S**

Cisco IOS Release 12.2SX

The following documents are specific to Cisco IOS Release 12.2SX and are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

- *Release Notes for Cisco IOS Release 12.2SX*

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 SX**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Routers: **Cisco 7600**: **Cisco IOS Software Release Notes**

- New Feature Documentation

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 SX**: **Feature Guides**

  On http://www.cisco.com/univercd/home/index.htm at

  Routers: **Cisco 7600**: **Cisco IOS Software Documentation**: **Cisco 7600 Series Router Cisco IOS Software Documentation, 12.2SX**: **12.2 SX New Features**

- Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 SX**

  On http://www.cisco.com/univercd/home/index.htm at

  Routers: **Cisco 7600**: **Cisco IOS Software Documentation**: **Cisco 7600 Series Router Cisco IOS Software Documentation, 12.2SX**

Platform-Specific Documents

Platform-specific information and documents for the Cisco 7600 series routers are available at the following locations:

- Cisco 7600 series home page on Cisco.com at

  Products & Solutions: **Products: Routers and Routing Systems**: **7600 Series Routers**

- Cisco 7600 series technical documentation on Cisco.com at

  Products & Solutions: **Products: Routers and Routing Systems**: **7600 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7600 Series Routers**

- For Cisco 7600 series technical documentation on http://www.cisco.com/univercd/home/index.htm, select **Cisco 7600** from the **Routers** pull-down menu on the top left of the page.
- Cisco 7200 series home page on Cisco.com at

  Support: Select a Product: Routers: Cisco 7200 Series Routers

- Cisco 7200 series technical documenation on Cisco.com at

  Support: Select a Product: Routers: Cisco 7200 Series Routers: Install and Upgrade: Install and Upgrade Guides

- Cisco 7300 series home page on Cisco.com at

  Support: Select a Product: Routers: Cisco 7300 Series Routers

- Cisco 7300 series technical documentation on Cisco.com at

  Support: Select a Product: Routers: Cisco 7300 Series Routers: Install and Upgrade: Install and Upgrade Guides

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2SR and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature modules for Cisco IOS Release 12.2SR are available at the following locations:

- Release 12.2(33)SRA

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/index.htm

- Release 12.2(33)SRB

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/index.htm

- Release 12.2(33)SRC

  http://www.cisco.com/en/US/docs/ios/12_2sr/12_2src/12_2_33_src_newfeatlist.html

Cisco Feature Navigator

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

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

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

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command reference publications, and several other supporting documents.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

- Configuration guides on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Reference Guides**: **Configuration Guides**

- Command references on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Configure**: **Command References**

- Configuration guides and command references on http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Cisco IOS Release 12.2 Configuration Guides and Command References**

Cisco IOS Release 12.2 Documentation Set Contents

Table 10 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

Note You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at

Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**

On http://www.cisco.com/univercd/home/index.htm at

Cisco IOS Software: **Release 12.2**

Table 10 Cisco IOS Release 12.2 Documentation Set

Modules	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM N2etworking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing IP Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX

Table 10 Cisco IOS Release 12.2 Documentation Set (continued)

Modules	Major Topics
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service

Table 10 Cisco IOS Release 12.2 Documentation Set (continued)

Modules	Major Topics
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • *New Features in Release 12.2 T* • *Release Notes* (Release note and caveat documentation for 12.2-based releases and various platforms)	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco.com. From Cisco.com, click the following path: **Support: Software Downloads: Network Management Software: Cisco Network Management Toolkit: Cisco MIBs**.

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 479.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.