Cross-Platform Release Notes for Cisco IOS Release 12.2SB

April 6, 2007

Cisco IOS Release 12.2(31)SB4

OL-9967-02 Rev. S0 Hd

Note Cisco IOS Release 12.2(31)SB4 supports only the Cisco 7200 series routers.

These release notes support Cisco IOS Release 12.2SB up to and including Cisco IOS Release 12.2(31)SB4. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and related documents.

Cisco IOS Release 12.2SB is tailored for service provider networks and large-scale enterprise networks. The main purposes of Release 12.2SB are the following:

- For the Cisco 10000 series, to introduce greater scalability for Multiprotocol Label Switching (MPLS) provider edge (PE) applications with the introduction of advanced High Availability (HA) capabilities.
- For the Cisco 7200 series, Cisco 7301, and Cisco 10000 series, to introduce the Intelligent Service Gateway (ISG).
- For the Cisco 7304, to introduce significant improvements for MPLS VPNs by supporting advanced quality of service (QoS) features such as a multiple action policer and support for 3-level hierarchical policies.

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

For a list of the software caveats that apply to Cisco IOS Release 12.2SB, see the "Caveats" section on page 119, the *Caveats for Cisco IOS Release 12.2* document, and the "Caveats" section in the *Cross-Platform Release Notes for Cisco IOS Release 12.2S*. These documents are updated for every maintenance release and are located on Cisco.com.

Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.2* document and the *Cross-Platform Release Notes for Cisco IOS Release 12.2S*, both of which are located on Cisco.com.

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

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

Introduction

Cisco IOS Release 12.2SB is based on Cisco IOS Release 12.2(25)S and includes many features from Cisco IOS Release 12.2T.

For the Cisco 10000 series, Release 12.2SB supports select features from Release 12.2(25)S that include Multiprotocol Label Switching (MPLS) provider edge (PE) feature parity with Cisco IOS Release 12.0(27)S, along with greater scalability and feature enhancements.

For the Cisco 7200 series and Cisco 7301, all features that are in Release 12.2(25)S are also in Release 12.2SB.

For the Cisco 7304, all features that are supported in Cisco IOS Release 12.2S, up to and including Release 12.2(25)S3, are also in Release 12.2SB.

Many of the features and the 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 12.2SB, see the "New and Changed Information" section on page 17 and the "Caveats" section on page 119.

Early Deployment Releases

These release notes describe the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 router, and Cisco 10000 series routers for Cisco IOS Release 12.2SB, which is an early deployment (ED) release based on Cisco IOS Release 12.2 and Release 12.2S. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features. Table 1 shows the Cisco IOS Release 12.2SB early deployment releases for the above-mentioned platforms.

Table 1 Early Deployment Releases for the Cisco 7200 Series, Cisco 7301, Cisco 7304, and Cisco 10000 Series

Cisco IOS ED Release	Type of ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(31)SB4	Rebuild	No new software features.	No new hardware features.	04/06/2007
12.2(31)SB3	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(31)SB3" section on page 17.	No new hardware features.	02/23/2007
12.2(31)SB2[1]	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(31)SB2" section on page 22.	See the "New Hardware Features in Cisco IOS Release 12.2(31)SB2" section on page 18.	12/04/2006
12.2(28)SB6	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(28)SB6" section on page 57.	See the "New Hardware Features in Cisco IOS Release 12.2(28)SB6" section on page 57.	01/12/2007
12.2(28)SB5	Rebuild	No new software features.	No new hardware features.	10/03/2006
12.2(28)SB4	Rebuild	No new software features.	No new hardware features.	08/31/2006
12.2(28)SB3	Rebuild	No new software features.	No new hardware features.	07/24/2006
12.2(28)SB2	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(28)SB2" section on page 58.	See the New Hardware Features in Cisco IOS Release 12.2(28)SB2, page 58.	06/19/2006
12.2(28)SB1	Rebuild	No new software features.	No new hardware features.	05/11/2006
12.2(28)SB	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(28)SB" section on page 64.	See the"New Hardware Features in Cisco IOS Release 12.2(28)SB" section on page 62.	03/20/2006

1. Cisco IOS Release 12.2(31)SB and Release 12.2(31)SB1 are not publicly available.

System Requirements

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

Memory Recommendations

Note Memory recommendations tables are not included in the Cisco IOS Release 12.2SB release notes to improve the usability of the release notes documentation. The memory recommendations 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/fn

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 12.2SB, 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, choose **12.2SB**.

Step 6 From the Release drop-down menu, choose 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

This section describes the platforms, port adapters, and line cards that are supported in Cisco IOS Release 12.2SB and consists of the following subsections:

Supported Platforms

Cisco IOS Release 12.2SB supports the following platforms:

- Cisco 7200 series routers (including the Cisco 7204VXR and Cisco 7206VXR routers)
- Cisco 7301 router
- Cisco 7304 router
- Cisco 10000 series routers (the Cisco 10008 with a PRE-2 or PRE-3)

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 17.

Table 2 describes the supported platforms for Cisco IOS Release 12.2SB and uses the following conventions:

- Yes—The platform is supported in the release.
- No—The platform is not supported in the release.

Table 2 Supported Platforms for Cisco IOS Release 12.2SB

Cisco IOS Release	7200 Series	7301 Router	7304 Router	10000 Series
12.2(31)SB4	Yes	No	No	No
12.2(31)SB3	Yes	Yes	Yes	Yes
12.2(31)SB2[1]	Yes	Yes	Yes	Yes
12.2(28)SB6	Yes	Yes	Yes	Yes
12.2(28)SB5	Yes	Yes	Yes	Yes
12.2(28)SB4	Yes	Yes	Yes	Yes
12.2(28)SB3	Yes	Yes	Yes	Yes
12.2(28)SB2	Yes	Yes	Yes	Yes
12.2(28)SB1	No	No	Yes	No
12.2(28)SB	Yes	Yes	Yes	Yes

1. Cisco IOS Release 12.2(31)SB and Release 12.2(31)SB1 are not publicly available.

Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, and Cisco 7304

Table 3 lists the port adapters that are supported for the Cisco 7200 series routers, and Cisco 7301 router in Cisco IOS Release 12.2SB and uses the following conventions:

- Yes—The port adapter is supported in the software image.
- No—The port adapter is not supported in the software image.
- In—The release in the "In" column indicates the Cisco IOS 12.2SB release in which the port adapter was introduced. If a cell in this column contains an em dash (—), support for the port adapter was inherited from Cisco IOS Release 12.2 or from another release and was included in the initial base release of Cisco IOS Release 12.2SB.

Table 3 Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, and Cisco 7304

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7304 Router
ATM Port Adapters					
PA-A3-OC3MM	1-port ATM Enhanced OC3c/STM1 multimode	—	Yes	Yes	Yes
PA-A3-OC3SMI	1-port ATM Enhanced OC3c/STM1 single mode (IR)	—	Yes	Yes	Yes
PA-A3-OC3SML	1-port ATM Enhanced OC3c/STM1 single mode (LR)	—	Yes	Yes	Yes
PA-A3-OC12MM	1-port ATM Enhanced OC12/STM4 multimode	—	No	No	No
PA-A3-OC12SMI	1-port ATM Enhanced OC12/STM4 single mode (IR)	—	No	No	No
PA-A3-E3	1-port ATM Enhanced E3	—	Yes	Yes	Yes
PA-A3-T3	1-port ATM Enhanced DS3	—	Yes	Yes	Yes
PA-A3-8E1IMA	8-port ATM Inverse Mux E1, 120 ohms	—	Yes	Yes	Yes
PA-A3-8T1IMA	8-port ATM Inverse Mux T1	—	Yes	Yes	Yes
PA-A6-OC3MM	1-port ATM OC-3c/STM-1 multimode, enhanced	12.2(28)SB	Yes	Yes	Yes[2]
PA-A6-OC3SMI	1-port ATM OC-3c/STM-1 single-mode (IR), enhanced	12.2(28)SB	Yes	Yes	Yes[2]
PA-A6-OC3SML	1-port ATM OC-3c/STM-1 single-mode (LR), enhanced	12.2(28)SB	Yes	Yes	Yes[2]
PA-A6-T3	1-port ATM DS3, enhanced	12.2(28)SB	Yes	Yes	Yes[2]
PA-A6-E3	1-port ATM E3, enhanced	12.2(28)SB	Yes	Yes	Yes[2]
Ethernet/Fast Ethernet/Gigabit Ethernet Port Adapters					
PA-4E	4-port Ethernet 10BASE-T	—	Yes	Yes	Yes
PA-4E1G/75	4-port E1 G.703 Serial, 75 ohms/unbalanced	—	Yes	Yes	Yes
PA-4E1G/120	4-port E1 G.703 Serial, 120 ohms/balanced	—	Yes	Yes	Yes
PA-8E	8-port Ethernet 10BASE-T	—	Yes	Yes	Yes
PA-2FE-FX	2-port Fast Ethernet 100BASE-FX	—	Yes	Yes	Yes
PA-2FE-TX	2-port Fast Ethernet 100BASE-TX	—	Yes	Yes	Yes
PA-GE	1-port Gigabit Ethernet	—	Yes	No	Yes
High-Speed Serial Port Adapters					
PA-H	1-port High-Speed Serial Interface (HSSI)	—	Yes	Yes	Yes
PA-2H	2-port High-Speed Serial Interface (HSSI)	—	Yes	Yes	Yes
Multichannel Serial Port Adapters					
PA-MC-T3	1-port multichannel T3	—	Yes	Yes	Yes
PA-MC-E3	1-port multichannel E3	—	Yes	Yes	Yes
PA-MC-2T3+	2-port multichannel T3	—	Yes	Yes	Yes
PA-MC-2T1	2-port multichannel T1, integrated CSU/DSUs	—	Yes	Yes	Yes
PA-MC-2E1/120	2-port multichannel E1, G.703 120-ohm interface	—	Yes	Yes	Yes
PA-MC-4T1	4-port multichannel T1, integrated CSU/DSUs	—	Yes	Yes	Yes
PA-MC-8TE1+	8-port multichannel T1/E1 8PRI	—	Yes	Yes	Yes
PA-MC-STM-1MM	1-port multichannel STM-1 multimode	—	Yes	Yes	Yes

Table 3 Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, and Cisco 7304 (continued)

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7304 Router
PA-MC-STM-1SMI	1-port multichannel STM-1 single mode	—	Yes	Yes	Yes
PA-4B-U	4-port BRI, U Interface	—	Yes	Yes	No
PA-8B-S/T	8-port BRI, S/T Interface	—	Yes	Yes	No
Shared Port Adapters (SPAs)					
SPA-4FE-7304	4-port 10/100 Fast Ethernet SPA	—	No	No	Yes
SPA-2GE-7304	2-port 10/100/1000 Gigabit Ethernet SPA	—	No	No	Yes
SPA-2XOC3-POS	2-port OC-3c/STM-1 POS SPA	—	No	No	Yes
SPA-4XOC3-POS	4-port OC-3c/STM-1 POS SPA	—	No	No	Yes
SPA-1OC12-POS	1-port OC-12c/STM-4 POS SPA	—	No	No	Yes
SPA-2XT3/E3	2-port T3/E3 Serial SPA	—	No	No	Yes
SPA-4XT3/E3	4-port T3/E3 Serial SPA	—	No	No	Yes
SONET Port Adapters					
PA-POS-OC3MM	1-port Packet over SONET OC3c/STM1 multimode	—	Yes	Yes	Yes
PA-POS-OC3SMI	1-port Packet over SONET OC3c/STM1 single mode (IR)	—	Yes	Yes	Yes
PA-POS-OC3SML	1-port Packet over SONET OC3c/STM1 single mode (LR)	—	Yes	Yes	Yes
PA-POS-1OC3	1-port OC-3/STM-1 POS (with APS)	12.2(28)SB6	Yes	Yes	Yes[3]
PA-POS-2OC3	2-port OC-3/STM-1 POS (with APS)	—	Yes	Yes	Yes
T1/E1 Port Adapters					
PA-4T+	4-port Serial, Enhanced	—	Yes	Yes	Yes
PA-8T-V35	8-port Serial, V.35	—	Yes	Yes	Yes
PA-8T-X21	8-port Serial, X.21	—	Yes	Yes	Yes
PA-8T-232	8-port Serial, 232	—	Yes	Yes	Yes
T3/E3 Port Adapters					
PA-T3+	1-port T3 Serial, Enhanced	—	Yes	Yes	Yes
PA-2T3+	2-port T3 Serial, Enhanced	—	Yes	Yes	Yes
PA-E3	1-port E3 Serial, E3 DSUs	—	Yes	Yes	Yes
PA-2E3	2-port E3 Serial, E3 DSUs	—	Yes	Yes	Yes

1. For a spare product number, append an equal sign (=) to the product number. For a spare product number, append an equal sign (=) to the product number. If a product number is listed as a spare product in the table, that is, with an equal sign (=), it means that the product is only available as a spare product. For End-of-Sale (EOS) and End-of-Life (EOL) information about port adapters, refer to the Cisco product bulletins at the following locations:
   Cisco 7200 series: http://www.cisco.com/en/US/products/hw/routers/ps341/prod_eol_notices_list.html
   Cisco 7300 series: http://www.cisco.com/en/US/products/hw/routers/ps352/prod_eol_notices_list.html
   Cisco 7400 series: http://www.cisco.com/en/US/products/hw/routers/ps354/prod_eol_notices_list.html

2. Support on the Cisco 7304 was added in both Cisco IOS Release 12.2(28)SB6 and Release 12.2(31)SB2.

3. Support on the Cisco 7200 series and Cisco 7301 was added in Cisco IOS Release 12.2(28)SB6; support on the Cisco 7304 was added in Release 12.2(31)SB2.

For information about troubleshooting port adapters and about alerts, see the Cisco documents at the following location:

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

Supported Line Cards for the Cisco 10000 Series Routers

Table 4 lists the line cards that are supported for the Cisco 10000 series routers in Cisco IOS Release 12.2(28)SB and later releases. The number in the "In" column indicates the Cisco IOS 12.2SB release in which the line card was introduced. For example, (28) means that a line card was introduced in Cisco IOS Release 12.2(28)SB. If a cell in this column contains an em dash (—), support for the line card was inherited from other releases and was included in Cisco IOS Release 12.2(28)SB.

Table 4 Supported Line Cards for the Cisco 10000 Series Router

Common Abbreviation	Cisco Product Number[1]	Line Card Description	In
ATM Line Cards			
1-Port OC-12 ATM	ESR-1OC-12-ATM[2]	1-port OC-12 ATM	—
4-Port OC-3 ATM	ESR-4OC3-ATM-SM	4-port OC-3/STM-1 ATM, single mode	—
4-Port OC-3 ATM LR	ESR-4OC3-ATM-SM-LR	4-port OC-3/STM-1 ATM, long reach	(28)
8-Port E3/DS3 ATM	ESR-8E3/DS3-ATM	8-port E3/DS3 ATM	—
Channelized Line Cards			
1-Port Channelized OC-12/STM-4	ESR-1COC-12/STM-4-SMI[3]	1-port channelized OC-12/STM-4 (STS-12), single mode, intermediate reach	—
	ESR-1COC-12/STM-4-SML	1-port channelized OC-12/STM-4 (STS-12), single mode, long reach	—
4-Port Channelized STM-1/OC-3	ESR-4OC3-ChSTM-1/OC-3	4-port channelized OC-3/STM-1 SDH, single mode	—
4-Port Channelized T3 Half-Height	ESR-HH-4CT3	4-port channelized T3 half-height	(28)
6-Port Channelized T3	ESR-6CT3	6-port channelized T3	—
24-Port T1/E1	ESR-24CT1/E1	24-port channelized E1/T1	—
Electrical Interface Line Card			
8-Port Unchannelized E3/T3	ESR-8E3/DS3	8-port clear channel E3/DS3 line card	—
Ethernet Line Cards			
1-Port GE	ESR-1GE	1-port Gigabit Ethernet	—
1-Port GE Half-Height	ESR-HH-1GE	1-port Gigabit Ethernet half-height	—
8-Port FE Half-Height	ESR-HH-8FE-TX	8-port Fast Ethernet half-height	—
Half-Height Carrier	ESR-HH-CARRIER	Full-length base carrier for half-height line card	—

Table 4 Supported Line Cards for the Cisco 10000 Series Router (continued)

Common Abbreviation	Cisco Product Number[1]	Line Card Description	In
Packet over SONET (POS)/Synchronous Digital Hierarchy (SDH) Line Cards			
1-Port OC-12/STM-4 POS	ESR-1OC-12/P-SMI	1-port OC-12/STS-12c/STM-4 POS/SDH, single mode, intermediate reach	—
	ESR-1OC-12/P-SML	1-port OC-12/STS-12c/STM-4 POS, single mode, long reach	—
1-port OC-48/STM-16 POS	ESR1OC48/P/SRPSMS	1-port OC-48/STM-16 POS/SRP, single mode, short reach	—
	ESR1OC48/P/SRPSML	1-port OC-48/STM-16 POS/SRP, single mode, long reach	—
6-Port OC-3c/STM-1 POS	ESR-6OC3/P-SMI	6-port OC-3c/STS-3c/STM-1 POS/SDH, single mode, intermediate reach	—
	ESR-6OC3/P-SML	6-port OC-3c/STS-3c/STM-1 POS/SDH, single mode, long reach	—

1. For a spare product number, append an equal sign (=) to the product number. If a product number is listed as a spare product in the table, that is, with an equal sign (=), it means that the product is only available as a spare product. For End-of-Sale (EOS) and End-of-Life (EOL) information about line cards, refer to the Cisco product bulletins at the following location: http://www.cisco.com/en/US/products/hw/routers/ps133/prod_eol_notices_list.html
2. The old part number for this line card is ESR-1OC12ATM-SM.
3. The old part number for this line card is ESR-1COC12-SMI.

For information about troubleshooting line cards and about alerts, see the Cisco documents at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps133/tsd_products_support_troubleshoot_and_alerts.html

Determining the Software Version

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

```
Router#> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (rsp-jsv-mz), Version 12.2(31)SB3, 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 7200 series routers, Cisco 7301 router, Cisco 7304 router and Cisco 10000 series routers, see the document at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080094c07.shtml

In addition, for the Cisco 10000 series, see the *Upgrading to Cisco IOS Release 12.2(28)SB on a Cisco 10000 Series Router* document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/upgrade/upgdsb.htm

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 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/fn

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 7304 in Cisco IOS Release 12.2S and consists of the following subsections:

- Bundled FPGAs for the Cisco 7304, page 10
- Shared Port Adapter FPD Image Packages for the Cisco 7304, page 12

Bundled FPGAs for the Cisco 7304

This section provides information about the field-programmable gate array (FPGA) images for the Cisco 7304. These images apply only to the Cisco 7304.

If the versions of the FPGA images that are running on your Cisco 7304 do not match the versions that are bundled in the Cisco IOS software, we recommend that you update your FPGA images. For more details, see the *Cisco 7304 FPGA Bundling and Update* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121ex/121ex10/73fpga.htm

Bundled FPGAs for Cisco IOS Release 12.2(31)SB3

There are no new FPGA images for Cisco IOS Release 12.2(31)SB3. All Cisco IOS Release 12.2(31)SB3 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(31)SB2.

Bundled FPGAs for Cisco IOS Release 12.2(31)SB2

All Cisco IOS Release 12.2(31)SB2 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 5.

Table 5 Bundled FPGA Versions for Cisco IOS Release 12.2(31)SB2 Sorted by Hardware Type

FPGA Image	Hardware Type	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
NSE-100 Motherboard FPGA	0x0001	1.10	2.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.13	4.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.14	5.00	15
NSE-100 Daughterboard FPGA	0x0002	1.07	0.00	6
NSE-100 Daughterboard FPGA	0x0002	1.08	5.00	6
OC-48 POS line card FPGA	0x0003	0.16	2.00	5
OC-3 POS line card FPGA	0x0004	0.22	2.00	8
6E3 line card FPGA	0x0005	0.21	2.00	12
6T3 line card FPGA	0x0005	0.21	2.00	12
OC-12 POS line card FPGA	0x0006	0.20	1.00	12
OC-3 ATM line card FPGA	0x0007	0.19	2.00	8
OC-12 ATM line card FPGA	0x0007	0.19	2.00	8
CC-PA line card FPGA	0x0008	1.40	1.01	8
NPE-G100 FPGA (PS)	0x000A	2.05	0.30	12
NPE-G100 FPGA (ES)	0x000A	2.05	0.20	12
MSC-100 FPGA	0x000D	0.27	0.10	22
NSE-150 FPGA	0x000E	0.08	0.00	12

Bundled FPGAs for Cisco IOS Release 12.2(28)SB6

There are no new FPGA images for Cisco IOS Release 12.2(28)SB6. All Cisco IOS Release 12.2(28)SB6 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(28)SB.

Bundled FPGAs for Cisco IOS Release 12.2(28)SB5

There are no new FPGA images for Cisco IOS Release 12.2(28)SB5. All Cisco IOS Release 12.2(28)SB5 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(28)SB.

Bundled FPGAs for Cisco IOS Release 12.2(28)SB4

There are no new FPGA images for Cisco IOS Release 12.2(28)SB4. All Cisco IOS Release 12.2(28)SB4 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(28)SB.

Bundled FPGAs for Cisco IOS Release 12.2(28)SB3

There are no new FPGA images for Cisco IOS Release 12.2(28)SB3. All Cisco IOS Release 12.2(28)SB3 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(28)SB.

Bundled FPGAs for Cisco IOS Release 12.2(28)SB2

There are no new FPGA images for Cisco IOS Release 12.2(28)SB2. All Cisco IOS Release 12.2(28)SB2 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(28)SB.

Bundled FPGAs for Cisco IOS Release 12.2(28)SB1

There are no new FPGA images for Cisco IOS Release 12.2(28)SB1. All Cisco IOS Release 12.2(28)SB1 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(28)SB.

Bundled FPGAs for Cisco IOS Release 12.2(28)SB

All Cisco IOS Release 12.2(28)SB software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 6.

Table 6 Bundled FPGA Versions for Cisco IOS Release 12.2(28)SB Sorted by Hardware Type

FPGA Image	Hardware Type	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
NSE-100 Motherboard FPGA	0x0001	1.10	2.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.13	4.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.14	5.00	15
NSE-100 Daughterboard FPGA	0x0002	1.07	0.00	6
NSE-100 Daughterboard FPGA	0x0002	1.08	5.00	6
OC-48 POS line card FPGA	0x0003	0.16	2.00	5
OC-3 POS line card FPGA	0x0004	0.22	2.00	8
6E3 line card FPGA	0x0005	0.21	2.00	12
6T3 line card FPGA	0x0005	0.21	2.00	12
OC-12 POS line card FPGA	0x0006	0.20	1.00	12
OC-3 ATM line card FPGA	0x0007	0.19	2.00	8
OC-12 ATM line card FPGA	0x0007	0.19	2.00	8
CC-PA line card FPGA	0x0008	1.40	1.01	8
NPE-G100 FPGA (PS)	0x000A	2.05	0.30	12
NPE-G100 FPGA (ES)	0x000A	2.05	0.20	12
MSC-100 FPGA	0x000D	0.27	0.10	22

Shared Port Adapter FPD Image Packages for the Cisco 7304

Field-programmable device (FPD) image packages are used to update shared port adapter (SPA) FPD images. If a discrepancy exists between an SPA FPD image and the Cisco IOS image that is running on the router, the SPA will be deactivated until this discrepancy is resolved. For additional information on FPDs, including the upgrade process, see the "Upgrading Field-Programmable Devices" section of the *Cisco 7304 Modular Services Card and Shared Port Adapter Software Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspasw/index.htm

Note The maximum time to upgrade the FPD image(s) on one SPA is 2 minutes. The total FPD upgrade time depends on the number of SPAs.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(31)SB3

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(31)SB3 is the c7304-fpd-pkg.122-31.SB3.pkg file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com. The content of this SPA FPD image package is the same as the content of the SPA FPD image package for Release 12.2(31)SB2.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(31)SB2

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(31)SB2 is the c7304-fpd-pkg.122-31.SB2.pkg file. This SPA 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 7 Release 12.2(31)SB2 FPD Image Package Contents

Supported SPAs	FPD ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
7304-4FE-SPA	1	Data & I/O FPGA	4.18	0.0
7304-2GE-SPA	1	Data & I/O FPGA	4.18	0.0
SPA-2XOC3-POS	1	I/O FPGA	3.4	0.0
SPA-4XOC3-POS	1	I/O FPGA	3.4	0.0
SPA-1OC12-POS	1	I/O FPGA	3.4	0.0
SPA-2XT3/E3	1	ROMMON	2.12	0.0
	2	I/O FPGA	0.24	0.0
	3	E3 FPGA	0.6	0.0
	4	T3 FPGA	0.14	0.0
SPA-4XT3/E3	1	ROMMON	2.12	0.0
	2	I/O FPGA	0.24	0.0
	3	E3 FPGA	0.6	0.0
	4	T3 FPGA	0.14	0.0

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(28)SB6

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(28)SB6 is the c7304-fpd-pkg.122-28.SB6.pkg file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com. The content of this SPA FPD image package is the same as the content of the SPA FPD image package for Release 12.2(28)SB.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(28)SB5

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(28)SB5 is the c7304-fpd-pkg.122-28.SB5.pkg file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com. The content of this SPA FPD image package is the same as the content of the SPA FPD image package for Release 12.2(28)SB.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(28)SB4

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(28)SB4 is the c7304-fpd-pkg.122-28.SB4.pkg file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com. The content of this SPA FPD image package is the same as the content of the SPA FPD image package for Release 12.2(28)SB.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(28)SB3

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(28)SB3 is the c7304-fpd-pkg.122-28.SB3.pkg file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com. The content of this SPA FPD image package is the same as the content of the SPA FPD image package for Release 12.2(28)SB.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(28)SB2

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(28)SB2 is the c7304-fpd-pkg.122-28.SB2.pkg file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com. The content of this SPA FPD image package is the same as the content of the SPA FPD image package for Release 12.2(28)SB.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(28)SB1

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(28)SB1 is the c7304-fpd-pkg.122-28.SB1.pkg file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com. The content of this SPA FPD image package is the same as the content of the SPA FPD image package for Release 12.2(28)SB.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(28)SB

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(28)SB is the c7304-fpd-pkg.122-28.SB.pkg file. This SPA 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 8 Release 12.2(28)SB FPD Image Package Contents

Supported SPAs	FPD ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
7304-4FE-SPA	1	Data & I/O FPGA	4.18	0.0
7304-2GE-SPA	1	Data & I/O FPGA	4.18	0.0
SPA-2XOC3-POS	1	I/O FPGA	3.4	0.0
SPA-4XOC3-POS	1	I/O FPGA	3.4	0.0
SPA-1OC12-POS	1	I/O FPGA	3.4	0.0
SPA-2XT3/E3	1	ROMMON	2.12	0.0
	2	I/O FPGA	0.24	0.0
	3	E3 FPGA	0.6	0.0
	4	T3 FPGA	0.14	0.0
SPA-4XT3/E3	1	ROMMON	2.12	0.0
	2	I/O FPGA	0.24	0.0
	3	E3 FPGA	0.6	0.0
	4	T3 FPGA	0.14	0.0

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 12.2SB 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/fn

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 12.2SB 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, choose **12.2SB**.

Step 6 From the Release drop-down menu, choose 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 12.2SB, 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, choose **12.2SB** from the Cisco IOS Major Release drop-down menu.

Step 3 Click **Continue**.

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

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

Step 6 From the Feature Set drop-down menu, choose 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 12.2SB and contains the following subsections:

Note These release notes are not cumulative and list only features that are new to Cisco IOS Release 12.2SB. The parent releases for Release 12.2SB are Release 12.2 and Release 12.2S. For information about inherited features, refer 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/fn.

Note For information about supported platforms, line cards, and port adapters, see the "Supported Hardware" section on page 4.

New Hardware Features in Cisco IOS Release 12.2(31)SB3

There are no new hardware features in Cisco IOS Release 12.2(31)SB3.

New Software Features in Cisco IOS Release 12.2(31)SB3

This section describes new and changed features in Cisco IOS Release 12.2(31)SB3. Some features may be new to Cisco IOS Release 12.2SB 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(31)SB3. 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 below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

Embedded Event Manager (EEM) 2.2

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sb_eem22.htm

IS-IS-MIB

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

QoS: MQC Classification, Policing, and Marking on LAC

Platform: Cisco 10000 series (PRE-2)

Note Support for this feature on the PRE-3 was introduced in Cisco IOS Release 12.2(31)SB2.

For detailed information about this feature, see the "Shaping Traffic" chapter in the *Cisco 10000 Series Router Quality of Service Configuration Guide:*

http://cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008061c374.html#wp1042680

TCP MSS Adjust

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the "Configuring PPPoE over Ethernet and IEEE 802.1Q VLAN" chapter in the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008050578c.html

New Hardware Features in Cisco IOS Release 12.2(31)SB2

This section describes new and changed features in Cisco IOS Release 12.2(31)SB2. Some features may be new to Cisco IOS Release 12.2SB 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(31)SB2. 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 below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

1-Port Enhanced ATM Port Adapter with Support for 8000 VCs

Platform: Cisco 7304 (NSE-100, NSE-150, NPE-G100)

Note Cisco IOS Release 12.2(28)SB introduced support for this port adapter on the Cisco 7200 series and Cisco 7301. Release 12.2(31)SB2 adds support for the Cisco 7304.

Cisco IOS Release 12.2(31)SB2 adds support for the PA-A6 port adapters and support for 8000 virtual circuits (VCs) on PA-A6 port adapters that are installed in the Cisco 7304 router. The PA-A6 is a series of single-width, single-port, ATM port adapters. With advanced ATM features, the PA-A6 port adapters support broadband aggregation, WAN aggregation, and campus/MAN aggregation.

The following PA-A6 port adapters are supported:

- PA-A6-OC3MM: 1-port ATM OC-3c/STM-1 multimode port adapter, enhanced
- PA-A6-OC3SMI: 1-port ATM OC-3c/STM-1 single-mode (IR) port adapter, enhanced
- PA-A6-OC3SML: 1-port ATM OC-3c/STM-1 single-mode (LR) port adapter, enhanced
- PA-A6-T3: 1-port ATM DS3 port adapter, enhanced
- PA-A6-E3: 1-port ATM E3 port adapter, enhanced

For detailed information about these products, see the *PA-A6 Port Adapter Installation and Configuration* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/7206/port_adp/atm_-pas/pa-a6/index.htm

1-Port Packet over SONET OC3c/STM1 Port Adapter

Platform: Cisco 7304 (NSE-100, NSE-150, NPE-G100)

For detailed information about the 1-port Packet over SONET OC3c/STM1 port adapter (PA-POS-1OC3), see the following documents:

- *Cisco 1-Port OC-3/STM-1 Packet-Over-SONET Port Adapter* data sheet:

  http://www.cisco.com/en/US/partner/products/hw/routers/ps341/products_data_sheet0900aecd80221d3d.html

- *PA-POS-1OC3 Single-Port Port Adapter Installation and Configuration Guide*:

  http://www.cisco.com/univercd/cc/td/doc/product/core/7301/73pa/73-son/6514_1oc/index.htm

Network Services Engine 150 (NSE-150)

Platform: Cisco 7304

The NSE-150 is a processor for the Cisco 7304 router. It contains two internal processors for forwarding network traffic: a Parallel eXpress Forwarding (PXF) processor, which accelerates the processing of IP packets for features supported in the PXF processing path; and a Route Processor (RP), which handles all non-IP packets and all packets that are not forwarded using the PXF processing path.

The NSE-150 introduces the following enhancements to the Cisco 7304 router:

- Additional port density through on-board Gigabit Ethernet ports. The NSE-150 has four on-board Gigabit Ethernet ports.
- Improved overall memory for better overall performance (for example, additional DRAM, column memory for PXF, packet memory for the Route Processor, and NVRAM).
- Increased RP and PXF memory to enable more scalability (for the routing table, FIB table, and Turbo ACL).
- Improved processing power for the control plane functions (for example, routing protocols and statistics collection).
- USB ports. Support for USB ports on the NSE-150 will be introduced as an enhancement in a future release of Cisco IOS Release 12.2SB.

For additional information on the NSE-150, see the *Cisco 7304 Network Services Engine Installation and Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/fru/nse/index.htm

NPE-G2 Network Processing Engine

Platform: Cisco 7200VXR series

The Network Processing Engine NPE-G2 is the latest and highest-performing routing engine with the largest scalability within the family of network processing engines for the Cisco 7200VXR series. A new chip design on the NPE-G2 provides up to double the performance of the NPE-G1. This great performance improvement makes the NPE-G2 an ideal solution for the new aggregation services for enterprises and service providers.

The NPE-G2 offers following benefits:

- Provides double the performance compared to the Cisco 7200 VXR series NPE-G1—up to 2 million packets per second (pps) in Cisco Express Forwarding (CEF)
- Offers three 10/100/1000-Mbps copper Ethernet ports and optical ports (10/100/1000 Mbps over copper or 1000 Mbps over industry-standard SFP) for LAN/WAN connectivity
- Provides two USB ports for general storage and security token storage
- Provides one dedicated 10/100-Mbps copper Ethernet port for management
- Offers 1 GB of DRAM memory by default and 2 GB DRAM is available as an option
- Eliminates the requirement for an I/O controller
- Extends the use of the available I/O slot for a single port adapter in combination with the Port Adapter Jacket Card (C7200-JC-PA)
- Offers greatly improved price/performance ratio

Note An I/O controller module can be used with the NPE-G2, but it is not necessary for system functionality. Installing an I/O controller in a Cisco 7200VXR series chassis with the NPE-G2 activates the console and auxiliary ports on the I/O controller and automatically disables the console and auxiliary ports on the NPE-G2. However, you can still use the CompactFlash Disk slots and Ethernet ports on both the NPE-G2 and I/O controller when both cards are installed.

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

- *Cisco 7200VXR NPE-G2 Network Processing Engine* data sheet

  http://www.cisco.com/en/US/products/hw/routers/ps341/products_data_sheet0900aecd8047177b.html

- The "NPE-G2 Overview" chapter of the *Network Processing Engine and Network Services Engine Installation and Configuration* document:

  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/fru/npense/4448o6.htm

- The "NPE-G1 and NPE-G2 Installation and Configuration Information" chapter of the *Network Processing Engine and Network Services Engine Installation and Configuration* document:

  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/fru/npense/4448c6.htm

Performance Routing Engine 3 (PRE-3)

Platform: Cisco 10000 series

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

- *Cisco 10000 Series Performance Routing Engine 3* data sheet:

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_data_sheet0900aecd8049f279.html

- *Cisco 10008 Router Performance Routing Engine 3 Installation* document:

  http://www.cisco.com/en/US/products/hw/routers/ps133/prod_installation_guide09186a008076ffd0.html

Note For the Cisco 10000 series, the PRE-3 supports all features that are supported on the PRE-2 in Cisco IOS Release 12.2(28)SB and Release 12.2(28)SB1. Even though these features are new for the PRE-3 in Cisco IOS Release 12.2(31)SB2, they are not called out in the "New Software Features in Cisco IOS Release 12.2(31)SB2" section to improve the usability of the release notes documentation. For information about these features, see the "New Software Features in Cisco IOS Release 12.2(28)SB" and "New Software Features in Cisco IOS Release 12.2(28)SB2" sections.

Port Adapter Jacket Card for Cisco 7200VXR Series (C7200-JC-PA)

Platform: Cisco 7200 series

The port adapter jacket card for the Cisco 7200VXR series addresses the demand for additional slot density and flexibility by enabling the I/O slot to hold a single port adapter for additional capacity on routers with the Cisco 7200VXR series NPE-G1 or NPE-G2. Benefits of the jacket card include the following:

- Provides one additional slot for a single selected port adapter.
- Allows a high-bandwidth port adapter such as the 2-port OC-3/STM-1 POS port adapter to be moved onto a dedicated Peripheral Component Interconnect (PCI) bus that the NPE-G1 or NPE-G2 provides.
- Reduces PCI contention among other port adapters.
- Provides a cost-effective way to increase the slot density in parallel to the increased switching capacity of the newest engine of the router, the Cisco NPE-G2.

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

- *Cisco 7200VXR Series Port Adapter Jacket Card* data sheet:

  http://www.cisco.com/en/US/products/hw/routers/ps341/products_data_sheet0900aecd804419c6.html

- *Port Adapter Jacket Card Installation Guide*:

  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/72vxfru/8427j.htm

New Software Features in Cisco IOS Release 12.2(31)SB2

This section describes new and changed features in Cisco IOS Release 12.2(31)SB2. Some features may be new to Cisco IOS Release 12.2SB 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(31)SB2. 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 below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

Note For the Cisco 10000 series, the PRE-3 supports all features that are supported on the PRE-2 in Cisco IOS Release 12.2(28)SB and Release 12.2(28)SB1. Even though these features are new for the PRE-3 in Cisco IOS Release 12.2(31)SB2, they are not called out in the "New Software Features in Cisco IOS Release 12.2(31)SB2" section to improve the usability of the release notes documentation. For information about these features, see the "New Software Features in Cisco IOS Release 12.2(28)SB" and "New Software Features in Cisco IOS Release 12.2(28)SB2" sections.

Table 9 lists the features that are supported for the Cisco 10000 series in Cisco IOS Release 12.2(31)SB2 and uses the following conventions:

- Yes—The feature is supported on the PRE-2 and/or PRE-3.
- No—The feature is not supported on the PRE-2 or PRE-3, or the feature is not New.
- New—The feature has never before been released in any public Cisco IOS software image for the Cisco 10000 series; the feature is released for the first time for the Cisco 10000 series in Cisco IOS Release 12.2(31)SB2. (Other features may be new for the Cisco 10000 series in Cisco IOS Release 12.2(31)SB2 but have been released before in other public Cisco IOS software images for the Cisco 10000 series.)

Table 9 Features Introduced for the Cisco 10000 Series in Cisco IOS Release 12.2(31)SB2

Feature Name	PRE-2	PRE-3	New
802.1p COS Bit Set for PPP & PPPoE Control Frames	Yes	Yes	New
AAA High Availability Support for Local PPPoX Sessions	Yes	Yes	New
BGP Features			
• BGP MIB Support Enhancements	Yes	Yes	New
• BGP Selective Address Tracking	Yes	Yes	New
• BGP Support for Fast Peering Session Deactivation	Yes	Yes	New

Table 9 Features Introduced for the Cisco 10000 Series in Cisco IOS Release 12.2(31)SB2 (continued)

Feature Name	PRE-2	PRE-3	New
• BGP Support for Next-Hop Address Tracking	Yes	Yes	New
• BGP Support for TCP Path MTU Discovery per Session	Yes	Yes	New
Calling Station ID Attribute 31	Yes	Yes	New
Cisco Express Forwarding - SNMP CEF-MIB Support	Yes	Yes	New
Cisco MIBs			
• CISCO-IP-URPF-MIB Support	Yes	Yes	New
• CISCO-NETFLOW-MIB	Yes	Yes	New
• CISCO-QINQ-VLAN-MIB	Yes	Yes	New
Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)	Yes	Yes	New
CNS - Image Agent	Yes	Yes	New
Configuration Replace and Configuration Rollback	Yes	Yes	New
Control Plane Policing (CPP)	Yes	Yes	New
Control Plane Policing - Time Based	Yes	Yes	New
DHCP Relay Option 82 - Per Interface Support	Yes	Yes	New
Dynamic Bandwidth Selection—ATM VC Weights Attribute Specification	Yes	Yes	No
Fast EtherChannel [Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces]	Yes	Yes	New
FHRP - Object Tracking List	Yes	Yes	New
Frame Relay - Multilink (MLFR-FRF.16)	No	Yes	New
IEEE 802.3ad, Link Aggregation Control Protocol	Yes	Yes	New
In-Service Software Upgrade Features			
• ISSU - DHCP ODAP Client/Server	Yes	Yes	New
• ISSU - DHCP Proxy Client	Yes	Yes	New
• ISSU - DHCP Relay on Unnumbered Interface	Yes	Yes	New
• ISSU - DHCP Server	Yes	Yes	New
• ISSU - GLBP	Yes	Yes	New
• ISSU - IS-IS	Yes	Yes	New
• ISSU - PPPoA	Yes	Yes	New
• ISSU - PPPoE	Yes	Yes	New
• ISSU - Remote Access to MPLS VPN	Yes	Yes	New
Intelligent Service Gateway Features			
• ISG: Accounting: Postpaid	Yes	Yes	New
• ISG: Accounting: Prepaid	Yes	Yes	New
• ISG: Accounting: Tariff Switching	Yes	Yes	New
• ISG: Instrumentation: Session and Flow Monitoring (Local and External)	Yes	Yes	New

Table 9 Features Introduced for the Cisco 10000 Series in Cisco IOS Release 12.2(31)SB2 (continued)

Feature Name	PRE-2	PRE-3	New
• ISG: Policy Control: DHCP Proxy	Yes	Yes	New
• ISG: Policy Control: Policy Server: CoA ASCII Command Code Support	Yes	Yes	New
• ISG: Policy Control: Policy: Triggers (Time, Volume, Duration)	Yes	Yes	New
• ISG: Session: Authentication (MAC, IP, EAP)	Yes	Yes	New
• ISG: Session: Creation: Interface IP Session: L2	Yes	Yes	New
• ISG: Session: Creation: Interface IP Session: L3	Yes	Yes	New
• ISG: Session: Creation: IP Session: Protocol Event (DHCP, RADIUS)	Yes	Yes	New
• ISG: Session: Creation: IP Session: Subnet & Source IP: L2	Yes	Yes	New
• ISG: Session: Creation: IP Session: Subnet & Source IP: L3	Yes	Yes	New
• ISG: Session: VRF Transfer	Yes	Yes	New
IP Options Selective Drop	Yes	Yes	New
IP SLAs Features			
• IP SLAs - DHCP Operation	Yes	Yes	No
• IP SLAs - Distribution of Statistics	Yes	Yes	No
• IP SLAs - DNS Operation	Yes	Yes	No
• IP SLAs - FTP Operation	Yes	Yes	No
• IP SLAs - HTTP Operation	Yes	Yes	No
• IP SLAs - ICMP Echo Operation	Yes	Yes	No
• IP SLAs - ICMP Path Echo Operation	Yes	Yes	No
• IP SLAs - LSP Health Monitor with LSP Discovery	Yes	Yes	New
• IP SLAs - MPLS VPN Aware	Yes	Yes	No
• IP SLAs - Multi-Operation Scheduler	Yes	Yes	No
• IP SLAs - One-way Measurements	Yes	Yes	No
• IP SLAs - Path Jitter	Yes	Yes	No
• IP SLAs - Reaction Threshold	Yes	Yes	No
• IP SLAs - Scheduling	Yes	Yes	No
• IP SLAs - TCP Connect Operation	Yes	Yes	No
• IP SLAs - UDP Echo Operation	Yes	Yes	No
• IP SLAs - UDP Jitter Operation	Yes	Yes	No
• IP SLAs - UDP VoIP Operation	Yes	Yes	No
• IP SLAs - VoIP Threshold Traps	Yes	Yes	No
IPv6 Hardware: PxF Accelerated for IPv6 over MPLS (6PE)	Yes	Yes	New
IPv6 MIBs	Yes	Yes	New
L2TP Calling Station ID Suppression	Yes	Yes	New

Table 9 Features Introduced for the Cisco 10000 Series in Cisco IOS Release 12.2(31)SB2 (continued)

Feature Name	PRE-2	PRE-3	New
L2TP Domain Screening	Yes	Yes	No
L2VPN Interworking: Ethernet to VLAN Interworking	Yes	Yes	New
Lawful Intercept Enhancements	Yes	Yes	New
MPLS Features			
• MPLS Embedded Management - LSP Ping/Traceroute for LDP	Yes	Yes	No
• MPLS Embedded Management - MPLS Multipath LSP Traceroute	Yes	Yes	New
• MPLS PE-to-PE Traffic Statistics for NetFlow	Yes	Yes	New
• MPLS Traffic Engineering MIB	Yes	Yes	No
• MPLS VPN MIB v05 - Trap Enhancements	Yes	Yes	New
• MPLS VPN - VRF Selection Based on Source IP Address	Yes	Yes	New
MQC Features			
• MQC - Distribution of Remaining Bandwidth via Ratio	No	Yes	New
• MQC - Hierarchical Queuing with 3 Level Scheduler	No	Yes	New
• MQC - Multi-Level Priority Queues	No	Yes	New
• MQC - Traffic Shaping Overhead Accounting for ATM	No	Yes	New
Multicast VPN Extranet Support	Yes	Yes	New
Multicast VPN Extranet VRF Select	Yes	Yes	New
Multiclass Multilink PPP Enhancement	Yes	No	New
NAS-Port ID Format C Enhancement	Yes	Yes	New
NetFlow Features			
• NetFlow Export of BGP Nexthop Information	Yes	Yes	New
• NetFlow MPLS Aggregation	Yes	Yes	New
• Random Sampled NetFlow	Yes	Yes	New
OSPF Features			
• NSF - OSPF RFC 3623 Graceful Restart	Yes	Yes	New
• OSPF MIB Support of RFC 1850 and Latest Extensions	Yes	Yes	New
• OSPF Sham-Link MIB Support	Yes	Yes	New
Persistent Storage	No	Yes	New
Per-VRF Assignment of BGP Router ID	Yes	Yes	New
PPP-Max-Payload and IWF PPPoE Tag Support	Yes	Yes	New
PPPoE Features			
• PPPoE Agent Remote ID & DSL Line Characteristics Enhancement	Yes	Yes	New
• PPPoE QinQ Support	Yes	Yes	New
• PPPoE Session Limiting on Inner QinQ VLAN	Yes	Yes	New
PXF-Based Frame Relay DE Bit Marking	Yes	Yes	New

Table 9 Features Introduced for the Cisco 10000 Series in Cisco IOS Release 12.2(31)SB2 (continued)

Feature Name	PRE-2	PRE-3	New
QoS Features			
• QoS: CBQoS Management - Policy-to-Interface Mapping Support	Yes	Yes	New
• QoS: CBQoS MIB Index Enhancements	Yes	Yes	New
• QoS Child Service Policy for Priority Class	No	Yes	New
• QoS: Classification, Policing, and Marking on LAC	No	Yes	New
• QoS - Hierarchical Queuing for Ethernet DSLAMs	No	Yes	New
• QoS: Match VLAN	Yes	Yes	New
• QoS - Percentage-Based Shaping	Yes	Yes	New
• QoS - Policing Support for GRE Tunnels	Yes	Yes	New
• QoS Priority Propagation in Multi-level Scheduler	No	Yes	New
• QoS - VLAN Tag Based	Yes	Yes	New
SNMP - Session to Interface Mapping Improvements	Yes	Yes	New
SNMP Support for VPNs	Yes	Yes	New
Stateful Switchover Features			
• SSO - DHCP ODAP Client/Server	Yes	Yes	New
• SSO - DHCP Proxy Client	Yes	Yes	New
• SSO - DHCP Relay on Unnumbered Interface	Yes	Yes	New
• SSO - DHCP Server	Yes	Yes	New
• SSO - GLBP	Yes	Yes	New
• SSO - Multilink Frame Relay	No	Yes	New
• SSO - PPPoA	Yes	Yes	New
• SSO - PPPoE	Yes	Yes	New
• SSO - Remote Access to MPLS VPN	Yes	Yes	New
Static MAC Address for PPPoE	Yes	Yes	No
VRF-Aware System Message Logging (Syslog)	Yes	Yes	New
VRF-Aware VPDN Tunnels	Yes	Yes	New
Weighted Random Early Detection Improvements	Yes	Yes	New

Table 10 shows how select features for the Cisco 7304 are supported and uses the following conventions:

- Yes—The feature is supported on the engine and/or in the PXF path.
- No—The feature is not supported on the engine and/or in the PXF path.

Table 10 Features Supported on the Cisco 7304 Engines and in the PXF Path

Feature	NSE-100	NSE-150	NPE-G100	Support in the PFX Path
BGP Features				
• BGP MIB Support Enhancements	Yes	Yes	Yes	No
• BGP Multicast Inter-AS (IAS) VPN	Yes	Yes	Yes	No
• BGP Selective Address Tracking	Yes	Yes	Yes	No
• BGP Support for Fast Peering Session Deactivation	Yes	Yes	Yes	No
• BGP Support for Next-Hop Address Tracking	Yes	Yes	Yes	No
• BGP Support for TCP Path MTU Discovery per Session	Yes	Yes	Yes	No
Cisco Express Forwarding - SNMP CEF-MIB Support	Yes	Yes	Yes	No
CISCO-IP-URPF-MIB Support	Yes	Yes	Yes	No
CISCO-NETFLOW-MIB	No	No	Yes	No
Clear IP Traffic CLI	Yes	Yes	Yes	No
CNS-Image Agent	Yes	Yes	Yes	No
Configuration Replace and Configuration Rollback	Yes	Yes	Yes	No
DHCP Relay Option 82 - Per Interface Support	Yes	Yes	Yes	No
Fast EtherChannel	Yes	Yes	Yes	Yes
FHRP - Object Tracking List	Yes	Yes	Yes	No
Gigabit EtherChannel	Yes	Yes	Yes	Yes
ICMP Unreachable Rate Limiting User Feedback	Yes	Yes	Yes	No
IEEE 802.1p Support	Yes	Yes	No	Yes
IP SLAs Features	Yes	Yes	Yes	No
IPv6 MIBs	Yes	Yes	Yes	No
Modular QoS CLI-Based Classification for Layer 2 Frames in PXF	Yes	Yes	No	Yes
MPLS Features				
• MPLS Embedded Management - LSP Ping/Traceroute for LDP	Yes	Yes	Yes	No
• MPLS Embedded Management - MPLS Multipath LSP Traceroute	Yes	Yes	Yes	No
• MPLS Traffic Engineering (TE) MIB	Yes	Yes	Yes	No
• MPLS VPN MIB v05 - Trap Enhancements	Yes	Yes	Yes	No
Multicast VPN Extranet Support	No	No	Yes	No

Table 10 Features Supported on the Cisco 7304 Engines and in the PXF Path (continued)

Feature	NSE-100	NSE-150	NPE-G100	Support in the PFX Path
Multicast VPN Inter-AS Support	Yes	Yes	Yes	No
NAT - Integration with MPLS VPNs	Yes	Yes	Yes	Yes
NetFlow Features				
• Flexible NetFlow	No	No	Yes	No
• NetFlow Egress Accounting	Yes	Yes	No	No
• NetFlow MPLS Aggregation	Yes	Yes	Yes	No
OSPF Features				
• NSF - OSPF RFC 3623 Graceful Restart	Yes	Yes	Yes	No
• OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3	Yes	Yes	Yes	No
• OSPF MIB Support of RFC 1850 and Latest Extensions	Yes	Yes	Yes	No
• OSPF Sham-Link MIB Support	Yes	Yes	Yes	No
• OSPF SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields	Yes	Yes	Yes	No
Per-VRF Assignment of BGP Router ID	Yes	Yes	Yes	No
QoS: CBQoS Management - Policy-to-Interface Mapping Support	Yes	Yes	Yes	No
QoS: CBQoS MIB Index Enhancements	Yes	Yes	Yes	No
Rate-Based Satellite Control Protocol (RBSCP)	Yes	Yes	Yes	No
SFP Security Verification	Yes	Yes	Yes	No
SNMP - Session to Interface Mapping Improvements	Yes	Yes	Yes	No
SSO-GLBP	No	No	Yes	No
Transmission Control Protocol Features	Yes	Yes	Yes	No
Turbo ACL Scalability Enhancements (Phase II)	Yes	Yes	No	Not applicable[1]
VRF-Aware System Message Logging (Syslog)	Yes	Yes	Yes	No

1. The Turbo ACL Scalability Enhancements (Phase II) feature consists of an internal enhancement that accelerates the removal of memory within the PXF path and a functionality that sets memory limits on the Route Processor (RP) path.

802.1p COS Bit Set for PPP and PPPoE Control Frames

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-2 and PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sb8021p2.htm

AAA High Availability Support for Local PPPoX Sessions

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

BGP Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following Border Gateway Protocol (BGP) features.

BGP MIB Support Enhancements

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/fs_bmibe.htm

BGP Multicast Inter-AS (IAS) VPN

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

BGP Selective Address Tracking

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

BGP Support for Fast Peering Session Deactivation

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

BGP Support for Next-Hop Address Tracking

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

BGP Support for TCP Path MTU Discovery per Session

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

Calling Station ID Attribute 31

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-2 and PRE-3)

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 first 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

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

Cisco MIBs

Cisco IOS Release 12.2(31)SB2 and later releases support the following Cisco MIBs.

CISCO-IP-URPF-MIB Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

CISCO-NETFLOW-MIB

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

- *Cisco 7200 Series Router MIB Specifications Guide*

  http://www.cisco.com/en/US/products/hw/routers/ps341/products_technical_reference_book09186a0080787cee.html
- *Cisco 7301 Router MIB Specifications Guide*

  http://www.cisco.com/en/US/products/hw/routers/ps352/products_technical_reference_book09186a00807837b7.html
- *Cisco 7304 Router MIB Specifications Guide*

  http://www.cisco.com/en/US/products/hw/routers/ps352/products_mib_quick_reference_book09186a00807811d3.html
- *Cisco 10000 Series Router Broadband MIB Specifications Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/mibs/bbgv4a/10kmib4a.pdf

CISCO-QINQ-VLAN-MIB

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *Cisco 10000 Series Router Broadband MIB Specifications Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/mibs/bbgv4a/10kmib4a.pdf

Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the following chapters in the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

- Chapter 2, "Classifying Traffic"

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008061c2e0.html

- Chapter 7, "Marking Traffic"

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008061c35e.html

Clear IP Traffic CLI

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

CNS - Image Agent

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

Configuration Replace and Configuration Rollback

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtrollbk.htm

Control Plane Policing (CPP)

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

Control Plane Policing - Time Based

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

DHCP Relay Option 82 - Per Interface Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *DHCP Option 82 per Interface Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/htdhopt8.htm

Dynamic Bandwidth Selection—ATM VC Weights Attribute Specification

Platform: Cisco 10000 series (PRE-2 and PRE-3)

The Dynamic Bandwidth Selection—ATM VC Weights Attribute Specification feature enables broadband customers to configure session bandwidth dynamically. The Cisco 10000 series router offers a dynamic quality of service (QoS) model that enables you to download QoS parameters from a RADIUS server to an ATM virtual circuit (VC).

This feature enables wholesale service providers to sell different levels of service to retail service providers, based on the bandwidth of the ATM VC connection. The retail service provider can then offer subscribers the ability to choose services with varying levels of bandwidth allocation. If a subscriber changes services, the service provider can dynamically change the ATM shaping on the VC based on the RADIUS profile of the subscriber. RADIUS accounting mechanisms control billing for the different services. An extension to Dynamic Bandwidth Selection (DBS) provides the ability to modify an existing VC weight and watermark values using a RADIUS pull model in which the subscriber triggers the parameter changes. The DBS Extensions—VC Weight and Watermark feature enables the modification of existing VC weight and watermark values without tearing down and recreating the VC.

On a RADIUS server, this feature allows VC weight and watermark parameters to be applied (through RADIUS pull) and installed or modified by specific events (through RADIUS push) while the session remains active. Any changes to these VC parameters configured using the Modular QoS CLI (MQC) affect only the NVGEN values and not the RADIUS-pulled values.

For detailed information about this feature, see the following chapters in the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

- “Configuring Dynamic Subscriber Services”

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008061c371.html
- “Distributing Bandwidth Between Queues”

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008061c2de.html
- “Shaping Traffic”

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008061c374.html

Fast EtherChannel and Gigabit EtherChannel Features

The following Fast EtherChannel (FEC) and Gigabit EtherChannel (GEC) features are supported in Cisco IOS Release 12.2(31)SB2.

Fast EtherChannel

Platform: Cisco 7304

This Fast EtherChannel (FEC) feature introduces Fast EtherChannel support for the Cisco 7304 router. This support is introduced for a Cisco 7304 router that uses an NSE-100, NSE-150, or NPE-G100. Fast EtherChannel bundles are PXF-accelerated for the NSE-100 and the NSE-150.

Additionally, PXF-acceleration for QoS rate limiting of Fast EtherChannel bundles is also introduced as part of this feature. Because this portion of the feature is PXF-related, it applies only to the NSE-100 and the NSE-150.

For additional information about Fast EtherChannels on the Cisco 7304 router, see *Cisco 7304 Router Fast EtherChannel and Gigabit EtherChannel Notes*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/7304swf/7304eth.htm

For additional information about PXF, see the *PXF Information for the Cisco 7304 Router* document:

http://www.cisco.com/en/US/products/hw/routers/ps352/prod_maintenance_guide09186a008057410a.html

Gigabit EtherChannel

Platform: Cisco 7304

This Gigabit EtherChannel (GEC) feature introduces Gigabit EtherChannel support for the Cisco 7304 router. This support is introduced for a Cisco 7304 router that uses an NSE-100, NSE-150, or NPE-G100. Gigabit EtherChannel bundles are PXF-accelerated for the NSE-100 and the NSE-150.

Additionally, PXF-acceleration for QoS rate limiting of Gigabit EtherChannel bundles is also introduced as part of this feature. Because this portion of the feature is PXF-related, it applies only to the NSE-100 and the NSE-150.

For additional information about Gigabit EtherChannels on the Cisco 7304 router, see *Cisco 7304 Router Fast EtherChannel and Gigabit EtherChannel Notes*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/7304swf/7304eth.htm

For additional information about PXF, see the *PXF Information for the Cisco 7304 Router* document:

http://www.cisco.com/en/US/products/hw/routers/ps352/prod_maintenance_guide09186a008057410a.html

Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces

Platform: Cisco 10000 series (PRE-2 and PRE3)

For detailed information about this feature, which for the Cisco 10000 series is also known as the Fast EtherChannel (FEC) feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/10gigeth.htm

FHRP - Object Tracking List

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE3)

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

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

Field-Programmable Device Upgrades

Platform: Cisco 7200 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xd4/fpd.htm

Frame Relay - Multilink (MLFR-FRF.16)

Platform: Cisco 10000 series (PRE-3)

For detailed information about this feature, see the *Multilink Frame Relay (FRF.16)* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs_mfr.htm

HTTP 1.1 Web Server and Client

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sb_http1.htm

ICMP Unreachable Rate Limiting User Feedback

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

For detailed information about this feature, see the *Configuring IP Services* document:

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

IEEE 802.1p Support

Platform: Cisco 7304

The IEEE 802.1p Support feature introduces IEEE 801.p support, which is also referred to as Class of Service (CoS) Value Marking in some Cisco documentation, in the PXF processing path for a Cisco 7304 router that uses an NSE-100 or an NSE-150.

Marking a packet with a local CoS value enables users to associate a Layer 2 CoS value with a packet. The value can then be used to classify packets based on user-defined requirements. Layer 2 to Layer 3 mapping can also be configured by matching on the CoS value, because switches already have the capability to match and set CoS values. If a packet that needs to be marked to differentiate user-defined quality of service (QoS) services is leaving a router and entering a switch, the router should set the CoS value of the packet, because the switch can process the Layer 2 CoS header marking.

There are two ways to configure marking of packets using the CoS value. The first method is configuring the **set cos** command in the Modular QoS CLI and marking CoS values based on user-defined criteria. The second method is using the **set-cos-transmit** option in the **police** command.

For additional information about IEEE 802.1p, see the *Class-Based Marking* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/cbpmark2.htm

For additional information about PXF, see the *PXF Information for the Cisco 7304 Router* document:

http://www.cisco.com/en/US/products/hw/routers/ps352/prod_maintenance_guide09186a008057410a.html

IEEE 802.3ad, Link Aggregation Control Protocol

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *IEEE 802.3ad Link Bundling* document:

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

In-Service Software Upgrade Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following In-Service Software Upgrade (ISSU) features.

ISSU - DHCP Features

Platform: Cisco 10000 series (PRE-2 and PRE-3)

Cisco IOS Release 12.2(31)SB2 and later releases support the following ISSU - Dynamic Host Configuration Protocol (DHCP) features.

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

ISSU - GLBP

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

ISSU - IS-IS

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

ISSU - PPPoA

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *Cisco IOS Broadband High Availability In-Service Software Upgrade* document:

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

ISSU - PPPoE

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *Cisco IOS Broadband High Availability In-Service Software Upgrade* document:

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

ISSU - Remote Access to MPLS VPN

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *Cisco IOS Broadband High Availability In-Service Software Upgrade* document:

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

Intelligent Service Gateway Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following Intelligent Service Gateway (ISG) features:

- ISG: Accounting: Postpaid
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Accounting: Prepaid
  Platform: Cisco 10000 series (PRE-2 and PRE-3)

  Note Cisco IOS Release 12.2(28)SB introduced support for the ISG: Accounting: Time-Based Prepaid feature; Release 12.2(31)SB2 adds support for the ISG: Accounting: Volume-Based Prepaid feature.

- ISG: Accounting: Tariff Switching
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Instrumentation: Session and Flow Monitoring (Local and External)
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Policy Control: DHCP Proxy
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Policy Control: Policy Server: CoA ASCII Command Code Support
  Platforms: Cisco 7200 series, Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Policy Control: Policy: Triggers (Time, Volume, Duration)
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Policy Control: RADIUS Proxy Enhancement
  Platforms: Cisco 7200 series, Cisco 7301

- ISG: Session: Authentication (MAC, IP, EAP)
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Session: Creation: Interface IP Session: L2
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Session: Creation: Interface IP Session: L3
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Session: Creation: IP Session: Protocol Event (DHCP, RADIUS)
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Session: Creation: IP Session: Subnet & Source IP: L2
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Session: Creation: IP Session: Subnet & Source IP: L3
  Platform: Cisco 10000 series (PRE-2 and PRE-3)
- ISG: Session: VRF Transfer
  Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about these features, see the following Cisco documents:

- *Cisco IOS Intelligent Service Gateway Configuration Guide, Release 12.2SB*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/cg/isg_lib/isg_c/index.htm
- *Cisco IOS ISG Command Reference, Release 12.2SB*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/cr/isg_r/index.htm

IP Options Selective Drop

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the "Protecting the Router from DoS Attacks" chapter in the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

IP SLAs Features

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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(31)SB2 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 - LSP Health Monitor with LSP Discovery
- 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

For detailed information about the IP SLAs - LSP Health Monitor with LSP Discovery feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sb2pdisc.htm

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

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/cr/sla_r/index.htm

IPv6 Hardware: PxF Accelerated for IPv6 over MPLS (6PE)

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *Cisco 10008 Router Performance Routing Engine 3 Installation* document:

http://www.cisco.com/en/US/products/hw/routers/ps133/prod_installation_guide09186a008076ffd0.html

IPv6 MIBs

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the “MIBs” section in the “Implementing IPv6 Addressing and Basic Connectivity” chapter of the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/v6addres.htm#wp1032445

IS-IS MIB

Platform: Cisco 7200 series

For detailed information about this feature, see the *IS-IS MIB Support* document:

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

L2VPN Interworking: Ethernet to VLAN Interworking

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the "Configuring Any Transport over MPLS" chapter of the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/atom.htm

Lawful Intercept Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following Lawful Intercept features:

Lawful Intercept Enhancements

Platform: Cisco 10000 series (PRE-2 and PRE-3)

In addition to support for the Lawful Intercept feature on the PRE-3, the following enhancements are introduced for the Lawful Intercept feature in Cisco IOS Release 12.2(31)SB2:

- The new CISCO-USER-CONNECTION-TAP-MIB that supports RADIUS-based user connection intercepts
- Support for lawful intercepts when Routed Bridged Encapsulation (RBE) is configured on the router (RFC 1483)
- VRF-aware IP taps via the citapStream VRF OID in the CISCO-IP-TAP-MIB
- PRE-2 and PRE-3 Layer 3 intercepts that are processed by the Parallel eXpress Forwarding (PXF) engine

For detailed information about the Lawful Intercept feature, see the *Cisco 10000 Series Router Lawful Intercept Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/10lawint.pdf

Service Independent Intercept Architecture: SNMP-Based Lawful Intercept

Platforms: Cisco 7200 series, Cisco 7301

Note For the Cisco 7200 series, SNMP-Based Lawful Intercept is supported only on Cisco 7200 VXR routers that are configured with an NPE-225, NPE-400, NPE-G1, or NPE-G2.

Note RADIUS-Based Lawful Intercept was introduced in Cisco IOS Release 12.2(28)SB for the Cisco 7200 series and Cisco 7301.

SNMP-Based Lawful Intercept, which is a Layer 3 feature (that is, a feature at the IP level), is based on SNMPv3. The following MIBs are supported for SNMP-Based Lawful Intercept:

- CISCO-IP-TAP-MIB
- CISCO-IP-TAP2-MIB
- CISCO-USER-CONNECTION-TAP-MIB

For detailed information about the Service Independent Intercept (SII) architecture, see the *Service Independent Intercept* document:

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

Layer 2 Tunnel Protocol Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following Layer 2 Tunnel Protocol (L2TP) features.

L2TP Calling Station ID Suppression

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-2 and PRE-3)

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

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

L2TP Domain Screening

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-2 and PRE-3)

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

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

L2TP Tunnel Selection Load Balancing with Random Algorithm

Platforms: Cisco 7200 series, Cisco 7301

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

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

MPLS Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following Multiprotocol Label Switching (MPLS) features.

MPLS Embedded Management - LSP Ping/Traceroute for LDP

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/ht_lspng.htm

MPLS Embedded Management - MPLS Multipath LSP Traceroute

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

MPLS Traffic Engineering (TE) MIB

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

Note This feature was introduced in Cisco IOS Release 12.2(28)SB2 for the Cisco 10000 series.

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/temib2.htm

MPLS VPN MIB v05 - Trap Enhancements

Platforms: Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

Note This feature was introduced in Cisco IOS Release 12.2(28)SB for the Cisco 7200 series and Cisco 7301.

For detailed information about this feature, see the *MPLS VPN—MIB Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsvnmb25.htm

MPLS VPN - VRF Selection Based on Source IP Address

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sz/12214sz/122szvrf.htm

MQC Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following Modular QoS CLI (MQC) features.

Modular QoS CLI-Based Classification for Layer 2 Frames in PXF

Platform: Cisco 7304

The Modular QoS CLI-Based Classification for Layer 2 Frames in PXF feature enables Parallel eXpress Forwarding (PXF) acceleration of various **match** commands in the Modular QoS CLI (MQC) to classify Layer 2 packets for Cisco 7304 routers that use an NSE-100 or an NSE-150.

Specifically, classification of the matching of the following packets is PXF-accelerated as a result of this feature:

- VLAN ID (**match-vlan**)
- Class of Service bit (**match cos**)
- Input interface (**match input-interface**)
- Frame Relay DLCI (**match fr-dlci**)
- Frame Relay Discard Eligibility (**match fr-de**)

For more information, see the following documents:

- For general information about how **match** commands are used in the MQC, see the "Modular Quality of Service Command-Line Interface" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt8/index.htm

- For additional information about the **match cos**, **match fr-dlci**, and **match input-interface** commands, see "Quality of Service Commands: M through N" chapter in the *Cisco IOS Quality of Service Solutions Command Reference, Release 12.4T.*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tqos_r/qos_m1ht.htm

- For additional information about the **match-vlan** command, see the "match vlan" section in the *Quality of Service on Aggregate VLAN Traffic Contents* document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/aggvlan.htm#1041050

- For additional information about the **match fr-de** command, see "match fr-de" section of the *QoS: Tunnel Marking for L2TPv3 Tunnels* document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12stnlmk.htm#wp1100535

- For additional information about PXF, see the *PXF Information for the Cisco 7304 Router* document:

  http://www.cisco.com/en/US/products/hw/routers/ps352/prod_maintenance_guide09186a008057410a.html

MQC - Distribution of Remaining Bandwidth via Ratio

Platform: Cisco 10000 series (PRE-3)

For detailed information about this feature, see the *Distribution of Remaining Bandwidth Using Ratio* document:

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

MQC - Hierarchical Queuing with 3 Level Scheduler

Platform: Cisco 10000 series (PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/3lvlschd.htm

MQC - Multi-Level Priority Queues

Platform: Cisco 10000 series (PRE-3)

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

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

MQC - Traffic Shaping Overhead Accounting for ATM

Platform: Cisco 10000 series (PRE-3)

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

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

Multicast VPN

Cisco IOS Release 12.2(31)SB2 and later releases support the following multicast Virtual Private Network (VPN) features.

Multicast VPN Extranet Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *Configuring Multicast VPN Extranet Support* document:

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

Multicast VPN Extranet VRF Select

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

Multicast VPN Inter-AS Support

Platforms: Cisco 7200 series, Cisco 7304

For detailed information about this feature, see the *Configuring Multicast VPN Inter-AS Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/iasmcvpn.htm

Multiclass Multilink PPP Enhancement

Platform: Cisco 10000 series (PRE-2)

Prior to Cisco IOS Release 12.2(31)SB2, the Multiclass Multilink PPP (MC-MLP) feature provided support for 16 reassembly classes by the receive logic, but only 2 classes were supported for transmit logic. Beginning with Cisco IOS Release 12.2(31)SB2, MC-MLP provides expanded support to include 4 classes for transmit logic on the Cisco 10000 series.

For detailed information about Multiclass Multilink PPP feature, see the following Cisco document:

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

NAS-Port ID Format C Enhancement

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-2 and PRE-3)

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

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

NAT - Integration with MPLS VPNs

Platform: Cisco 7304

The NAT - Integration with MPLS VPNs feature functions for a Cisco 7304 router that uses an NSE-100, NSE-150, or NPE-G100. The NAT - Integration with MPLS VPNs feature is PXF-accelerated on a Cisco 7304 router that uses an NSE-100 or NSE-150.

Network Address Translation (NAT) allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local (or private) network. Although NAT systems can provide broad levels of security advantages, their main objective is to economize on address space.

NAT allows organizations to resolve the problem of IP address depletion when they have existing networks and need to access the Internet. Sites that do not yet possess network interface card (NIC)-registered IP addresses must acquire them. Cisco IOS NAT eliminates concern and bureaucratic delay by dynamically mapping thousands of hidden internal addresses to a range of easy-to-get addresses.

In general, a NAT system makes it more difficult for an attacker to determine the following:

- Number of systems running on a network
- Type of machines and operating systems that they are running
- Network topology and arrangement

NAT integration with Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) allows multiple MPLS VPNs to be configured on a single device to work together. NAT can differentiate which MPLS VPN it receives IP traffic from even if the MPLS VPNs are all using the same IP addressing scheme. This enables multiple MPLS VPN customers to share services while ensuring that each MPLS VPN is completely separate from the other.

For additional information on this feature, see the *NAT Integration with MPLS VPNs* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftnatvpn.htm

For additional information about PXF, see the *PXF Information for the Cisco 7304 Router* document:

http://www.cisco.com/en/US/products/hw/routers/ps352/prod_maintenance_guide09186a008057410a.html

NetFlow Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following NetFlow features.

Flexible NetFlow

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

NetFlow Egress Accounting

Platform: Cisco 7304

The NetFlow Egress Accounting feature introduces egress NetFlow accounting in the Parallel eXpress Forwarding (PXF) processing path for a Cisco 7304 router that uses an NSE-100 or NSE-150.

The NetFlow Egress Accounting feature enables you to capture IP flow information for packets that undergo Multiprotocol Label Switching (MPLS) label disposition; that is, packets that arrive on a router as MPLS packets and are transmitted as IP packets. It also allows the router to capture IP information for packets that arrive on a router as IP packets and leave that router as an IP packet.

This feature enables service providers to compute MPLS core traffic matrices and better manage network traffic patterns.

For more information, see the following documents:

- For additional information on egress NetFlow accounting, see the *MPLS Egress NetFlow Accounting* document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/egress.htm

- For additional information about PXF, see the *PXF Information for the Cisco 7304 Router* document:

  http://www.cisco.com/en/US/products/hw/routers/ps352/prod_maintenance_guide09186a008057410a.html

NetFlow Export of BGP Nexthop Information

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

NetFlow MPLS Aggregation

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, which is also known for the Cisco 10000 series as the MPLS PE-to-PE Traffic Statistics for NetFlow feature, see the following Cisco document:

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

Random Sampled NetFlow

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

OSPF Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following Open Shortest Path First (OSPF) features.

NSF - OSPF RFC 3623 Graceful Restart

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s32/gr_ospf.htm

OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3

Platforms: Cisco 7200 series, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/htostats.htm

OSPF MIB Support of RFC 1850 and Latest Extensions

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/fsmibos.htm

OSPF Sham-Link MIB Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/ospfslms.htm

OSPF SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields

Platforms: Cisco 7200 series, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/ht_ifndx.htm

Persistent Storage

Platform: Cisco 10000 series (PRE-3)

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

Per-VRF Assignment of BGP Router ID

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

PPP-Max-Payload and IWF PPPoE Tag Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-2 and PRE-3)

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

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

PPPoE Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following PPP over Ethernet (PPPoE) features.

PPPoE Agent Remote ID & DSL Line Characteristics Enhancement

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-2 and PRE-3)

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

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

PPPoE QinQ Support

Platforms: Cisco 7200 series, Cisco 10000 series (PRE-2 and PRE-3)

Note This feature was introduced in Cisco IOS Release 12.2(28)SB2. Release 12.2(31)SB2 adds support for IP over Q-in-Q (IPoQ-in-Q).

For detailed information about this feature, which is also known as the IEEE 802.1Q-in-Q VLAN Tag Termination feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_qinq.htm

PPPoE Session Limiting on Inner QinQ VLAN

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/sbseslt2.htm

PXF-Based Frame Relay DE Bit Marking

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

QoS Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following quality of service (QoS) features.

QoS: CBQoS Management - Policy-to-Interface Mapping Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

QoS: CBQoS MIB Index Enhancements

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, which may be known also as the CBQOSMIB Index Persistency feature, see the following Cisco document:

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

QoS Child Service Policy for Priority Class

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-3)

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

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

QoS: Classification, Policing, and Marking on LAC

Platform: Cisco 10000 series (PRE-3)

For detailed information about this feature, see the following chapters in the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

- Chapter 2, “Classifying Traffic”

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008061c2e0.html
- Chapter 6, “Policing Traffic”

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008061c367.html
- Chapter 7, “Marking Traffic”

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008061c35e.html

QoS - Hierarchical Queuing for Ethernet DSLAMs

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/10edslam.htm

QoS: Match VLAN

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

QoS - Percentage-Based Shaping

Platform: Cisco 10000 series (PRE-2 and PRE-3)

Note This feature was introduced in Cisco IOS Release 12.2(28)SB for the Cisco 7200 series and Cisco 7301.

For detailed information about this feature, see the "Shaping Traffic" chapter of the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/qoscf/10qshape.htm

QoS - Policing Support for GRE Tunnels

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

QoS Priority Propagation in Multi-level Scheduler

Platform: Cisco 10000 series (PRE-3)

For detailed information about this feature, see the *MQC Hierarchical Queuing with 3 Level Scheduler* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/3lvlschd.htm

QoS - VLAN Tag Based

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

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

RADIUS Logical Line ID

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, which is also known as the LLID Blocking feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftlineid.htm

Rate-Based Satellite Control Protocol (RBSCP)

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

For detailed information about this feature, see the *RBSCP (Rate Based Satellite Control Protocol)* document:

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

Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

Platforms: Cisco 7200 series, Cisco 7301

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

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

SFP Security Verification

Platforms: Cisco 7200 series, Cisco 7304

Cisco IOS Release 12.2(31)SB2 supports the SFP Security Verification feature in Cisco transceivers (Gigabit Interface Converters [GBICs] or small form-factor pluggable [SFP]) converters). (This feature is also known as the Cisco Quality ID feature.)

The SFP Security Verification feature primarily consists of the following components:

- A unique encrypted code in the GBIC module or SFP module that enables the Cisco IOS software to identify Cisco-pluggable parts.
- The ability of the Cisco IOS software to enable only those ports that are populated with Cisco parts. The SFP Security Verification feature allows customers to have confidence that the GBIC modules or SFP modules being deployed are certified to be compatible with the Cisco network device in which they are being deployed.

SNMP - Session to Interface Mapping Improvements

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the "CISCO-AAA-SESSION-MIB" section in the following Cisco documents:

- *Cisco 7200 Series Router MIB Specifications Guide*

  http://www.cisco.com/en/US/products/hw/routers/ps341/products_technical_reference_book09186a0080787cee.html

- *Cisco 7301 Router MIB Specifications Guide*

  http://www.cisco.com/en/US/products/hw/routers/ps352/products_technical_reference_book09186a00807837b7.html

- *Cisco 7304 Router MIB Specifications Guide*

  http://www.cisco.com/en/US/products/hw/routers/ps352/products_mib_quick_reference_book09186a00807811d3.html

- *Cisco 10000 Series Router Broadband MIB Specifications Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/mibs/bbgv4a/10kmib4a.pdf

SNMP Support for VPNs

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *SNMP Support over VPNs—Context-Based Access Control* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtsnmpvp.htm

Stateful Switchover Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following Stateful Switchover (SSO) features.

SSO - DHCP ODAP Client/Server

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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 Proxy Client

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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 Relay on Unnumbered Interface

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

Platform: Cisco 10000 series (PRE-2 and PRE-3)

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

Platforms: Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

SSO - Multilink Frame Relay

Platform: Cisco 10000 series (PRE-3)

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 - PPPoA

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *Cisco IOS Broadband High Availability Stateful Switchover* document:

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

SSO - PPPoE

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *Cisco IOS Broadband High Availability Stateful Switchover* document:

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

SSO - Remote Access to MPLS VPN

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the *Cisco IOS Broadband High Availability Stateful Switchover* document:

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

Static MAC Address for PPPoE

Platform: Cisco 10000 series (PRE-2 and PRE-3)

For detailed information about this feature, see the "Static MAC Address for PPPoE" section in the "Configuring PPPoE over Ethernet and IEEE 802.1Q VLAN" chapter of the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008050578c.html#wp1079081

Transmission Control Protocol Features

Cisco IOS Release 12.2(31)SB2 and later releases support the following Transmission Control Protocol (TCP) features.

TCP Application Flags Enhancement

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

TCP - Explicit Congestion Notification

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

TCP Show Extension

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

TCP Window Scaling

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

Turbo ACL Scalability Enhancements (Phase II)

Platform: Cisco 7304

The Turbo ACL Scalability Enhancements (Phase II) feature improves processing of access control lists (ACLs) for a Cisco 7304 router that uses an NSE-100 or NSE-150.

These enhancements improve processing of all Parallel eXpress Forwarding (PXF) traffic on a Cisco 7304 router that uses a network services engine (NSE) by more efficiently processing traffic that requires Turbo ACL classification in the PXF processing path. This feature also introduces user-configuration options that allow users to define the amount of memory used for Turbo ACL purposes in the Route Processor (RP) processing path.

For additional information on this feature, see *Turbo Access Control List Scalability Enhancements* document:

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

VPDN Debug Output

Platforms: Cisco 7200 series, Cisco 7301

The VPDN Debug Outputs feature enhances the **debug vpdn 12x-packets** command to decode both inbound and outbound Layer 2 Tunneling Protocol (L2TP) hexadecimal control packets for each L2TP Access Controller (LAC) or L2TP Network Server (LNS). In releases earlier than Cisco IOS Release 12.2(31)SB2, the **debug vpdn 12x-packets** command decoded only incoming L2TP hexadecimal control packets. With Cisco IOS Release 12.2(31)SB2 or later releases, in addition to decoding outbound control packets, the **debug vpdn 12x-packets** command decodes information regarding tunnel and session setup and teardown, Zero-Length Body (ZLB) packets, and attribute-value (AV) pairs. This feature also improves the readability of debug output.

You can debug outbound L2TP hexadecimal control packets by using the **debug vpdn 12x-packets** command in privileged EXEC mode.

The following example shows the **debug vpdn 12x-packets** command output with outbound debug output highlighted in **bold**:

```
3d22h: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
3d22h: Tnl 29029 L2TP: O SCCRQ
3d22h: Tnl 29029 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Parse SCCRQ
3d22h: Tnl 29029 L2TP: Parse AVP 2, len 8, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Protocol Ver 256
3d22h: Tnl 29029 L2TP: Parse AVP 6, len 8, flag 0x0
3d22h: Tnl 29029 L2TP: Firmware Ver 0x1130
3d22h: Tnl 29029 L2TP: Parse AVP 7, len 16, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Hostname LAC-tunnel
3d22h: Tnl 29029 L2TP: Parse AVP 8, len 25, flag 0x0
3d22h: Tnl 29029 L2TP: Vendor Name Cisco Systems, Inc.
3d22h: Tnl 29029 L2TP: Parse AVP 10, len 8, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Rx Window Size 20050
3d22h: Tnl 29029 L2TP: Parse AVP 11, len 22, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Chlng
B1 E9 3B 84 72 66 19 B1 C5 46 8F E7 31 A8 3B BC
3d22h: Tnl 29029 L2TP: Parse AVP 9, len 8, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Assigned Tunnel ID 29029
3d22h: Tnl 29029 L2TP: Parse AVP 3, len 10, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Framing Cap 0x0
3d22h: Tnl 29029 L2TP: Parse AVP 4, len 10, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Bearer Cap 0x0
3d22h: Tnl 29029 L2TP: Parse Cisco AVP 110, len 6, flag 0x0
3d22h: Tnl 29029 L2TP: PPPoE Relay Forward Capable
3d22h: Tnl 29029 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0, ns 0, nr 0
 C8 02 00 8D 00 00 00 00 00 00 00 80 08 00 00
 C8 02 00 8D 00 00 00 00 00 00 00 80 08 00 00
 00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
 00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
 6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
 53 79 73 74 65 6D 73 ...
3d22h: Tnl 29029 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Parse SCCRP
3d22h: Tnl 29029 L2TP: Parse AVP 2, len 8, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Protocol Ver 256
3d22h: Tnl 29029 L2TP: Parse AVP 6, len 8, flag 0x0
3d22h: Tnl 29029 L2TP: Firmware Ver 0x1120
3d22h: Tnl 29029 L2TP: Parse AVP 7, len 16, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Hostname LNS-tunnel
3d22h: Tnl 29029 L2TP: Parse AVP 8, len 25, flag 0x0
3d22h: Tnl 29029 L2TP: Vendor Name Cisco Systems, Inc.
3d22h: Tnl 29029 L2TP: Parse AVP 10, len 8, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Rx Window Size 20050
3d22h: Tnl 29029 L2TP: Parse AVP 11, len 22, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Chlng
7F 8B 30 8C 1D CD 44 49 CA 71 C3 6F 45 C2 89 B1
3d22h: Tnl 29029 L2TP: Parse AVP 13, len 22, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Chlng Resp
C3 A8 1B 39 6B 42 82 A5 AC A1 11 36 94 97 A2 1D
3d22h: Tnl 29029 L2TP: Parse AVP 9, len 8, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Assigned Tunnel ID 18566
3d22h: Tnl 29029 L2TP: Parse AVP 3, len 10, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Framing Cap 0x0
3d22h: Tnl 29029 L2TP: Parse AVP 4, len 10, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Bearer Cap 0x0
3d22h: Tnl 29029 L2TP: Parse Cisco AVP 110, len 6, flag 0x0
3d22h: Tnl 29029 L2TP: PPPoE Relay Forward Capable
3d22h: Tnl 29029 L2TP: No missing AVPs in SCCRP
3d22h: Tnl 29029 L2TP: I SCCRP, flg TLS, ver 2, len 163, tnl 29029, ns 0, nr 1
contiguous pak, size 163
```

```
 C8 02 00 A3 71 65 00 00 00 00 00 01 80 08 00 00
 00 00 00 02 80 08 00 00 00 02 01 00 00 08 00 00
 00 06 11 20 80 10 00 00 00 07 4C 4E 53 2D 74 75
 6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
 53 79 73 74 65 6D 73 2C ...
3d22h: Tnl 29029 L2TP: I SCCRP from LNS-tunnel
3d22h: Tnl 29029 L2TP: O SCCCN to LNS-tunnel tnlid 18566
3d22h: Tnl 29029 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Parse SCCCN
3d22h: Tnl 29029 L2TP: Parse AVP 13, len 22, flag 0x8000 (M)
3d22h: Tnl 29029 L2TP: Chlng Resp
3B 74 77 E8 DD 30 64 48 C2 63 42 D5 37 C3 B9 F2
3d22h: Tnl 29029 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl 18566, ns 1, nr 1
 C8 02 00 2A 48 86 00 00 00 01 00 01 80 08 00 00
 00 00 00 03 80 16 00 00 00 0D 3B 74 77 E8 DD 30
 64 48 C2 63 42 D5 37 C3 B9 F2
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: O ICRQ to LNS-tunnel 18566/0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse ICRQ
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 15, len 10, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Serial Number 1563200007
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 14, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Assigned Call ID 61
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 18, len 10, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Bearer Type 2
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse Cisco AVP 100, len 15, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Client NAS Port
53 65 72 69 61 6C 33 2F 30
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: O ICRQ, flg TLS, ver 2, len 63, tnl 18566,
lsid 61, rsid 0, ns 2, nr 1
 C8 02 00 3F 48 86 00 00 00 02 00 01 80 08 00 00
 00 00 00 0A 80 0A 00 00 00 0F 5D 2C 8A 07 80 08
 00 00 00 0E 00 3D 80 0A 00 00 00 12 00 00 00 02
 00 0F 00 09 00 64 53 65 72 69 61 6C 33 2F 30
3d22h: Tnl 29029 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 29029, ns
1, nr 2
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse ICRP
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 14, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Assigned Call ID 9
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: No missing AVPs in ICRP
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: I ICRP, flg TLS, ver 2, len 28, tnl 29029,
lsid 61, rsid 0, ns 1, nr 3
contiguous pak, size 28
 C8 02 00 1C 71 65 00 3D 00 01 00 03 80 08 00 00
 00 00 00 0B 80 08 00 00 00 0E 00 09
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: O ICCN to LNS-tunnel 18566/9
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse ICCN
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 24, len 10, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Connect Speed 1544000
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 19, len 10, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Framing Type 1
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 27, len 17, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Last Sent LCPREQ
 03 05 C2 23 05 05 06 1D 9C 69 09
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 28, len 12, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Last Rx LCPREQ
 05 06 1F 19 E3 07
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 31, len 22, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth Chal
 FF 0D CB C7 E4 07 74 9F 43 0C 82 B5 17 69 4D 9E
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 32, len 8, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth ID 60
```

```
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 30, len 22, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth Name client@cisco.com
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 33, len 22, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth Resp
 80 45 E2 C5 A7 D0 8C C1 0F 0A 14 F8 9E F7 21 F3
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse AVP 29, len 8, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth Type 2
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: O ICCN, flg TLS, ver 2, len 151, tnl 18566,
lsid 61, rsid 9, ns 3, nr 2
 C8 02 00 97 48 86 00 09 00 03 00 02 80 08 00 00
 00 00 00 0C 80 0A 00 00 00 18 00 17 8F 40 80 0A
 00 00 00 13 00 00 00 01 00 11 00 00 00 1B 03 05
 C2 23 05 05 06 1D 9C 69 09 00 0C 00 00 00 1C 05
 06 1F 19 E3 07 00 16 ...
3d22h: Tnl 29029 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 29029, ns 2, nr 4
3d22h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
```

For more information about the **debug vpdn 12x-packets** command, see the *Cisco IOS Debug Command Reference*:

http://www.cisco.com/en/US/products/ps6441/products_command_reference_book09186a0080497a2b.html

VRF-Aware System Message Logging (Syslog)

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series (PRE-2 and PRE-3)

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

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

VRF-Aware VPDN Tunnels

Platform: Cisco 10000 series (PRE-2 and PRE-3)

Note This feature was introduced in Cisco IOS Release 12.2(28)SB for the Cisco 7200 series and Cisco 7301.

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

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

Weighted Random Early Detection Improvements

Platform: Cisco 10000 series (PRE-2 and PRE-3)

Cisco IOS Release 12.2(31)SB2 contains the following Weighted Random Early Detection (WRED) improvements for the Performance Routing Engine 3 (PRE-3):

- Instantaneous per-packet calculation of the average queue depth
- Better approximation of drop curves
- Maximum of 21 WRED profiles and 13 default profiles per policy map with typical configurations

Improvements have also been made in the collection of statistical information for WRED and other quality of service (QoS) features. Instead of polling for statistics, the PRE-3 transfers statistical data to the Route Processor (RP) on-demand every 10 seconds. As a result, statistics can be collected more quickly and with a significant improvement in memory requirements.

For more information about WRED improvements, see the "Managing Packet Queue Congestion" chapter in the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/qoscf/10qqueue.htm

New Hardware Features in Cisco IOS Release 12.2(28)SB6

This section describes new and changed features in Cisco IOS Release 12.2(28)SB6. Some features may be new to Cisco IOS Release 12.2SB 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(28)SB6. 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 below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

1-Port Packet over SONET OC3c/STM1 Port Adapter

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about the 1-port Packet over SONET OC3c/STM1 port adapter (PA-POS-1OC3), see the following documents:

- *Cisco 1-Port OC-3/STM-1 Packet-Over-SONET Port Adapter* data sheet:

  http://www.cisco.com/en/US/partner/products/hw/routers/ps341/products_data_sheet0900aecd80221d3d.html

- *PA-POS-1OC3 Single-Port Port Adapter Installation and Configuration Guide*:

  http://www.cisco.com/univercd/cc/td/doc/product/core/7301/73pa/73-son/6514_1oc/index.htm

New Software Features in Cisco IOS Release 12.2(28)SB6

This section describes new and changed features in Cisco IOS Release 12.2(28)SB6. Some features may be new to Cisco IOS Release 12.2SB 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(28)SB6. 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 below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

Service Independent Intercept Architecture: SNMP-Based Lawful Intercept

Platforms: Cisco 7200 series, Cisco 7301

Note For the Cisco 7200 series, SNMP-Based Lawful Intercept is supported only on Cisco 7200 VXR routers that are configured with an NPE-225, NPE-400, or NPE-G1. Support for the NPE-G2 is available as of Cisco IOS Release 12.2(31)SB2.

Note RADIUS-Based Lawful Intercept was introduced in Cisco IOS Release 12.2(28)SB for the Cisco 7200 series and Cisco 7301.

SNMP-Based Lawful Intercept, which is a Layer 3 feature (that is, a feature at the IP level), is based on SNMPv3. The following MIBs are supported for SNMP-Based Lawful Intercept:

- CISCO-IP-TAP-MIB
- CISCO-IP-TAP2-MIB

For detailed information about the Service Independent Intercept (SII) architecture, see the *Service Independent Intercept* document:

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

Static MAC Address for PPPoE

Platform: Cisco 10000 series

For detailed information about this feature, see the "Static MAC Address for PPPoE" section in the "Configuring PPPoE over Ethernet and IEEE 802.1Q VLAN" chapter of the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a008050578c.html#wp1079081

New Hardware Features in Cisco IOS Release 12.2(28)SB2

This section describes new and changed features in Cisco IOS Release 12.2(28)SB2. Some features may be new to Cisco IOS Release 12.2SB 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(28)SB2. 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 below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

CWDM SFP for the 1-Port Gigabit Ethernet Half-Height Line Card

The 1-port Gigabit Ethernet half-height line card includes support for Coarse Wave Division Multiplexer (CWDM) Small Form-Factor Pluggable (SFP) laser optical transceiver modules. For more information, see the following *Cisco CWDM GBIC and CWDM SFP Installation Note*:

http://www.cisco.com/univercd/cc/td/doc/product/gbic_sfp/gbic_doc/78_15222.htm

New Software Features in Cisco IOS Release 12.2(28)SB2

This section describes new and changed features in Cisco IOS Release 12.2(28)SB2. Some features may be new to Cisco IOS Release 12.2SB 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(28)SB2. 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 below.

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

Table 11 shows features that have never before been released in any public Cisco IOS software image for the Cisco 10000 series and that released for the first time for the Cisco 10000 series in Cisco IOS Release 12.2(28)SB2. Other features may be new for the Cisco 10000 series in Cisco IOS Release 12.2(28)SB2, but have been released before in other public Cisco IOS software images for the Cisco 10000 series, and are therefore not included in Table 11.

Table 11 New Features for the Cisco 10000 Series in Cisco IOS Release 12.2(28)SB2

Feature Name
MPLS VPN Half-Duplex VRF with Dynamic and Static PE-CE Routing

BGP Support for NonStop Routing (NSR) with Stateful Switchover (SSO)

Platform: Cisco 10000 series

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

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

Lawful Intercept

Platform: Cisco 10000 series

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

http://www.cisco.com/application/pdf/en/us/guest/products/ps133/c1090/ccmigration_09186a008071ab8d.pdf

MPLS Traffic Engineering Features

Cisco IOS Release 12.2(28)SB2 introduces support for the following Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) features on the Cisco 10000 series.

Note With the exception of the MPLS Traffic Engineering—Overload Avoidance Support for IS-IS feature, support for these features was introduced in Cisco IOS Release 12.2(28)SB on the Cisco 7200 series, Cisco 7301, and Cisco 7304.

MPLS Diff-Serv-Aware Traffic Engineering (DS-TE)

Platform: Cisco 10000 series

For detailed information about this feature, see the *MPLS Traffic Engineering—DiffServ Aware* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/12s_dste.htm

MPLS Traffic Engineering (TE)

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/fs23te.htm

MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsbandaj.htm

MPLS Traffic Engineering (TE)—Configurable Path Calculation Metric for Tunnels

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsmetric.htm

MPLS Traffic Engineering (TE)—Forwarding Adjacency

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fstefa_3.htm

MPLS Traffic Engineering (TE)—Interarea Tunnels

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fsiarea3.htm

MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftaddexc.htm

MPLS Traffic Engineering (TE) MIB

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/temib2.htm

MPLS Traffic Engineering—Overload Avoidance Support for IS-IS

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/fsscen.htm

MPLS Traffic Engineering (TE)—Scalability Enhancements

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/fsscen.htm

MPLS Traffic Engineering (TE)—SNMP Notification Support

Platform: Cisco 10000 series

For detailed information about this feature, see the *MPLS Traffic Engineering MIB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/temib2.htm

MPLS VPN Half-Duplex VRF with Dynamic and Static PE-CE Routing

Platform: Cisco 10000 series

For detailed information about this feature, see the *MPLS VPN Half-Duplex VRF* document:

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

NetFlow PXF Timers

Platform: Cisco 10000 series

For detailed information about this feature, see the *Configuring NetFlow PXF Timers* document:

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

PPPoE QinQ Support

Platform: Cisco 10000 series

For detailed information about this feature, which is also known as the IEEE 802.1Q-in-Q VLAN Tag Termination feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_qinq.htm

RSVP Refresh Reduction and Reliable Messaging

Platform: Cisco 10000 series

Note This feature was introduced in Cisco IOS Release 12.2(28)SB for the Cisco 7200 series, Cisco 7301, and Cisco 7304.

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

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

New Hardware Features in Cisco IOS Release 12.2(28)SB

This section describes new and changed features in Cisco IOS Release 12.2(28)SB. Some features may be new to Cisco IOS Release 12.2SB 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(28)SB. 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 below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

1–Port Enhanced ATM Port Adapter with Support for 8000 VCs

Platforms: Cisco 7200 series, Cisco 7301

Cisco IOS Release 12.2(28)SB adds support for the PA-A6 port adapters and support for 8000 virtual circuits (VCs) on the PA-A6 port adapters. The PA-A6 is a series of single-width, single-port, ATM port adapters. With advanced ATM features, the PA-A6 port adapters support broadband aggregation, WAN aggregation, and campus/MAN aggregation.

The following PA-A6 port adapters are supported:

- PA-A6-OC3MM: 1-port ATM OC-3c/STM-1 multimode port adapter, enhanced
- PA-A6-OC3SMI: 1-port ATM OC-3c/STM-1 single-mode (IR) port adapter, enhanced
- PA-A6-OC3SML: 1-port ATM OC-3c/STM-1 single-mode (LR) port adapter, enhanced
- PA-A6-T3: 1-port ATM DS3 port adapter, enhanced
- PA-A6-E3: 1-port ATM E3 port adapter, enhanced

For detailed information about these products, see the *PA-A6 Port Adapter Installation and Configuration* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/7206/port_adp/atm_-pas/pa-a6/index.htm

4-Port Half-Height Channelized T3 Line Card

Platform: Cisco 10000 series

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

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_book09186a00805b3798.html

4-Port OC-3/ATM Long-Reach Line Card

Platform: Cisco 10000 series

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

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_book09186a00805b3798.html

1000BASE-T GBIC Support for the Network Services Engine 100

Platform: Cisco 7304

The 1000BASE-T GBIC (WS-G5483=) is supported on Gigabit Ethernet interfaces of the Network Services Engine 100 (NSE-100).

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

http://www.cisco.com/en/US/products/hw/modules/ps872/products_data_sheet09186a008014cb5e.html

CWDM GBIC Support for the Network Services Engine 100

Platform: Cisco 7304

Support for the following Coarse Wave Division Multiplexer (CWDM) Gigabit Interface Converters (GBICs) is introduced on Gigabit Ethernet ports of the Network Service Engine 100 (NSE-100):

- CWDM-GBIC-1470=
- CWDM-GBIC-1490=
- CWDM-GBIC-1510=
- CWDM-GBIC-1530=
- CWDM-GBIC-1550=
- CWDM-GBIC-1570=
- CWDM-GBIC-1590=
- CWDM-GBIC-1610=

For detailed information about these products, see the following Cisco document:

http://www.cisco.com/en/US/products/hw/modules/ps4999/products_data_sheet09186a00801a557c.html

CWDM SFP Support for the Network Processing Engine 100

Platform: Cisco 7304

The following Coarse Wave Division Multiplexer (CWDM) Small Form-Factor Pluggable (SFP) laser optical transceiver modules are supported on Gigabit Ethernet ports of the Network Processing Engine 100 (NPE-G100):

- CWDM-SFP-1470=
- CWDM-SFP-1490=
- CWDM-SFP-1510=
- CWDM-SFP-1530=
- CWDM-SFP-1550=
- CWDM-SFP-1570=
- CWDM-SFP-1590=
- CWDM-SFP-1610=

For detailed information about these products, see the following Cisco document:

http://www.cisco.com/en/US/products/hw/modules/ps4999/products_data_sheet09186a00801a557c.html

CWDM SFP Support for the 2-Port Gigabit Ethernet SPA on the Cisco 7304 Router

Platform: Cisco 7304

The following Coarse Wave Division Multiplexer (CWDM) Small Form-Factor Pluggable (SFP) laser optical transceiver modules are supported on Gigabit Ethernet ports of the 2-port Gigabit Ethernet SPA (SPA-2GE-7304):

- CWDM-SFP-1470=
- CWDM-SFP-1490=
- CWDM-SFP-1510=
- CWDM-SFP-1530=
- CWDM-SFP-1550=
- CWDM-SFP-1570=
- CWDM-SFP-1590=
- CWDM-SFP-1610=

For detailed information about these products, see the following Cisco document:

http://www.cisco.com/en/US/products/hw/modules/ps4999/products_data_sheet09186a00801a557c.html

New Software Features in Cisco IOS Release 12.2(28)SB

This section describes new and changed features in Cisco IOS Release 12.2(28)SB. Some features may be new to Cisco IOS Release 12.2SB 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(28)SB. 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 below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

Table 12 shows features that have never before been released in any public Cisco IOS software image for the Cisco 10000 series and that released for the first time for the Cisco 10000 series in Cisco IOS Release 12.2(28)SB. Other features may be new for the Cisco 10000 series in Cisco IOS Release 12.2(28)SB, but have been released before in other public Cisco IOS software images for the Cisco 10000 series, and are therefore not included in Table 12.

Table 12 New Features for the Cisco 10000 Series in Cisco IOS Release 12.2(28)SB

Feature Name
AAA CLI Stop Record Enhancement
Any Transport over MPLS (AToM): Frame Relay over MPLS (FRoMPLS)
ATM Conditional Debug Support
Dual Rate Three Color Policer
Hierarchical Input Policing
IGMPv3
Intelligent Service Gateway (ISG) Features
IP Multicast Load Splitting Across Equal-Cost Paths
IP SLAs - LSP Health Monitor
IPv6 Features
L2TP Congestion Avoidance
Layer 2 Local Switching
Link Fragmentation Interleave over Frame Relay (FRF.12)
Logging to Local Non-Volatile Storage (ATA Disk)
MLPPP with Link Fragmentation Interleave (LFI)
MPLS Carrier Supporting Carrier Features: • MPLS VPN—Carrier Supporting Carrier • MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution
MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV
MPLS HA Features: • NSF/SSO: MPLS LDP and LDP Graceful Restart • NSF/SSO: MPLS VPN • MPLS High Availability and • Cisco Express Forwarding: Command Changes • MPLS High Availability: Command Changes
MPLS LDP MD5 Global Configuration
MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session

Table 12 New Features for the Cisco 10000 Series in Cisco IOS Release 12.2(28)SB (continued)

Feature Name
Multicast-VPN: Multicast Support for MPLS VPN
Pseudowire Emulation Edge-to-Edge MIBs for Ethernet Services
RADIUS Server Load Balancing
Stateful Switchover (SSO) for Multilink PPP (MLP)
Template ACL/12-Bit ACE

Table 13 shows how select features for the Cisco 7304 are supported and uses the following conventions:

- Yes—The feature is supported on the engine and/or in the PXF path.
- No—The feature is not supported on the engine and/or in the PXF path.

Table 13 Features Supported on the Cisco 7304 Engines and in the PXF Path

Feature	Support on the NSE-100	Support on the NPE-G100	Support in the PFX Path
Frame Relay—show and debug Command Enhancements	Yes	Yes	No
IP SLAs LSP Health Monitor	Yes	Yes	No
MPLS VPN—eiBGP Multipath Loadbalancing Enhancements	Yes	Yes	Yes
MPLS VPN—VRF-Select for PXF	Yes	Not applicable[1]	Yes
Multiple Action Policer for PXF	Yes	Not applicable[1]	Yes
Three-level Hierarchical Policy Support in PXF	Yes	Not applicable[1]	Yes
Turbo Access Control List Scalability Enhancements [Phase 1]	Yes	Not applicable[1]	No[2]
Warm Reload	Yes	Yes	Not applicable[3]

1. This feature is supported on the NPE-G100 but not in the PXF path of the NPE-G100. Therefore, the PXF enhancement is not applicable to the NPE-G100.
2. Although this feature is not supported in the PXF path, this enhancement improve system memory utilization in the PXF path.
3. This feature does not apply to the PXF path.

AAA Features

Cisco IOS Release 12.2(28)SB introduces support for the following AAA features.

AAA CLI Stop Record Enhancement

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature, see the *Per VRF AAA* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvrfaaa.htm

AAA Double Authentication Secured by Absolute Timeout

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_dasat.htm

AAA Per-User Scalability

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Per VRF AAA* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvrfaaa.htm

AAA-PPP-VPDN Non-Blocking

Platforms: Cisco 7200 series, Cisco 7301

Previously, 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.

ACL Default Direction

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftacldir.htm

Any Transport over MPLS (AToM): Frame Relay over MPLS (FRoMPLS)

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature for the Cisco 10000 series, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

ATM Features

Cisco IOS Release 12.2(28)SB introduces support for the following ATM features.

ATM Bulk VC Configuration

Platform: Cisco 10000 series

For detailed information about this feature, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

ATM Conditional Debug Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

For detailed information about this feature (which is also known as the ATM Conditional debug/show Commands feature), see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/12satmdb.htm

ATM Multilink PPP Support on Multiple VCs

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 7500 series, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftatmmlt.htm

ATM OAM Ping

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s21/12atmpng.htm

ATM OAM Traffic Reduction

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/atmoam.htm

ATM PVCs

Platform: Cisco 10000 series

The ATM line cards support the full range of virtual path identifier (VPI)/virtual channel identifier (VCI) pairs (unidirection only)—8-bit VPI range and 16 bit VCI range. Table 14 lists the maximum number of active virtual channels (VCs) supported on ATM line cards for Cisco IOS Release 12.2(28)SB.

Table 14 Active VCs on ATM Line Cards

Line Card	Maximum VCs per Port	Maximum VCs per Module	Number of VBR, CBR, Shaped UBR VCs
E3/DS3	4,096	32,768[1]	28,672[2]
OC-3	8,191	32,764[3]	28,672[4]
OC-12	16,384	16,384	16,384

1. For 32,768 VCs per module, 4096 VCs must be unshaped UBR VCs.
2. For 28,672 VBR, CBR, and shaped UBR VCs, no VCs can be in shaped VP tunnels. If VCs are in shaped VPs, the number of VBR, CBR, and shaped UBR VCs is 22,204.
3. For 32,764 VCs per module, 4096 VCs must be unshaped UBR VCs.
4. For 28,672 VBR, CBR, and shaped UBR VCs, no VCs can be in shaped VP tunnels. If VCs are in shaped VPs, the number of VBR, CBR, and shaped UBR VCs is 22,204.

You can configure the maximum number of VCs across the ports in any fashion, provided that you do not exceed the per-port maximum.

Although the maximum number of VBR, CBR, and shaped UBR VCs per E3/DS3 and OC-3 ATM line card is 28,672, the router supports a maximum of 22,204 VBR, CBR, and shaped UBR VCs per line card that you can place within virtual path (VP) tunnels. If you attempt to bring up more than 22,204 VCs in a configuration that includes VP tunnels and VCs (hierarchical traffic shaping configuration), the VCs might not assign traffic correctly or the VCs might not come up at all. Be sure to limit the number of configured VBR, CBR, and shaped UBR VCs on an ATM card to less than 22,204 VCs if you place the VCs in VP tunnels.

ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtatmpvr.htm

ATM VC into VP Shaping

Platform: Cisco 10000 series

For detailed information about this feature, see the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_book09186a00805b9497.html

Attribute Screening for Access Requests

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123b/123b3/gt_asfar.htm

Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/ftpauto2.htm

BGP Features

Cisco IOS Release 12.2(28)SB introduces support for the following Border Gateway Protocol (BGP) features.

BGP 4 MIB Support for per-Peer Received Routes

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature, which is also known as the BGP Received Routes MIB feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s21/sbgprmib.htm

BGP Convergence Optimization

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

BGP Convergence Optimization introduces a new algorithm for update generation that reduces the time that is required for Border Gateway Protocol (BGP) convergence. Neighbor update messages are optimized before they are forwarded to neighbors. Updates are optimized and forwarded based on peer groups and per-individual neighbors. This enhancement improves BGP convergence, router boot time, and transient memory usage. This enhancement is not user configurable.

Note This feature is also known as BGP: Reduction in Transient Memory Usage.

BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsbgpcce.htm#wp1027129

BGP Increased Support of Numbered AS-Path Access Lists to 500

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/ftiaaspa.htm

BGP Support for IP Prefix Import from a Global Table into a VRF Table

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fs_bgivt.htm

Bit Error Rate Testing (BERT)

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s21/bert.htm

Bridged 1483 Encapsulated Traffic over ATM SVCs

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbridge.htm

Byte-Based Weighted Random Early Detection

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsbyte.htm

CEF/dCEF - Cisco Express Forwarding

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature for the Cisco 10000 series, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

Clear IPC Statistics

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_ipc.htm

Configurable MAC Address for PPPoE

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gt_cmppp.htm

Crashinfo Support

Platform: Cisco 10000 series

The Crashinfo Support feature for the Cisco 10000 series is a mechanism to reliably and quickly store useful information related to unexpected system shutdowns directly to a local flash card. This information can be retrieved after a system reload to aid in the analysis and resolution of a system error.

To enable the Crashinfo Support feature, enter the **exception crashinfo file** *device***:***filename* global configuration command. Use the *device* and *filename* arguments to specify the flashcard and file to be used for storing the diagnostic information. To change the size of the crashinfo buffer, enter the **exception crashinfo buffersize** command. The default buffer size is 32 Kilobytes.

Define Interface Policy-Map AV Pairs AAA

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xi7/123xiqos.htm

DHCP Features

Cisco IOS Release 12.2(28)SB introduces support for the following DHCP features.

DHCP Accounting

Platform: Cisco 10000 series

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

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

DHCP Address Allocation Using Option 82

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftrbeo82.htm

DHCP Client Dynamic Subnet Allocation API

Platform: Cisco 7200 series

The DHCP Client Dynamic Subnet Allocation API feature is an application programming interface (API) that is called by the DHCP Server—On-Demand Address Pool Manager feature for obtaining a subnet or releasing a subnet to the source server via DHCP. This feature allows automated configuration of Layer 3 devices for simplified deployment.

DHCP—Configurable DHCP Client

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

DHCP Lease Limit per ATM RBE Unnumbered Interface

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

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

DHCP ODAP Server Support

Platform: Cisco 10000 series

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

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

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

Platform: Cisco 10000 series

For detailed information about this feature, see the following *DHCP Server—On-Demand Address Pool Manager* document:

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

DHCP Option 82 Support for Routed Bridge Encapsulation

Platforms: Cisco 7200 series, Cisco 7301

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

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

DHCP Relay MPLS VPN Support

Platform: Cisco 10000 series

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

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

DHCP Relay Subscriber Identifier Suboption

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

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

DHCP Release and Renew CLI in EXEC Mode

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

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

DHCP Server—On-Demand Address Pool Manager

Platform: Cisco 10000 series

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

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

DHCP Server—Option to Ignore All BOOTP Requests

Platforms: Cisco 7200 series, Cisco 7301

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

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

DHCP—Static Mapping

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

DHCP—Statically Configured Routes Using a DHCP Gateway

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

DHCPv6 Prefix Delegation via AAA

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature, see the “Prefix Delegation” section in the “Implementing ADSL and Deploying Dial Access for IPv6” chapter that is part of the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_dial6.htm

DHCPv6 Relay Agent

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

A client locates a DHCP server by using a reserved, link-scoped multicast address. Therefore, it is a requirement for direct communication between the client and the server that the client and the server be attached to the same link. However, in some situations in which ease of management, economy, or scalability is a concern, it is desirable to allow a DHCP client to send a message to a DHCP server that is not connected to the same link. A DHCP relay agent, which may reside on the client's link, is used to relay messages between the client and the server. DHCP relay agent operation is transparent to the client.

For more information, see the *Implementing Basic Connectivity for IPv6* chapter that is part of the *Cisco IOS IPv6 Configuration Library*:

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

Distributed Time-Based Access Lists

Platform: Cisco 10000 series

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

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

Dialer CEF

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftdlrcef.htm

DNS Spoofing

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtdnsspf.htm

Dynamic ATM VP and VC Configuration Modification

Platform: Cisco 10000 series

The Dynamic ATM VP and VC Configuration Modification feature enables you to change the virtual circuit (VC) weight or virtual path (VP) shaping parameters without affecting the state of the VC or VP. In other words, the VC and VP remain up and operational (the VC or VP is not torn down at the segmentation and reassembly [SAR], and the session does not go down). The dynamic parameters include ATM VP parameters (peak cell rate [PCR] or cell delay variation tolerance [CDVT]) and VC parameters (weight, PCR, sustainable cell rate [SCR], maximum burst size [MBS], and CDVT). When you change the VC parameters or the VP rate, there can be a momentary change in the shaped rate of the VP, in which the rate at which cells are sent may be over or under the configured rate. The session stays up, and no data is lost.

The range of integer values that are supported by the *weighting-value* argument of the **weight** command is 5 to 255.

Dynamic DNS Support for Cisco IOS Software

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123ya8/gt_ddns.htm

Dynamic Subscriber Bandwidth Selection

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftdbs.htm

EIGRP MPLS VPN PE-CE Site of Origin (SoO)

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gtmvesoo.htm

Embedded Event Manager 2.1

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gteem21.htm

Enabling OSPFv2 on an Interface Using the ip ospf area Command

Platform: Cisco 10000 series

For detailed information about this feature, which is also known as the Area Command in Interface Mode for OSPFv2 feature, see the following Cisco document:

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

Enhanced Tracking Support

Platform: Cisco 10000 series

For detailed information about this feature, including Enhanced Object Tracking, see the following Cisco document:

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

Entity/Environment Monitoring

Platforms: Cisco 7200 series, Cisco 7301

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

- For the Cisco 7200 series, see the *Cisco 7200 Series Router MIB Specifications Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps341/products_technical_reference_book09186a0080787cee.html

- For the Cisco 7301, see the *Cisco 7301 Router MIB Specifications Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps352/products_technical_reference_book09186a00805fee95.html

Extended NAS-Port-Type and NAS-Port Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

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

Frame Relay Features

Cisco IOS Release 12.2(28)SB introduced support for the following Frame Relay features.

Frame Relay Fast Restart

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st19/19stfr72.htm

Frame Relay MIB Enhancements

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftfrmibe.htm

Frame Relay—show and debug Command Enhancements

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series.

For detailed information about this feature, which is also known as the Frame Relay show Command and debug Command Enhancements feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/sbfrshow.htm

Frame Relay VC Bundling

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Frame Relay PVC Bundles with IP and MPLS QoS Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_frbnd.htm

Generic Routing Encapsulation (GRE) Tunnel Keepalive

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

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

Globalized Channelizations for SONET/SDH

Platform: Cisco 10000 series

The Globalized Channelizations for SONET/SDH feature enables the Cisco 10000 series 1-port channelized OC-12 line card and 4-port channelized STM-1 line card to support the following globalized channelization modes:

- SONET channelization:
  - STS-1 over DS3/T3
  - STS-1 over DS3/T3 over DS1
  - STS-1 over DS3/T3 over DS3 subrate
  - STS-1 over VT1.5 over DS1
  - STS-1 over VT2 over E1
- Synchronous Digital Hierarchy (SDH) channelization:
  - STM-1 over AU-3 over DS3/T3
  - STM-1 over AU-3 over DS3/T3 over DS3 subrate
  - STM-1 over AU-3 over TUG-2 over C-11 over DS1/T1
  - STM-1 over AU-3 over TUG-2 over C-12 over E1
  - STM-1 over AU-4 over TUG-3 over TUG-2 over C-11 over DS1/T1
  - STM-1 over AU-4 over TUG-3 over TUG-2 over C-12 over E1

IEEE 802.1p Support

Platform: Cisco 10000 series

The IEEE's 802.1p standard now allows a range of traffic prioritization of Layer 2 frames from critical to non-critical through a frame priority tag, providing a higher quality of service (QoS) on high-speed LANs. Network managers can implement traffic prioritization through infrastructure device upgrades. IEEE 802.1p is a key enabler to QoS by enabling "Prioritized Ethernet" with up to eight priorities in Ethernet and Token Ring networks.

IGMP State Limit

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

The IGMP State Limit feature provides protection against denial of service attacks caused by IGMP packets. The new CLI introduced by this feature allows you to configure a limit on the number of IGMP states that results from IGMP, IGMP Version 3 lite, and URL Rendezvous Directory (URD) membership reports on a per-interface or global basis. Membership reports in excess of the configured limits will not be entered in the IGMP cache, and traffic for those excess membership reports will not be forwarded.

For more information, see the *Customizing IGMP* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/chap10/mcbcigmp.htm

IGMPv3

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature, see the *Customizing IGMP* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/chap10/mcbcigmp.htm

Improved show commands for MLP-ATM LFI

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

For detailed information about this feature, see the *Troubleshooting Enhancements for Multilink PPP over ATM Link Fragmentation and Interleaving* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gttrbmlp.htm

Intelligent Service Gateway (ISG) Features

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series.

Cisco IOS Release 12.2(28)SB introduces support for the following Intelligent Service Gateway (ISG) features on the Cisco 7200 series, Cisco 7301, and Cisco 10000 series as explained in Table 15.

Table 15 ISG Features Supported per Platform

ISG Feature	Cisco 7301 Router	Cisco 7200 Series	Cisco 10000 Series
ISG: Authentication: DHCP Option 82 Line ID - AAA Authorization Support	Yes	Yes	No
ISG: Accounting: Postpaid	Yes	Yes	No
ISG: Accounting: Time-Based Prepaid	Yes	Yes	Yes
ISG: Accounting: Volume-Based Prepaid	Yes	Yes	No
ISG: Accounting: Per Session, Service & Flow	Yes	Yes	Yes
ISG: Accounting: Tariff Switching	Yes	Yes	No
ISG: Flow Control: Flow Redirect (L4, Captive Portal)	Yes	Yes	Yes
ISG: Flow Control: QoS Control: Dynamic Rate Limiting	Yes	Yes	Yes

Table 15 ISG Features Supported per Platform

ISG Feature	Cisco 7301 Router	Cisco 7200 Series	Cisco 10000 Series
ISG: Instrumentation: Advanced Conditional Debugging	Yes	Yes	Yes
ISG: Instrumentation: Session & Flow Monitoring (local and external)	Yes	Yes	No
ISG: Network Interface: IP Routed, VRF Aware MPLS	Yes	Yes	No
ISG: Network Interface: Tunneled (L2TP)	Yes	Yes	Yes
ISG: Policy Control: DHCP Proxy	Yes	Yes	No
ISG: Policy Control: Multidimensional Identity per Session	Yes	Yes	Yes
ISG: Policy Control: Policy: Domain Based (Auto-domain)	Yes	Yes	Yes
ISG: Policy Control: Policy Server: CoA (QoS, L4 Redirect, User ACL, TimeOut)	Yes	Yes	Yes
ISG: Policy Control: Policy Server: SSG-SESM Protocol	Yes	Yes	Yes
ISG: Policy Control: Policy: Triggers: Duration	Yes	Yes	No
ISG: Policy Control: Service Profiles	Yes	Yes	Yes
ISG: Policy Control: User Profiles	Yes	Yes	Yes
ISG: Session: Auth: PBHK	Yes	Yes	Yes
ISG: Session: Auth: Single Sign On	Yes	Yes	Yes
ISG: Session: Authentication (MAC, IP, EAP)	Yes	Yes	No
ISG: Session: Creation: Interface IP Session: L2	Yes	Yes	No
ISG: Session: Creation: Interface IP Session: L3	Yes	Yes	No
ISG: Session: Creation: IP Session: Protocol Event (DHCP)	Yes	Yes	No
ISG: Session: Creation: IP Session: Subnet & Source IP: L2	Yes	Yes	No
ISG: Session: Creation: IP Session: Subnet & Source IP: L3	Yes	Yes	No
ISG: Session: LifeCycle: Idle Timeout	Yes	Yes	Yes
ISG: Session: LifeCycle: POD	Yes	Yes	Yes
ISG: Session: Multi-Service Creation and Flow Control	Yes	Yes	Yes
ISG: Session: VRF Transfer	Yes	Yes	No

For detailed information about these features, see the *Cisco IOS Intelligent Service Gateway Configuration Guide* that is part of the *Cisco IOS ISG Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/cg/isg_lib/index.htm

Interface Alias Long Name Support

Platform: Cisco 10000 series

For detailed information about this feature, see the following *Interface Index Display and Interface Alias Long Name Support for SNMP* document:

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

IP Features

Cisco IOS Release 12.2(28)SB introduced support the following IP features.

IPMROUTE-STD-MIB

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

The IPMROUTE-STD-MIB, as defined in RFC 2932, is a module for IP multicast routing in a manner 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

The ipMRouteScopeNameTable MIB object is not supported because it is not relevant to multicast routers.

IP Multicast Load Splitting Across Equal-Cost Paths

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature, see the *Load Splitting IP Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/mcbsplit.htm

For detailed information about this feature for the Cisco 10000 series, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

IP SLAs LSP Health Monitor

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/sbchmon.htm

IPv6 Access Services: DHCPv6 Prefix Delegation

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

DHCP for IPv6 can be used in environments to deliver stateless address assignment information. Stateless address assignment uses configuration parameters that do not require a server to maintain a dynamic state for individual clients, such as DNS server addresses and domain search list options.

For more information, see the *Implementing Basic Connectivity for IPv6* document:

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

IPv6 Features for the Cisco 10000 Series

Platform: Cisco 10000 series

Cisco IOS Release 12.0(28)SB supports the IPv6 Hardware: PXF Accelerated for IPv6 Forwarding feature for the Cisco 10000 series, which includes support for the following IPv6 features:

- IPv6 features:
  - IPv6 address types: Unicast
  - IPv6: ICMPv6
    (Note: A ping in the fast-path mode is not supported; the support rate is limited to 10 pings per second per interface.)
  - IPv6: IPv6 neighbor discovery
  - IPv6: IPv6 stateless autoconfiguration
  - IPv6: IPv6 MTU path discovery
  - IPv6: ICMPv6 redirect
  - IPv6: neighbor discovery duplicate address detection
  - IPv6: IPv6 static cache entry for neighbor discovery
  - IPv6 address types: Anycast
- IPv6 Switching Services features:
  - IPv6 switching: CEF/dCEF support
  - IPv6 switching: CEFv6 switched configured IPv6 over IPv4 tunnels
- IPv6 Routing features:
  - IPv6 routing: RIP for IPv6 (RIPng)
  - IPv6 routing: static routing
  - IPv6 routing: route redistribution
  - IPv6 routing: multiprotocol BGP extensions for IPv6
  - IPv6 routing: multiprotocol BGP link-local address peering
  - IPv6 routing: IS-IS support for IPv6
  - IPv6 routing: IS-IS multitopology support for IPv6
  - IPv6 routing: OSPF for IPv6 (OSPFv3)
- IPv6 Services and Management features:
  - IPv6 services: AAAA DNS lookups over an IPv4 transport
  - IPv6 services: standard access control lists
  - IPv6 services: DNS lookups over an IPv6 transport
  - IPv6 services: Secure Shell support over IPv6
  - IPv6 services: Cisco Discovery Protocol—IPv6 address family support for neighbor information
  - IPv6 services: CISCO-IP-MIB support
  - IPv6 services: CISCO-IP-FORWARDING-MIB support
  - IPv6 services: extended access control lists3

- IPv6 Tunnel Services features:
  - IPv6 tunneling: manually configured IPv6 over IPv4 tunnels
  - IPv6 tunneling: IPv6 over IPv4 GRE tunnels
- IPv6 Data Link Layer features:
  - IPv6 data link: ATM PVC and ATM LANE
  - IPv6 data link: Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet
  - IPv6 data link: Frame Relay PVC
  - IPv6 data link: Cisco High-Level Data Link Control
  - IPv6 data link: PPP service over packet over SONET, ISDN, and serial (synchronous and asynchronous) interfaces
    (Note: PPPoA, PPPoE, and PPP over a VLAN are not supported; PPP over a serial link is supported.)
  - IPv6 data link: VLANs using IEEE 802.1Q encapsulation

For more information about these IPv6 features, see the "Start Here: Cisco IOS Software Release Specifics for IPv6 Features" chapter of the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/ftipv6s.htm

ISDN Backup in MPLS Core

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtisdnbk.htm

In Service Software Upgrade (ISSU)

Platform: Cisco 10000 series

The In Service Software Upgrade (ISSU) feature includes support for the following features:

- ISSU - ARP
- ISSU - ATM
- ISSU - Frame Relay
- ISSU - HDLC
- ISSU - HSRP
- ISSU - PPP/MLP
- ISSU - QoS
- ISSU - SNMP

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

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

The ISSU feature includes support for the following MPLS features:

- ISSU - MPLS LDP
- ISSU - MPLS QoS
- ISSU - MPLS L3VPN

For detailed information about these features, see the *ISSU MPLS Clients* document:

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

The ISSU feature is supported on the following line cards:

- 1-port channelized OC-12/STM-4
- 1-port Gigabit Ethernet
- 1-port half-height Gigabit Ethernet
- 1-port OC-12 ATM
- 1-port OC-12 Packet over SONET (PoS)
- l-port OC-48 PoS
- 4-port channelized OC-3/STM-1
- 4-port channelized half-height T3
- 4-port OC-3 ATM
- 6-port channelized T3
- 6-port OC-3 PoS
- 8-port ATM E3/DS3
- 8-port E3/DS3
- 8-port half-height Fast Ethernet
- 24-port channelized E1/T1

L2TP and L2TPv3 Features

Cisco IOS Release 12.2(28)SB introduces support for the following L2TP and L2TPv3 features.

L2TP Congestion Avoidance

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2scca.htm

L2TP Disconnect Cause Information

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtl2disc.htm

L2TP Extended Failover

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2tpef.htm

L2TP Redirect

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2tpmr.htm

L2TP Security

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2tsec.htm

L2TP Tunnel Connection Speed Labeling

Platforms: Cisco 7200 series, Cisco 7301

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

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

L2TPv3 Control Message Hashing

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

L2TPv3 Control Message Rate Limiting

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

Protocol Demultiplexing for L2TPv3

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

Layer 2 Local Switching

Platform: Cisco 10000 series

For detailed information about this feature, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

Layer 2 Local Switching: Frame Relay to Frame Relay

Platform: Cisco 10000 series

For detailed information about this feature, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

Layer 2 VPN Features

Cisco IOS Release 12.2(28)SB introduces support for the following Layer 2 VPN features.

L2VPN Pseudowire Redundancy

Platform: Cisco 7403

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

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

L2VPN Pseudowire Switching

Platforms: Cisco 7200 series, Cisco 7301

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

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

Layer 2 VPN: Syslog, SNMP Trap and Show Command Enhancements for AToM and L2TPv3

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

NSF/SSO: L2VPN Pseudowire Redundancy Support

Platforms: Cisco 7200 series, Cisco 7301

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

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

Local AAA Server

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

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

Local Template-Based ATM PVC Provisioning

Platform: Cisco 10000 series

The Local Template-Based ATM PVC Provisioning feature supports permanent virtual circuit (PVC) autoprovisioning for an infinite range of virtual path identifier (VPI)/virtual channel identifier (VCI) combinations on an ATM interface. This feature enables ATM PVCs to be provisioned automatically as needed from a local configuration, which makes the provisioning of large numbers of digital subscriber line (DSL) subscribers easier, faster, and less prone to error. ATM PVC autoprovisioning can be configured on a PVC, an ATM PVC range, or a virtual circuit (VC) class. If a VC class that is configured with ATM PVC autoprovisioning is assigned to the main interface, all the PVCs on that main interface will be autoprovisioned; this configuration is sometimes called an infinite range.

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/ftpvcaut.htm

Logging to Local Non-Volatile Storage (ATA Disk)

Platform: Cisco 10000 series

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

MLP LFI over ATM Configuration Scaling

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, which is also known as the Link Fragmentation and Interleaving for Frame Relay and ATM Virtual Circuits feature, see the following Cisco document:

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

MPLS Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) and MPLS-related features.

MPLS (Multiprotocol Label Switching)

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature for the Cisco 10000 series, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

MPLS-Aware NetFlow

Platforms: Cisco 7200 series, Cisco 7301

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

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

MPLS Egress NetFlow Accounting

Platform: Cisco 10000 series

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

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

MPLS Embedded Management—High Capacity Counter

Platforms: Cisco 7200 series, Cisco 7301

As of Cisco IOS Release 12.2(28)SB, the MPLS IF MIB has a 64-bit structure to ensure that high-capacity loads can be handled.

MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/lsping28.htm

MPLS Label Distribution MIB: MPLS LDP Trap Enhancement

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, which is also known as the MPLS VPN MIB v05 - Trap Enhancements feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsvnmb25.htm#wp1027129

MPLS Label Distribution Protocol (LDP)

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftldp13.htm

MPLS—LDP AutoConfiguration

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/fsldpaut.htm

MPLS—LDP MD5 Global Configuration

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sb_md5.htm

MPLS—LDP Session Protection

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/fssespro.htm

MPLS—Multilink PPP Support

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtmpmlp.htm

MPLS QoS—DiffServ Tunnel Mode Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftdtmode.htm

MPLS HA Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) High Availability (HA) features for the Cisco 10000 series.

Note In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series supports Route Processor Redundancy Plus (RPR+) and Stateful Switchover (SSO). However for broadband aggregation features, the Cisco 10000 series supports RPR+ only.

NSF/SSO: MPLS LDP and LDP Graceful Restart

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsldpgr.htm

NSF/SSO: MPLS VPN

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsvpngr.htm

MPLS High Availability

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fshaov.htm

Command Changes in Relation to MPLS HA

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

For command changes in relation to Multiprotocol Label Switching (MPLS) high availability (HA), see the following documents:

- Cisco Express Forwarding: Command Changes

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fscefcmd.htm

- MPLS High Availability: Command Changes

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fscmdha.htm

MPLS Traffic Engineering Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) features:

MPLS Diff-Serv-Aware Traffic Engineering (DS-TE)

Platforms: 7200 series, Cisco 7301, Cisco 7304

For detailed information about this feature, see the *MPLS Traffic Engineering—DiffServ Aware* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/12s_dste.htm

MPLS Traffic Engineering (TE)

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/fs23te.htm

MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsbandaj.htm

MPLS Traffic Engineering (TE)—Configurable Path Calculation Metric for Tunnels

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsmetric.htm

MPLS Traffic Engineering (TE)—Forwarding Adjacency

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fstefa_3.htm

MPLS Traffic Engineering (TE)—Interarea Tunnels

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fsiarea3.htm

MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftaddexc.htm

MPLS Traffic Engineering (TE)—Scalability Enhancements

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/fsscen.htm

MPLS Traffic Engineering (TE)—SNMP Notification Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

For detailed information about this feature, see the *MPLS Traffic Engineering MIB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/temib2.htm

MPLS VPN Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) features.

MPLS VPN—Carrier Supporting Carrier

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbb2scsc.htm

MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbbcsc13.htm

MPLS VPN—eiBGP Multipath Loadbalancing Enhancements

Platform: Cisco 7304, Cisco 10000 series

In this Cisco IOS release, the MPLS-VPN eiBGP Multipath Loadbalancing feature has been enhanced to support up to 96,000 VPN routes in a scenario in which there are four BGP paths and one IGP path to each BGP peer. In previous Cisco IOS releases, up to 48,000 VPN routes were supported.

It is important to note that the maximum number of load-balanced paths used per route decreases from 16 to 8 as a result of this feature. The number of load-balanced paths per route is determined using a round-robin algorithm, but the round-robin algorithm now can only use up to 8 paths instead of 16, like it could previously.

This is a functional enhancement that introduces no new configuration.

MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/gsxnlbsp.htm

MPLS VPN—Half Duplex VRF (HDVRF) Support with Static Routing

Platform: Cisco 10000 series

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

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

MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

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

MPLS VPN—Inter-Autonomous System Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/interas.htm

MPLS VPN—MIB Support: MPLS VPN Trap Enhancement

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *MPLS VPN—MIB Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsvnmb25.htm#wp1027129

MPLS VPN—Show Running VRF

Platform: Cisco 10000 series

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

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

MPLS VPN—VPN-Aware LDP MIB

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *MPLS Label Distribution Protocol MIB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ldpmib13.htm#wp1015327

MPLS VPN—VRF-Select for PXF

Platform: Cisco 7304

VRF-Select is supported in the PXF processing path for a Cisco 7304.

For information about MPLS VPN VRF-Select, see the *MPLS VPN: VRF Selection Based on Source IP Address* document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a0080173d55.html

For additional information about this feature and all other features in the PXF-processing path, including restrictions, see the *Cisco 7304 Troubleshooting and Configuration Notes* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm#wp65935

Multicast-VPN: Multicast Support for MPLS VPN

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature (which is also known as the Multicast VPN—IP Multicast Support for MPLS VPNs feature), see the following Cisco document:

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

MQC Policy Map Support on Configured VC Range

Platforms: Cisco 7200 series, Cisco 7301

The MQC Policy Map Support on Configured VC Range feature extends policy map functionality to simplify the configuration of ranges of ATM VCs. Using the **service-policy** command, this feature allows you to apply a QoS service policy to a range of VCs.

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/28sbvrng.htm

Multilink Frame Relay (FRF.16.1) Variable Bandwidth Class Support

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Multilink Frame Relay (FRF.16.1)* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs_mfr.htm

Multiple Action Policer for PXF

Platform: Cisco 7304

The Multiple Action Policer feature further extends the functionality of the Cisco IOS Traffic Policing feature (a single-rate policer feature). The Traffic Policing feature is a traffic policing mechanism that allows you to control the maximum rate of traffic sent or received on an interface. Both of these traffic policing mechanisms mark packets as conforming to, exceeding, or violating a specified rate. After a packet is marked, you can specify an action to be taken on the packet based on that marking.

With the Traffic Policing feature, you can specify only one conform action, one exceed action, and one violate action. Now with the Multiple Action Policer feature, you can specify multiple conform, exceed, and violate actions for the marked packets.

The Multiple Action Policer feature is introduced in the PXF processing path for the first time. For additional information about this feature and all other features in the PXF-processing path, including restrictions, see the *Cisco 7304 Troubleshooting and Configuration Notes* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm#wp65935

Multirouter Automatic Protection Switching (APS)

Platform: Cisco 10000 series

For detailed information about this feature, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

NetFlow MPLS Label Export

Platforms: Cisco 7200 series, Cisco 7301

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

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

Nonstop Forwarding and Stateful Switchover Features

Nonstop Forwarding

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

Cisco IOS Release 12.2(28)SB supports the following Nonstop Forwarding (NSF) features:

- Integrated IS-IS Nonstop Forwarding Awareness
- Nonstop Forwarding (NSF) Awareness
- Nonstop Forwarding (NSF) for BGP
- Nonstop Forwarding (NSF) for IS-IS
- Nonstop Forwarding with Stateful Switchover (NSF/SSO)

For detailed information about these features, see the *Cisco Nonstop Forwarding* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fsnsf20s.htm

Stateful Switchover

Platforms: Cisco 7304, Cisco 10000 series

Cisco IOS Release 12.2(28)SB supports the following Stateful Switchover (SSO) features:

- APS Stateful Switchover (APS SSO)

Note APS SSO is supported only on the Cisco 10000 series.

- Stateful Switchover (SSO) for ATM
- Stateful Switchover (SSO) for Frame Relay
- Stateful Switchover (SSO) for HDLC
- Stateful Switchover (SSO) for Multilink PPP (MLP)
- Stateful Switchover (SSO) for PPP

For detailed information about these features with the exception of the SSO - Multilink PPP (MLP) feature, see the *Stateful Switchover* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fssso20s.htm

For detailed information about the SSO - Multilink PPP (MLP) feature, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

Offload Server Accounting Enhancement

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftoffact.htm

OSPF ABR Type 3 LSA Filtering

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftabrt3f.htm

Packet Classification Using the Frame Relay DLCI Number

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/ftdlc26i.htm

peer pool backup Command

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

For detailed information about this feature, see the *Peer Pool Backup* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpeerpl.htm

Per-Packet Load Balancing (PPLB)

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s21/pplb.htm

Per-User QoS via AAA Policy Name

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_puq.htm

Per VRF AAA

Platform: Cisco 10000 series

For detailed information about this feature, see the *Per VRF AAA* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvrfaaa.htm

PIM Multicast Scalability

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

The PIM Multicast Scalability feature enhances the Protocol Independent Multicast (PIM) protocol in Cisco IOS software by adding a new level of scalability. With this feature, edge devices can have a large number of multicast groups and users without increasing the CPU utilization of the router.

Policer Enhancement: Multiple Actions

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsmu26s.htm

Post-Switchover Core Dump

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/coredump.htm

PPP MLP MRRU Negotiation Configuration

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtmpmrru.htm

PPPoE Features

Cisco IOS Release 12.2(28)SB introduces support for the following PPPoE features.

PPPoA/PPPoE Autosense for ATM PVCs

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftp_auto.htm

PPPoE Circuit-ID Tag Processing

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

PPPoE over Gigabit Ethernet Interface

Platform: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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 Relay

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpppoer.htm

PPPoE Service Selection

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpoess.htm

PPPoE Session Limit

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftppoesl.htm

PPPoE Session Limit per NAS Port

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/12b_nas.htm

PPPoE Session Recovery After Reload

Platforms: Cisco 7200 series, Cisco 7301 Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtppprec.htm

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet Services

Platform: Cisco 10000 series

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

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

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS Features for the Cisco 7200 Series and Cisco 7301

Cisco IOS Release 12.2(28)SB supports the following QoS features for the Cisco 7200 series and Cisco 7301.

QoS: ATM Cell-Based Policer

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS: ATM-CLP and Layer 2 CoS-Based WRED

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12swred.htm

QoS: CBQoSMIB Parity Across Cisco IOS Release 12.0S, 12.2SB, and 12.3T

Platforms: Cisco 7200 series, Cisco 7301

Several MIB objects have been added to existing tables, and a new table has been added to the Class-Based Quality of Service (QoS) MIB (CBQoSMIB). These additions to the CBQoSMIB provide parity of the MIB across three specific Cisco IOS Releases—Cisco IOS Release 12.0S, 12.2SB, and 12.3T. As a result of these additions and revisions, the CBQoSMIB now supports the same features across all three of these platforms.

The CBQoSMIB now supports the following Cisco IOS features:

- QoS: ATM Cell-Based Policer

  The QoS: ATM Cell-Based Policer feature allows you to configure traffic policing for ATM cells. This feature allows you to specify traffic policing in cells, bytes, or percentage of bandwidth.

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

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

- QoS: ATM-CLP and Layer 2 CoS-Based WRED

  The QoS: ATM-CLP and Layer 2 CoS-Based WRED feature extends the functionality of the Cisco Weighted Random Early Detection (WRED) software. With the QoS: ATM-CLP and Layer 2 CoS-Based WRED feature, WRED can take into account the Layer 2 class of service (CoS) value of a packet and the ATM cell loss priority (CLP) of a packet when calculating the drop probability of network traffic.

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12swred.htm

- QoS: Color-Aware Policer

  The QoS: Color-Aware Policer feature enables a “color-aware” method of traffic policing. This feature allows you to police traffic according to the color classification of a packet that is based on packet-matching criteria defined for two user-specified traffic classes: the conform-color class and the exceed-color class. These two traffic classes are created using the **conform-color** command, and the metering rates are defined using the **police** command.

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/12s_cap.htm

- Low Latency Queuing with Priority Percentage Support

  This feature allows you to configure bandwidth as a percentage within low latency queuing (LLQ).

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12sllqpc.htm

- QoS: Percentage-Based Policing

  The QoS: Percentage-Based Policing feature allows you to configure traffic policing on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed burst (bc) size and the excess burst (be) size (used for configuring traffic policing) in milliseconds (ms). Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spctpg.htm

- QoS: Percentage-Based Shaping

  The QoS: Percentage-Based Shaping feature allows you to configure traffic policing and traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed (conform) burst (bc) size and the excess (peak) burst (be) size (used for configuring traffic shaping) in milliseconds (ms). Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spctsg.htm

- QoS: Time-Based Thresholds for WRED and Queue Limit

  The QoS: Time-Based Thresholds for WRED and Queue Limit feature allows you to specify the Weighted Random Early Detection (WRED) minimum and maximum thresholds or the queue limit threshold in milliseconds (ms). Previously, these thresholds could only be specified in packets or bytes. Now, all three units of measure are available. Once the threshold limits are configured in a policy map, the policy map can be used on multiple interfaces, including those with different amounts of bandwidth.

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12swrdql.htm

The following additional changes were made to the MIB tables:

- One new table was added (cbQosSetStats), and objects were added to an existing table (chQosSetCFG). These tables are associated with the various **set** commands available in the Cisco IOS software.

  For more information about the Cisco IOS **set** commands, see the Cisco command reference publications for the Cisco IOS release that you are using.

For a list of the specific MIB objects added, see the CISCO-CLASS-BASED-QOS-MIB-CAPABILITY.html file at the following URL:

http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&mibName=CISCO-CLASS-BASED-QOS-MIB-CAPABILITY

For more information about the preceding CBQoSMIB and the MIB objects and tables, and 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

QoS: Color-Aware Policer

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/12s_cap.htm

QoS: Frame Relay QoS Hierarchical Queueing Framework Support

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS: Match on ATM CLP

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12smcatm.htm

QoS: Percentage-Based Policing

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spctpg.htm

QoS: Percentage-Based Shaping

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spctsg.htm

QoS: Percentage-Based and Time-Based Policing Parameters

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spbtbp.htm

QoS: Per-Session Shaping and Queuing on LNS

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS Features for the Cisco 10000 Series

Cisco IOS Release 12.2(28)SB supports the following quality of service (QoS) features for the Cisco 10000 series:

- Dual Rate Three Color Policer
- Enhanced Random Early Detection (RED) Statistics
- Hierarchical Input Policing
- MLPPP with Link Fragmentation Interleave (LFI)
- Link Fragmentation Interleave over Frame Relay (FRF.12)
- Policy Map Scaling
- Random Early Detection (RED) with Queue-Limit
- Three Color Policer
- Three-Level Policy Maps
- VC Oversubscription

In addition to the Cisco 10000 series, the following features are also supported on the Cisco 7200 series, Cisco 7301, and Cisco 7304:

- Class-Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)
- Class-Based Marking
- Class-Based Policing
- Class-Based Shaping
- Class-Based Weighted Fair Queuing (CBWFQ)
- Diffserv Compliant WRED
- Low Latency Queueing (LLQ)

- Low Latency Queueing (LLQ) for Frame Relay
- Modular QoS CLI (MQC)
- Priority Queueing (PQ)
- QoS for Virtual Private Networks
- QoS Packet Marking
- QoS Policy Propagation via Border Gateway Protocol (QPPB)
- Random Early Detection (RED)
- Weighted RED (WRED)

For information about all features that are mentioned in this section, see the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_book09186a00805b9497.html

In addition, Cisco IOS Release 12.2(28)SB supports the following QoS features for the Cisco 10000 series.

Modular QoS CLI (MQC)-Based Frame Relay Traffic Shaping

Platform: Cisco 10000 series

The Modular QoS CLI (MQC)-based Frame Relay Traffic Shaping feature provides users with the ability to configure Frame Relay Traffic Shaping (FRTS) by using MQC commands.

QoS: Broadband Aggregation Enhancements, Phase 1

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbbbrs1a.htm

QoS: Enhanced Show Commands for Active Policies

Platform: Cisco 10000 series

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

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

RADIUS Features

Cisco IOS Release 12.2(28)SB introduces support for the following RADIUS features.

Framed-Route in RADIUS Accounting

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_fra22.htm

RADIUS-Based Lawful Intercept

Platforms: Cisco 7200 series, Cisco 7301

Note For the Cisco 7200 series, RADIUS-Based Lawful Intercept is supported only on Cisco 7200 VXR routers that are configured with an NPE-225, NPE-400, or NPE-G1. Support for the NPE-G2 will be available as of Cisco IOS Release 12.2(31)SB2.

RADIUS-Based Lawful Intercept is a Layer-2 feature, that is, a feature at the user-session level. With RADIUS-Based Lawful Intercept, traffic interception is provisioned through RADIUS and the resulting interception data is sent to the mediation device by using a RADIUS interface. The SNMP interface is completely bypassed.

For detailed information about RADIUS-Based Lawful Intercept, see the following Cisco document:

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

RADIUS NAS-IP-Address Configurability

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123b/123b3/gt_siara.htm

RADIUS Push for MOD CLI Policies

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

For detailed information about this feature, see the *Define Interface Policy-Map AV Pairs AAA* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xi7/123xiqos.htm

RADIUS Server Load Balancing

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7403, Cisco 10000 series

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

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

RADIUS Server Reorder on Failure

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/gt_rsrof.htm

radius-server source-port Command

Platform: Cisco 10000 series

The **radius-server source-ports extended** command enabled you to configure the NAS to use 200 ports in the range from 21645 to 21844 as the source ports for sending out RADIUS requests. With 200 source ports, up to 256*200 authentication and accounting requests can be outstanding at one time. During peak call volume, typically when a router first boots or when an interface flaps, the extra source ports allow sessions to recover more quickly on large-scale aggregation platforms.

To return to the default setting, in which ports 1645 and 1646 are used as the source ports for RADIUS requests, use the **no** form of this command.

For more information, see the *Cisco IOS Security Command Reference, Release 12.3* document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a008017cf42.html

RADIUS Timeout Set During Pre-Authentication

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftattr27.htm

RADIUS Tunnel Preference for Load Balancing and Fail-Over

Platform: Cisco 10000 series

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

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

RADIUS Attributes

Cisco IOS Release 12.2(28)SB introduces support for the following RADIUS attributes.

Connect-Info RADIUS Attribute 77

Platform: Cisco 10000 series

The Connect-Info RADIUS Attribute 77 feature introduces support for RADIUS attribute 77 (Connect-Info), which provides information about connection speeds, modulation, and compression for modem dial-in connections via RADIUS accounting “start” and “stop” records.

When the NAS sends attribute 77 in accounting “start” and “stop” records, you can measure—across the platform—the connect rates. That is, attribute 77 allows you to record “transmit” speed (the speed at which the NAS modem sends information) and “receive” speed (the speed at which the NAS receives information). These modem speeds for user sessions allow you to determine whether user modem connections renegotiate to lower speeds shortly into a session. If the transmit and receive speeds are different from each other, attribute 77 will report both speeds, which allows you to establish the modem connection speeds that customers gets from their session.

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

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/ra5f.htm

RADIUS Attribute 52 and 53 Gigaword Support

Platform: Cisco 10000 series

The RADIUS Attribute 52 and 53 Gigaword Support feature introduces support for attribute 52 (Acct-Input-Gigawords) and attribute 53 (Acct-Output-Gigawords). Attribute 52 keeps track of the number of times that 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 accurately account for and bill for usage.

RADIUS Attribute 77 for DSL

Platform: Cisco 10000 series

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 class name 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 82: Tunnel Assignment ID

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbrad_82.htm

RADIUS Attribute 91 Encrypted and Tagged VSA Support

Platform: Cisco 10000 series

For detailed information about this feature, see the *Encrypted and Tagged VSA Support for RADIUS Attribute 91* section in the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/6400/64_24b6.htm#115840

RADIUS Attribute Screening

Platform: Cisco 10000 series

For detailed information about this feature, which is also known as the RADIUS Attribute Value Screening feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftras.htm

Reserve Memory for Console Access

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/ftresmem.htm

Route Processor Redundancy Plus (RPR+)

Platforms: Cisco 7304, Cisco 10000 series

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

RSVP Refresh Reduction and Reliable Messaging

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

Secure Shell Version 2 Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

For detailed information about this feature, including the Secure Shell SSH Version 2 Client Support feature, also known as the SSHv2 feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_ssh2.htm

show Command Redirect

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftshowre.htm

Sticky IP

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

For detailed information about this feature, which is also known as the RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/radattr8.htm

Subscriber Service Switch

Platforms: Cisco 7200 series, Cisco 7301

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

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

TCP MSS Adjustment

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_admss.htm

Template ACL/12-Bit ACE

Platform: Cisco 10000 series

For detailed information about this feature, see "Chapter 19, Configuring Template ACLs" in the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/index.htm

Three-level Hierarchical Policy Support in PXF

Platform: Cisco 7304

The Modular QoS CLI (MQC) enables users to configure hierarchical policy maps, in which a grandparent policy uses a parent policy, and a parent policy uses a child policy. Support for all three levels of hierarchy was previously not available on the Cisco 7304 router, which used to support two levels of hierarchy. This feature is available in the PXF-processing path.

This feature is the addition of a third level of hierarchy within the MQC. It does not introduce any new commands. For information on configuring the MQC, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt8/qcfmcli2.htm

For additional information about this feature and all other features in the PXF-processing path, including restrictions, see the *Cisco 7304 Troubleshooting and Configuration Notes* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm#wp65935

Turbo Access Control List Scalability Enhancements [Phase 1]

Platform: Cisco 7304

In previous Cisco IOS releases, the ability of Turbo Access Control Lists to control PXF traffic could be limited. When the Turbo ACL classification tables grew large because of substantially-sized configurations and certain traffic patterns, all traffic that required ACL classification was punted to the Route Processor because the Turbo ACL table sizes exceeded the amount of available PXF memory.

This feature improves Turbo ACL scalability and enables support for large ACL tables.

This is a functional enhancement that introduces no new configuration.

UDI - Unique Device Identifier

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpepudi.htm

UDP Forwarding Support of IP Redundancy Virtual Router Group (VRG)

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftudpvrg.htm

Using 31-Bit Prefixes on IPv4 Point-to-Point Links

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft31addr.htm

VBR - NRT Oversubscription

Platform: Cisco 10000 series

For detailed information about this feature, see the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_book09186a00805b9497.html

Virtual Sub-Interface

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

For detailed information about this feature, see the *Configuration Enhancements for Broadband Scalability* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftbbenh.htm

Virtual Template Interfaces Limit Expansion

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

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

VLAN ID Rewrite

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this 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

VLANs over IP Unnumbered Subinterfaces

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtunvlan.htm

VPDN Features

Cisco IOS Release 12.2(28)SB introduces support for the following VPDN features.

Accounting of VPDN Disconnect Cause

Platforms: Cisco 7200 series, Cisco 7301

In the past, when a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) session failed or disconnected, the network access server (NAS) and Home GateWay (HGW) reported a very generic disconnect-cause code, such as "LOST CARRIER." These generic codes did not provide enough detailed information for accounting and debugging purposes. The Accounting of VPDN Disconnect Cause feature adds eight new disconnect-cause codes that describe the status of Virtual Private Dialup Network (VPDN) failures and disconnects more specifically than existing generic disconnect-cause codes. These new disconnect-cause codes can be found in the "RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values" appendix of the *Cisco IOS Security Configuration Guide, Release 12.2*:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00801fd174.html

RFC-2867 Tunnel Accounting

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

For detailed information about this feature, see the *RFC-2867 RADIUS Tunnel Accounting* document:

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

Shell-Based Authentication of VPDN Users

Platforms: Cisco 7200 series, Cisco 7301

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

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

Timer and Retry Enhancements for L2TP and L2F

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

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

Tunnel Authentication via Radius on LNS

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

For detailed information about this feature, see the *Tunnel Authentication via RADIUS on Tunnel Terminator* document:

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

VPDN Default Group Template

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

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

VPDN Group Session Limiting

Platforms: Cisco 7200 series, Cisco 7301

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

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

VPDN Multihop by DNIS

Platforms: Cisco 7200 series, Cisco 7301

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

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

VPN MIB Enhancements for per-VRF Session Counting

Platforms: Cisco 7200 series, Cisco 7301

An extension has been added to the virtual private dialup network (VPDN) CISCO-VPDN-MGMT-MIB that returns the total number of active sessions for each VPDN template. For customers that associate a VPDN template to each VPN routing and forwarding (VRF) instance, this MIB extension provides a way to monitor session usage per VRF.

Service providers can terminate sessions from multiple customer accounts on the same L2TP network server (LNS). Sharing of the LNS is done by creating one VRF per customer. Session limits on VPDN templates and VPDN groups are configured to control the allocation of sessions among customers and among users within the same customer account. A VPDN template is associated with each VRF, and its session limit restricts the total number of sessions for a customer account. Within that account, users may be assigned to different VPDN groups as their access requirements dictate. Session limits on VPDN groups further control the allocation of customer sessions among VPDN users. In such a setup, the service provider must use Simple Network Management Protocol (SNMP) to retrieve the total number of active sessions per customer to monitor their usage on the LNS.

Prior to the introduction of this MIB enhancement, only the total number of sessions on the LNS across all customer accounts could be retrieved through SNMP. This enhancement extends the CISCO-VPDN-MGMT-MIB to include a read-only table of VPDN template entries, with each entry reporting the number of active sessions across all VPDN groups that are associated with that template. The table entries can be accessed individually by using GET requests or consecutively using repeated GET-NEXT requests.

VPDN Session Disconnect AAA Attribute

Platforms: Cisco 7200 series, Cisco 7301, Cisco 10000 series

The VPDN Session Disconnect AAA Attribute feature adds support for a new vendor-specific attribute (VSA) to be included in accounting stop records. The VSA provides information about the reason for the session disconnect and the identity of the device that initiated the disconnection. This feature introduces support for the **accounting** keyword of the vpdn-logging command in Cisco IOS Release 12.2(28)SB, and is enabled by entering the **vpdn-logging accounting** command and keyword.

VRF-Aware VPDN Tunnels

Platforms: Cisco 7200 series, Cisco 7301

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

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

VPN Routing/Forwarding (VRF) CLI Command

Platform: Cisco 10000 series

The Virtual Private Network (VPN) routing/forwarding (VRF) command enables you to enter comments about your VRF configuration.

description *description string*

no description

The following output is from a configuration example:

```
Router(config)# ip vrf V4
Router(config-vrf)# ?
IP VPN Routing/Forwarding instance configuration commands:
  default       Set a command to its defaults
  description   VRF specific description
  exit          Exit from VRF configuration mode
  export        VRF export
  import        VRF import
  maximum       Set a limit
  no            Negate a command or set its defaults
  rd            Specify Route Distinguisher
  route-target  Specify Target VPN Extended Communities
Router(config-vrf)# desc
Router(config-vrf)# description ?
  LINE  Up to 80 characters describing this VRF
Router(config-vrf)# description This Is My 4th VRF
Router(config-vrf)# end
```

```
Router# sh ru | beg V4
ip vrf V4
 description This Is My 4th VRF
 rd 1:406
 route-target export 1:400
 route-target import 1:400
```

Warm Reload

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

The Warm Reload feature enables you to reload your routers without reading images from storage. That is, the Cisco IOS image reboots without ROM monitor mode (ROMMON) intervention by restoring the read-write data from a previously saved copy in the RAM and by starting execution without either copying the image from flash to RAM or self-decompressing the image. Thus, the overall availability of your system improves because the time to reboot your router is significantly reduced.

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtwrmrbt.htm

XML Interface to Syslog Messages

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftxmlsys.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 12.2SB that can apply to the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 router, and Cisco 10000 series routers.

Limitations and Restrictions in Cisco IOS Release 12.2(31)SB2

This section describes limitations and restrictions in Cisco IOS Release 12.2(31)SB2 and later releases.

NSE-150 USB Ports Not Supported

The NSE-150 USB ports are currently not supported on a Cisco 7304 router and should not be used for any reason. Support for USB ports on the NSE-150 will be introduced as an enhancement in a future release of Cisco IOS Release 12.2SB.

Limitations and Restrictions in Cisco IOS Release 12.2(28)SB

This section describes limitations and restrictions in Cisco IOS Release 12.2(28)SB and later releases.

High Availability Support for the Cisco 10000 Series

In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series supports Route Processor Redundancy Plus (RPR+), Stateful Switchover (SSO), and In Service Software Upgrade (ISSU). However for broadband aggregation features, the Cisco 10000 series supports RPR+ only.

ISSU Restriction for the Cisco 10000 Series

The In Service Software Upgrade (ISSU) feature for the Cisco 10000 series is not supported for MPLS VPN—Inter-Autonomous System (Inter-AS) configurations.

Per Precedence WRED Statistics

In the output of the **show policy-map interface** command, the Tail Drops counter indicates the number of packets dropped because the average queue length exceeded the maximum threshold for the given precedence. However, under burst conditions, it is possible that packets can be dropped because the queue is full. These packets are not counted as Tail Drops. The number of packets that are dropped under burst conditions when the queue is full are counted as Output Queue Drops.

RADIUS Attribute 31: PPPoX Calling Station ID

In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series does not support the RADIUS Attribute 31: PPPoX Calling Station ID feature.

Scaling Limits for L2TP Tunnels on the Cisco 10000 Series

For information about scaling limits for L2TP tunnels on the Cisco 10000 series, see the "Scaling Enhancements" section in the "Scalability and Performance" chapter of the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/scaling.htm#wp1030846

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.

System Limits for Policy Maps on the Cisco 10000 Series

The maximum number of classes supported per policy map on a Cisco 10000 series in Cisco IOS Release 12.2(28)SB is 64. The maximum number of policy maps supported per system is 4096.

tunnel vrf Command Not Supported on the Cisco 10000 Series

The Cisco 10000 series does not support the **tunnel vrf** *vrf-name* command in Cisco IOS Release 12.2(28)SB. Therefore, you cannot configure a tunnel for which both the source address and the destination address are located in a VPN routing/forwarding (VRF) instance, for example, when a tunnel is established between a customer edge (CE) router and a provider edge (PE) router. All tunnel source and destination addresses must be located in the global routing table.

The Cisco 10000 series does support a configuration in which the IP address of the tunnel itself is located in a VRF instance, for example, when the tunnel extends a VRF instance from one PE router to another PE router.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2SB that can apply to the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 router, and Cisco 10000 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/1654_pp.htm

- 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/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.
- 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(31)SB2

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(31)SB2 and later releases.

ARP Commands

As of Cisco IOS Release 12.2(31)SB2, new Address Resolution Protocol (ARP) commands are supported for the Cisco 7200 series, Cisco 7301, and Cisco 7304. For detailed information about these commands, see the *Monitoring and Maintaining ARP Information* document:

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

MLP Interface Range on the Cisco 10000 Series

As of Cisco IOS Release 12.2(31)SB2, the MLP interface range for multimember bundles on the Cisco 10000 series has been expanded. Earlier releases support a range of 1 through 9,999. As of Cisco IOS Release 12.2(31)SB2, the supported ranges are 1 through 9,999 and 65,536 through 2,147,483,647.

NPE-G2 Support for the show environment Command

The output of the **show environment** command has been modified to support the NPE-G2 network processing engine on the Cisco 7200 VXR in Cisco IOS Release 12.2(31)SB2 and later releases. For detailed information about this command, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xd4/showenv2.htm

Outdated ATA ROM Monitor Library (Monlib) [CSCsg64518]

Symptoms: The following symptoms may occur:

- When you enter the **dir** command for a disk from the ROM monitor (ROMMON) prompt, it make take too long to list the files or the command may time-out and fails to list the files.

- When you boot the router from a disk by entering the **boot** command or by initiating a switchover, it make take too long to load the image or the operation may time-out and the router fails to boot.

Conditions: These symptoms are observed on a Cisco router that has an ATA file system when the ATA ROM monitor library (Monlib) on the disk for which the **dir** command is entered or on which the boot image resides is very old. However, the symptoms can also occur because of other software issues or disk related-hardware issues.

Workaround: Upgrade the Monlib of the disk.

Further Problem Description:

To check the Monlib version of the disk, enter the **show disk0: filesys** command. In the output, look for the details under "ATA MONLIB INFO," as in the following example:

```
ATA MONLIB INFO

    Image Monlib size      69912
    Disk Monlib Size       69912
    Disk Space Available   73728
    Name                   NA
    End Sector             NA
    Start sector           NA
    Updated By             NA <-- Look for this information.
    Version                NA <-- Look for this information.
```

"NA" is very old image. You should see a Cisco IOS version that created the Monlib. The Cisco IOS version can be a good indicator of how old the Monlib is, as in the following example:

```
ATA MONLIB INFO

    Image Monlib size = 67288
    Disk monlib size = 70656
    Name = c10k-atafslib-m
    Monlib Start sector = 2
    Monlib End sector = 133
    Monlib updated by = C10K2-P11-M12.2(31)SB2 <--Look for the Cisco IOS software image
    Monlib version = 1 <-- Look for the MONLIB version no.
```

You can upgrade the Monlib through two methods:

- 1st Method: Enter the **upgrade filesystem monlib disk0:** command. Monlib software resides on the disk. By entering the above-mentioned command you upgrade the Monlib to the Monlib in the Cisco IOS software image that resides on the router without deleting the other files on the disk.

  There is a reserved space for the Monlib on the disk. If this reserved space is not sufficiently large enough to hold the new Monlib, the upgrade command may fail. (Note that this reserved space is not the disk space and should not be confused with the free space on the disk).

- 2nd Method: Upgrade by entering the **format** command for the disk, in which case the other files on the disk are deleted. When you format the disk, a reserved space is created and the Monlib is upgraded to the Monlib in the Cisco IOS software image that resides on the router.

QoS CLI Migration from PRE-2 to PRE-3

The Quality of Service (QoS) Command-Line Interface (CLI) Migration from PRE-2 to PRE-3 feature provides QoS CLI backward-compatibility between the Cisco 10000 series PRE-2 and PRE-3, thereby enabling the PRE-3 to accept PRE-2-style commands. For detailed information about this feature, see the following Cisco document:

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

Important Notes for Cisco IOS Release 12.2(28)SB

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(28)SB and later releases.

MPLS MTU Command Change

The behavior of the **mpls mtu** command has changed in Cisco IOS Release 12.2(28)SB and later releases. You cannot set the MPLS MTU value larger than the interface MTU value. This prevents problems such as dropped packets when MPLS MTU value settings are larger than interface MTU values. Cisco IOS software allows the MPLS MTU value to be higher than the interface MTU value only for interfaces that have a default interface MTU value of 1580 or less. For more information, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/newmtu.htm

Tuning I/O Buffers for Nonstop Forwarding (NSF)/Stateful Switchover (SSO) Functionality

For proper Nonstop Forwarding (NSF)/Stateful Switchover (SSO) functionality in scaled configurations, we recommend that you tune the number of I/O buffers on the Cisco 10000 series. (The default I/O buffer settings are good settings for standard configurations.) When NSF/SSO functionality is enabled, tune the I/O buffers by entering the following commands:

- **buffers small permanent 2500**
- **buffers small max-free 4000**
- **buffers small min-free 1000**
- **buffers middle permanent 2500**
- **buffers middle max-free 3500**
- **buffers middle min-free 1000**
- **buffers verybig permanent 1000**
- **buffers verybig max-free 2000**
- **buffers verybig min-free 150**

For more information about buffer tuning, see the *Buffer Tuning for all Cisco Routers* document:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a00800a7b80.shtml

If you need assistance with the buffer tuning process, call your support team.

Upgrading PCI Port Adapter Carrier Card ROMmon for the Cisco 7304 Router

Beginning in Cisco IOS Release 12.2(28)SB, the PCI Port Adapter Carrier Card (7300-CC-PA) requires a one-time ROMmon upgrade to function. If this upgrade is not performed, the PCI Port Adapter Carrier Card with the incompatible ROMmon will be deactivated until the PCI Port Adapter Carrier Card ROMmon upgrade is performed.

The upgraded ROMmon image is bundled with the Cisco IOS software image; no additional images need to be downloaded to perform the upgrade. The upgrade can be performed by answering a prompt that will appear when certain processes, including the Cisco IOS bootup process, recognize that the PA-CC ROMmon requires an upgrade. Other methods of upgrading PA-CC ROMmon exist.

For additional information on this process, see the *Upgrading PCI Port Adapter Carrier Card ROMmon* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/7304swf/paccrom.htm

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 12.2SB is based on Cisco IOS Release 12.2, many caveats that apply to Cisco IOS Release 12.2 also apply to Cisco IOS Release 12.2SB. 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:

Resolved Caveats—Cisco IOS Release 12.2(31)SB4

Cisco IOS Release 12.2(31)SB4 is a rebuild release for Cisco IOS Release 12.2(31)SB2 and supports only the Cisco 7200 series routers. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB4 but may be open in previous Cisco IOS releases.

Basic System Services

- 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.

Interfaces and Bridging

- 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

- CSCeg52659

  Symptoms: A Cisco 7200 series may not withdraw a BGP route from an iBGP peer.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(3) when the **clear ip bgp** *neighbor-address* **soft out** command is entered for one of the members of the peer group of which the Cisco 7200 series is a member and when some changes to the outbound policy are made to the same member of the peer group. This situation causes some prefixes to remain struck in the other members of the peer group. The symptom may also occur in other releases.

  The symptom is a very old behavior of the BGP peer group functionality: when one member of a peer group is cleared via either a hard reset or a soft reset and a policy change causes some of the prefixes to be withdrawn, inconsistencies may occur in the routes on the other members of the peer group.

  Workaround: For peer groups and neighbors that are members of a peer group, do not enter the BGP neighbor-specific **clear ip bgp** *neighbor-address* **soft out** command or the **clear ip bgp** *neighbor-address* command. Rather, enter the peer group-specific **clear ip bgp** *peer-group-name* **soft out** command or the **clear ip bgp** *peer-group-name* command.

- 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.

- CSCsg45637

  Symptoms: A traceback may be generated when the router accesses the “bgp_vpnv4_lookup_prefix” function.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP VPNv4.

  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.

Miscellaneous

- 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.

- CSCin99725

  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
  ```

- 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.

- 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

- 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.

- 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.

- CSCsg10134

  Symptoms: A router crashes when PPPoEoA sessions are torn down.

  Conditions: This symptom is observed when the maximum number of class-map instances are configured on the router.

Workaround: There is no workaround.

- CSCsg98611

  Symptoms: When you enter the **issu loadversion** command, the ISSU mail fail with the following error message:

  ```
  Active [ ] and Standby [ ] images should be the same for running loadversion
  ```

  Conditions: This symptom is observed in a rare situation on a Cisco router and occurs even when the Cisco IOS software images on the active and standby RPs are identical.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 he 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.

- 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.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(28)SB5.

Wide-Area Networking

- CSCse45182

  Symptoms: When a PPPoE server receives a second PADI from a client (that is, a PADI with the same unique client ID), the PPPoE server may send a PADS with an unknown MAC address.

  Conditions: This symptom is observed on a Cisco platform that functions as a PPPoE server that has established a PPPoE session with a client and occurs while PPP LCP negotiation is in progress.

  Workaround: There is no workaround.

- 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.

Open Caveats—Cisco IOS Release 12.2(31)SB3

Cisco IOS Release 12.2(31)SB3 is a rebuild release for Cisco IOS Release 12.2(31)SB2. This section describes a severity 1 caveat that is open in Cisco IOS Release 12.2(31)SB and its rebuilds. There are other open caveats in Cisco IOS Release 12.2(31)SB3. However, open caveats are normally listed only for maintenance releases, and the listing of CSCsh94923 is an exception.

Miscellaneous

- CSCsh94923

  Symptoms: The PXF engine may crash many times on a Cisco 10000 series that is functions as an L2TP Network Server (LNS). Each time that the PXF engine crashes, the following error message is generated:

  ```
  PXF DMA Error - Input Command Has Sequence Problem.
  ```

  This situation may cause the router to crash (that is, a software-forced crash may occur).

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 or PRE-3 and that runs Cisco IOS release 12.2(31)SB or one of its rebuilds when packets arrive on an L2TP tunnel and when the inner IP packet is destined for the router. This means that the destination address of the user packet that is carried within the L2TP tunnel is a local address on the LNS. One example of this condition is a keepalive message that is used between the subscriber and the LNS.

  Workaround: The router crashes because IP packets with an L3-destination address are sent to the router over PPP sessions. For packets that arrive on L2TP tunnels, deny access to the IP addresses of the router: on the LNS, configure an input ACL on the virtual template to deny IP access to all router interfaces.

  Further Problem Description: If this workaround is not an option for you because your system requires packets to be sent to the LNS, you must upgrade to a new software image. Download Release 12.2(31)SB3a that contains the fix for this caveat from the following location:

  http://www.cisco.com/cgi-bin/tablebuild.pl/0ecdfbf854c2eec61d29594911754 36f

  Note that Release 12.2(31)SB4 is the migration path for Release 12.2(31)SB3a.

- CSCsi18240

  Symptoms: After receiving packets through an L2TP tunnel and decapsulating these packets, a Cisco 10000 series that functions as an L2TP network server (LNS) may corrupt certain packets.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB3. There is a two-byte window for packets that are corrupted:

  - For a PRE-2: if the packet size including all encapsulations prior to L2TP decapsulation is 113 or 114 bytes, respectively, a one- or two-byte corruption of the inner IP packet occurs.
  - For a PRE-3: if the packet size including all encapsulations prior to L2TP decapsulation is 145 or 146 bytes, respectively, a one- or two-byte corruption of the inner IP packet occurs.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs only in Release 12.2(31)SB3 and does not affect other releases, nor does the symptom occur when the Cisco 10000 series functions as an L2TP access concentrator (LAC).

Resolved Caveats—Cisco IOS Release 12.2(31)SB3

Cisco IOS Release 12.2(31)SB3 is a rebuild release for Cisco IOS Release 12.2(31)SB2. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB3 but may be open in previous Cisco IOS releases.

Basic System Services

- 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.

  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.

  Workaround: There is no workaround.

- CSCse42235

  Symptoms: A packet of disconnect (POD) does not disconnect a user. When you enable the **debug aaa pod** command, the output shows the following:

  ```
  POD: Added Reply Message: No Matching Session
  POD: Added NACK Error Cause: Session Context Not Found
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for AAA when the Account-Session-Id is prepended with information. For example, if the Account-Session-Id is “7/0/0/1.40_00000039” in a POD, the POD fails to find a match.

  Workaround: If the Account-Session-Id is “7/0/0/1.40_00000039”, configure the POD application to take only the eight right digits: “00000039”.

- 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.

- CSCsh19482

  Symptoms: A Cisco 10000 series may crash and generate an "%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.

EXEC and Configuration Parser

- CSCsd45386

  Symptoms: When you enter the **write memory** command, the following error message and a traceback are generated:

  ```
  Router#wr Building configuration...
  % String too long to write to nvram (2578):Compressed configuration from 3452120 bytes
  to 786685 bytes[OK] Uncompressed configuration from 786685 bytes to 3452120 bytes
  ```

  Conditions: This symptom is observed on a Cisco router when the configuration is saved after you have entered the **parser config cache interface** command.

  Workaround: Disable the **no parser config cache interface** command.

Interfaces and Bridging

- 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.

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.

- CSCsc96746

  Symptoms: PIM may not choose 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.

- 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.

- 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.

- 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.

- 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

- CSCsc63871

  Symptoms: When IS-IS and CLNS are configured, a router may enter a state in which only one adjacency is shown in the output of the **show clns interface** command, even though the **show clns neighbors** command may correctly display all the neighbors that are connected to the interface.

  When this situation occurs and any one of the neighbors on the segment goes down, all routing updates may be lost. The single adjacency is torn down and despite the fact that the output of the **show clns neighbors** command still shows the neighbors, routing stops because there are no adjacencies.

  Conditions: This symptom is observed when an adjacency goes down while it is still in the INIT state. The symptom occurs because the adjacency counter is incorrectly decremented.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that reports only one adjacency.

  Alternate Workaround: Enter the **clear clns neighbors** command on the affected router.

Miscellaneous

- CSCdw80441

  Symptoms: A router crashes when you add a new SONET-related interface.

  Conditions: This symptom is observed on a Cisco router when no more memory is available.

  Workaround: There is no workaround.

- CSCej00340

  Symptoms: A Cisco 7304 crashes when you configure an SVC, unconfigure the SVC, configure a VC, and unconfigure the VC.

  Conditions: This symptom is observed on a Cisco 7304 when you perform the following actions:

  1. Configure an SVC, ping another interface, and unconfigure the SVC.
  2. Configure a VC, and ping another interface.
  3. Unconfigure the VC by entering the following commands:

     no ip routing

     no ip address *ip-address mask*

     no atm pvc *vcd vpi vci*

     aal5snap inarp *minutes*

  At this point, the router crashes.

  Workaround: Do not unconfigure a VC by using the method that is indicated in the Conditions above.

  Alternate Workaround: When the router has the **atm bandwidth dynamic** command enabled for an IMA group, remove this command to prevent the router from crashing.

- 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.

- CSCek55603

  Symptoms: Spurious memory accesses may occur on a Cisco 10000 series that is configured for PPPoA.

Conditions: This symptom is observed when you first add and then remove Variable Bit Rate (VBR) from a VC class for active PPPoA sessions.

Workaround: There is no workaround.

- CSCek56426

  Symptoms: The police counters are not properly incremented after a class has been added or deleted.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB2 when the total number of classes crosses a power-of-2 boundary after a class has been added to or deleted from the policy that is attached to an interface.

  For example, the symptom occurs under the following conditions:

  - There are 2, 4, 8, or 16 classes in a policy, including the class default, and you add a class.
  - There are 3, 5, 9, or 17 classes in a policy, including the class default, and you delete a class.

  Workaround: Detach the service policy from the interface, add or delete a class to or from the policy, and re-attach the policy.

- CSCek61519

  Symptoms: When you continuously perform OIRs of a SPA or port adapter that is installed in a Port Adapter Carrier Card, tracebacks are generated, and the router eventually crashes.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for HA.

  Workaround: There is no workaround.

- 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.

- CSCek65046

  Symptoms: After a microcode reload has occurred, traffic is dropped for all users that have a per-user ACL configured and for which the user IP address is specified in the ACL.

  Conditions: This symptom is observed on a Cisco 10000 series when a per-user ACL is applied to each session and when an ACL Template is enabled.

  Workaround: After you have performed a microcode reload, disconnect and reconnect all sessions. Note that it is very likely that a user will reconnect a session after traffic has dropped.

- CSCek65838

  Symptoms: The Lawful Intercept feature may not function for active tapped sessions after a microcode reload has occurred. Tapping works fine for new sessions that come up after the microcode reload has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Disconnect and reconnect the existing active tapped sessions after the microcode reload has occurred.

- CSCek67590

  Symptoms: MFR interfaces do not come up when the router boots.

Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS software image that includes the fix for CSCsg86572 and that has MFR interfaces configured on either a 1 port channelized OC-12 line card or a 4-port channelized OC-3 line card. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg86572. 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.

- CSCir01277

  Symptoms: A Cisco 7304 may reload unexpectedly because of a watchdog reset condition, which can be seen in the output of the **show version** command.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

- CSCsc66658

  Symptoms: A ping does not work when a loopback is configured on an interface.

  Conditions: This symptom is observed on a Cisco 7200 series, Cisco 7500 series, and Cisco 7600 series that are configured with a T3 interface.

  Workaround: There is no workaround.

- CSCsd47447

  Symptoms: A router crashes when a non-VLAN user class is configured under a parent policy with an action such as the **set qos-group** command.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs because a non-VLAN user class under a parent policy is an illegal configuration.

  Workaround: Do not configure a non-VLAN user class under a parent policy. However, note that you can configure a VLAN user class under a parent policy.

- 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.

- 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.

- CSCse84099

  Symptoms: When you configure the C2 overhead byte under SONET T3 or VT controllers on a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card, the T3 or VT controllers may not come up.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse98988

  Symptoms: DHCP control messages that are sent by a DHCP relay agent and that are destined for an external DHCP server do not pass through an interface of an Intelligent Service Gateway (ISG).

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the interface is configured for IP Session Creation.

  Workaround: There is no workaround.

- CSCsf17521

  Symptoms: When a hierarchical policy with CoS is configured, traffic shaping that is applied on the parent policy does not function properly for speeds that are slower than 2000 kbps because the throughput is reduced.

  Conditions: This symptom is observed on a Cisco 7304 when there is a priority class configured in a policy that is attached to an interface. The larger the packets, the more the throughput is reduced.

  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.

- CSCsf20019

  Symptoms: When traffic is being processed at a low speed such as 56 Kbps, intermittently, traffic comes to a complete halt on a Frame Relay subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2. The symptom occurs when the PXF engine stops dequeueing packets on the Frame Relay subinterface, causing the interface output queue to become wedged.

  Workaround: Remove the service policy from the subinterface and then re-apply the service policy to the subinterface.

  Further Problem Description: Without applying the workaround, about 60 to 70 minutes after the output queue has become wedged, the output queue starts to dequeue itself.

- 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.

- CSCsf97199

  Symptoms: High CPU usage may occur during the "XDR mcast" and "XDR RP" background processes. Each of these processes uses more than 30 percent of the CPU while no data traffic passes through the router.

  Conditions: This symptom is observed on a Cisco 10000 series but is platform-independent.

  Workaround: Reload the router.

- 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.

  Possible 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.

- CSCsg64438

  Symptoms: When a prepaid service is unapplied from rules, the accounting stop record does not contain packet counts and octet counts.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the **service-policy type service unapply name** *policy-map-name* command (in which the *policy-map-name* argument indicates the prepaid service) is configured in the rules.

  Workaround for the packet counts: There is no workaround.

  Workaround for the octet counts: Look for the information in the following attributes that are present in the according stop record:

  ```
  ssg-control-info [253] 6 "I<high>;<low>" <low> indicates the input octets.
  ssg-control-info [253] 6 "O<high>;<low>" <low> indicates the output octets.
  ```

- CSCsg71200

  Symptoms: During dynamic VLAN class modifications, the queueing policy inheritance fails. This situation causes traffic to be dropped.

  Conditions: This symptom is observed on a Cisco 10000 series that has a hierarchical queueing policy for VLAN classes and a flat shaper for the class default. When the VLAN class modifications occur that shift the matching subinterfaces to the class default, then back to the original VLAN class, and then to another VLAN class, the child queues are not created, causing traffic to drop.

  Workaround: Remove and re-attach the hierarchical queueing policy.

- CSCsg71247

  Symptoms: Non-Priority Queuing (PQ) traffic in a class default in a QoS policy that includes the **match vlan** command is not dequeued during oversubscription of the PQ class.

  Conditions: This symptom is observed on a Cisco 10000 series only when there are multiple VLAN classes and when there are child queueing policies in the class default and the VLAN classes. The PQ policer takes the interface bandwidth as reference, causing policing to occur at the wrong rates and starvation of non-PQ child classes in the class default. The symptom does not occur for child classes in a VLAN class.

  Workaround: There is no workaround.

- CSCsg71400

  Symptoms: Traffic stops matching to a child policy.

  Conditions: This symptom is observed on a Cisco 10000 series when an interface has a hierarchical policy defined on a PVC, when you remove the child policy, and when you re-attach the child policy to the parent policy of the hierarchical policy. In this situation, the traffic no longer matches to the child policy.

  Workaround: Detach the hierarchical policy from the PVC, modify the child policy, and re-attach the hierarchical policy to the PVC.

- CSCsg72950

  Symptoms: Temperature alarms on a Cisco 10000 series PRE-3 assert at lower ambient temperatures than necessary.

  Conditions: This symptom may occur in an operating environment in which the ambient temperature is in the low 30s (degrees Celsius).

  Workaround: You can reprogram the temperature alarm thresholds. The recommended thresholds are:

  ```
  inlet minor: 41 C
  inlet major: 51 C
  inlet critical: 73 C
  outlet minor: 48 C
  outlet major: 58 C
  outlet critical: 85 C
  ```

- CSCsg75132

  Symptoms: When the standby PRE comes up, the following error message is generated on the console of the active PRE:

  ```
  REDUNDANCY-3-IPC: cannot open standby port session in use
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has dual PRE engines that function in ISSU, RPR+, or SSO mode. The symptom may also occur on other platforms that support Enhanced High System Availability (EHSA) such as the Cisco 7304 and Cisco AS5850.

  Workaround: There is no workaround.

  Further Problem Description: The error message indicates that some of the Entity MIB information such as standby PRE version, standby flash information, and standby EEPROM data has failed to synchronize to the active PRE.

- CSCsg75266

  Symptoms: A Cisco 10000 series with a PRE-3 may crash when you delete an ATM VC.

Conditions: This symptom is observed when the following sequence of events occur:

- You enter the **protocol pppoe** command to configure an ATM VC.
- You enter the **no protocol pppoe** command to remove PPPoE from the VC.
- You delete the ATM VC.

Workaround: There is no workaround.

- CSCsg78469

  Symptoms: A Cisco 10000 series may generate an “SW_CORRUPTION” error message when a service of the ISG Layer 4 Redirect feature is removed from a session in a broadband aggregation (BBA) configuration.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) when a service of the ISG Layer 4 Redirect feature is removed via the configuration of a service policy.

  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(28)SB5 (PGP ver.4)
  - Release 12.2(27)SBC5 (PGP ver.4)

  On the Cisco 7600 series:

  - Release 12.2(18)SXD5 (PGP ver.3)
  - Release 12.2(33)SRA1 (PGP ver.4)

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsh06611

  Symptoms: A Cisco 10000 series that has a PRE2 may crash when you clean the configuration via TFTP.

Conditions: This symptom is observed when you first define hierarchical queuing for a QoS VLAN-group policy with a large number of VLAN classes, each class with matching subinterfaces, and then you clean the configuration. The symptom occurs only when you download the configuration via TFTP to the running configuration and when you clean the configuration via TFTP.

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCsh24174

  Symptoms: A "%CHKPT-4-INVALID error" error message is generated when you upgrade the Cisco IOS software image to Release 12.2(31)SB.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for ISSU.

  Workaround: There is no workaround.

- CSCsh26001

  Symptoms: When the MIB variable tftpHost is empty (that is, it is not defined), you cannot copy an image via ISSU.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB.

  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.

- CSCsh33371

  Symptoms: A static Auto-Rendezvous Point (Auto-RP) may not function when both a Frame Relay main interface and one of its subinterfaces have the **ip pim sparse-dense mode** command enabled.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router in an MVPN network.

  Workaround: Remove the **ip pim sparse-dense mode** command from the main interface but leave the **ip pim sparse-dense mode** command enable on the subinterface.

- 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.

- 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.

- 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.

- CSCsh46427

  Symptoms: A spurious memory access is generated when you remove the **no evaluate tcptraffic** command.

  Conditions: This symptom is observed on a Cisco router that is configured with IP ACLs.

  Workaround: There is no workaround.

- CSCsh46790

  Symptoms: Traffic may no longer be forwarded over a PPPoA session when you remove a policy map from the ATM VC on which the PPPoA session is established.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 when the policy map is applied to the ATM VC and then removed via the **no service-policy output** *policy-map-name* command.

  Workaround: There is no workaround.

  Further Problem Description: With PPPoA (or PPPoEoA), PXF queues are created on the virtual access interface (VAI) even though the policy map is applied to the VC. When the VC policy map is removed, the default PXF queue is also removed from the VAI, causing a traffic black hole.

- CSCsh47261

  Symptoms: A Cisco 10000 series may either fragment or drop an IPv4 packet when the IPv4 packet length is smaller than the configured MTU. Drops may occur when the DF bit is set in the IPv4 header.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB2 when an ARP cache entry times out or when a static ARP entry is deleted from the configuration.

  Possible Workaround: Increase the MTU of the interface MTU to mitigate the symptom.

  Further Problem Description: The unexpected fragments or packet drops occur in a very short time window after the ARP entry is removed.

- 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.

- CSCsh56152

  Symptoms: You cannot suppress the creation of F4 OAM VCs when you configure a PVP at the subinterface level. If the PPP client does not support OAM, this situation could prevent the PPP session from being initiated.

  Conditions: This symptom is observed on a Cisco router and occurs because there is no *no-f4-oam* argument available when you configure a PVP on a subinterface.

The following command options are available at the main interface level:

router(config-if)#**atm pvp 2 10000 ?**
cdvt [Cell Delay Variation Tolerance (CDVT)]
no-f4-mgmt [inhibits the management of f4 oam vcs]
no-f4-oam [inhibits the creation of f4 oam vc's]
cr

However, only the following options are available at the sub interface level:

router(config-if)#**atm pvp 2 10000 ?**
cdvt [Cell Delay Variation Tolerance (CDVT)]
cr

Workaround: Do not configure the PVP on the subinterface. Rather, configure the PVP on the main interface, for which the *no-f4-oam* argument is available.

- CSCsh63369

  Symptoms: All traffic that arrives on a PPP over VLAN session or PPPoE over QinQ session may be processed indiscriminately by the class default of a service policy that is applied to the VLAN or QinQ VLAN.

  Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS software image that integrates the fix for caveat CSCsg89172. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg89172. 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.

TCP/IP Host-Mode Services

- 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 send 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.

- 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.

Wide-Area Networking

- CSCsf29303

  Symptoms: On a Cisco 7200 series, an error message and traceback such as the following are generated and/or the router may crash because of an "%ALIGN-1-FATAL: Illegal access to a low address" condition:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=652AA0C0, count=0
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x621FD418 reading 0x278
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB when end-to-end Frame Relay fragmentation is configured on an interface.

  Workaround: Do not configure end-to-end Frame Relay fragmentation. Rather, configure end-to-end fragmentation that is based on a map class, that is, attach to each PVC a map class that contains an end-to-end fragmentation configuration.

- CSCsg56725

  Symptoms: When you enter the **terminate-from hostname** *host-name* 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.

- 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 have attempted to configure Frame Relay fragmentation on a Frame Relay main interface that has a service policy on a subinterface, when you then have removed 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.

Open Caveats—Cisco IOS Release 12.2(31)SB2

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(31)SB2. All the caveats listed in this section are open in Cisco IOS Release 12.2(31)SB2. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCse42235

  Symptoms: A packet of disconnect (POD) does not disconnect a user. When you enable the **debug aaa pod** command, the output shows the following:

  ```
  POD: Added Reply Message: No Matching Session
  POD: Added NACK Error Cause: Session Context Not Found
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for AAA when the Account-Session-Id is prepended with information. For example, if the Account-Session-Id is "7/0/0/1.40_00000039" in a POD, the POD fails to find a match.

  Workaround: If the Account-Session-Id is "7/0/0/1.40_00000039", configure the POD application to take only the eight right digits: "00000039".

- CSCsg74449

  Symptoms: When a PVC with a policy map is unconfigured on a 1-port OC-12 ATM line card, a Cisco 7304 with an NSE-100 crashes and generates an "ALIGN-1-FATAL" error message.

  Conditions: This symptom is observed on a Cisco 7304 that functions as both a core router and a route reflector (RR) when you unconfigure the PVC while traffic is being processed.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsd45386

  Symptoms: When you enter the **write memory** command, the following error message and a traceback are generated:

  ```
  Router#wr Building configuration...
  % String too long to write to nvram (2578):Compressed configuration from 3452120 bytes
  to 786685 bytes[OK] Uncompressed configuration from 786685 bytes to 3452120 bytes
  ```

  Conditions: This symptom is observed on a Cisco router when the configuration is saved after you have entered the **parser config cache interface** command.

  Workaround: Disable the **no parser config cache interface** command.

IP Routing Protocols

- CSCek39951

  Symptoms: CPUHOG messages are generated when the standby RP boots with a very large configuration such as more than 1000 BGP peers.

  Conditions: This symptom is observed on a Cisco 10000 series with a PRE-3 when the *milliseconds* argument of the **process-max-time** *milliseconds* command has a value of 50 ms. The symptom is platform-independent.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsc32700

  Symptoms: A router may not resume to forward VPN traffic after you have entered the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco router that function as a PE router in a VPN environment.

  Workaround: There is no workaround.

- CSCsc37461

  Symptoms: A PE router that functions in an MPLS VPN configuration may take a long time to converge.

  Conditions: This symptom is observed when an interface goes down and when an MP-BGP next hop that points to this interface is no longer reachable. This MP-BGP next hop remains unreachable until the Interior Gateway Protocol (IGP) finds an alternate path. If the BGP scanner runs while the MP-BGP next hop is unreachable, VRF routes that use this MP-BGP next hop may be removed from the VRF routing table. However, usually, when the next BGP scanner runs, these VRF routes are updated and then re-imported into VRF routing table.

  Workaround: The probability for the symptom to occur depends on the elapse time between the interface going down and the IGP convergence and can be decreases by tuning the IGP parameters for a faster convergence.

- 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.

- 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.

- 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 12.4, or Release 12.4T.

  Workaround: Enter the **clear ip bgp** *neighbor-address* command to enable the networks to enter the MBGP table.

- CSCsg78768

  Symptoms: Multiprotocol BGP (mBGP) peers may not receive modified cost-community routes.

  Conditions: This symptom is observed on a Cisco router after route maps have been applied. The router checks if the modified routes are sent to its peers. However, the multicast peers do not receive the modified routes.

  Workaround: There is no workaround.

  Further Problem Description: The routes are sent properly to unicast and VPN peers.

- CSCsg84949

  Symptoms: After a router has booted, BGP links start to flap, and the router crashes.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router, that is connected to a route reflector (RR), and that is configured with 500 VRFs and 500 routes per VRF.

  Workaround: There is no workaround.

Miscellaneous

- CSCdy19642

  Symptoms: Performance counters under T1.5, T3, and VT2 controllers for T1 and E1 interfaces on a channelized line card are not properly updated and displayed.

  Conditions: This symptom is observed on a Cisco 10000 series when cyclic redundancy check (CRC) errors occur.

  Workaround: There is no workaround.

- CSCeh04362

  Symptoms: Routed Bridge Encapsulation (RBE) does not function in an IPv6 environment.

  Conditions: This symptom is observed on a Cisco router when traffic attempts to pass through an interface that is configured for both RBE and IPv6.

Workaround: There is no workaround.

- CSCeh71337

  Symptoms: Traffic loss may occur for more than 80 seconds after a high availability (HA) switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that has line cards that are configured for Automatic Protection Switching (APS).

  Workaround: There is no workaround.

- CSCeh92464

  Symptoms: The output of the **show policy-map** command may show incorrect WRED counters.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that has DSCP-based WRED enabled.

  Workaround: There is no workaround.

- CSCej02774

  Symptoms: When you use the **BREAK** key to interrupt the image boot process and then enter the **dir** command from the ROMmon prompt, a recurring "Arithmetic Overflow Exception" may occur.

  Conditions: This symptom is observed on a Cisco 10000 series that has 104480 Kbytes of main memory and occurs only when a file system device driver is recursively loaded because you used the **BREAK** key to interrupt the image boot process and then entered the **dir** command without first resetting the ROMmon.

  Workaround: Let the image boot and then enter the **dir** command. If you must interact with the file system via the ROMmon when the boot process has been interrupted, enter the **reset** command. If autoboot is enabled, use the **BREAK** key immediately after the banner line appears on screen.

- CSCej07319

  Symptoms: A router may crash when you configure Mobile IP.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.12SB or Release 12.2SBC.

  Workaround: There is no workaround.

- CSCej62041

  Symptoms: The following symptoms may occur:

  – When a service policy for traffic shaping is applied to an mGRE tunnel interface, most of the packets are dropped.

  – When a service policy is applied to an outbound physical interface, very few or none of the packets are matched, policed, and/or shaped, or the queuing features do not function.

  Conditions: This symptom is observed when multicast fast switching is configured over mGRE tunnels.

  Workaround: There is no workaround.

- CSCej66992

  Symptoms: The statistic counters for a parent policy and for parts of a child policy may be incorrect in the output of the **show policy-map interface** *interface-name* command.

  Conditions: This symptom is observed on a Cisco 10000 series when an egress policy map is attached to an interface, when the egress policy map has a nested child service policy, and when you modify class maps in the child policy.

Workaround: Remove the child policy map from the parent policy map before you modify the child class maps. Then, re-attach the child policy to the parent.

- CSCek19916

  Symptoms: When more than 100 pseudowire (PW) VCs are brought down simultaneously, enqueue failures occur, preventing PWE3-MIB notifications from being sent for the PW VCs beyond the first 100 PW VCs that went down.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs because the notification queue of the PWE3-MIB is full.

  Workaround: Configure a network management station (NMS) to report that a state change occurs for PW VCs, for example, via the MPLS-LDP-MIB.

- CSCek20073

  Symptoms: A Cisco 10000 series may reload unexpectedly during HA configuration synchronization operations.

  Conditions: This symptom is observed very rarely on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek24445

  Symptoms: A Cisco 10000 series that has a scaled configuration may crash when an SSO switchover occurs.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in the following large Remote Access (RA) to MPLS VPN configuration:

  - 250 PPPoA sessions over one VPN.
  - 500 MPLS VPNs with eBGP
  - 500 L2vPNs (EoMPLS) VCs
  - 200 ATMoMPLS sessions
  - 200 FRoMPLS sessions
  - mVPN on T1, E1, and MLP links
  - MPLS TE tunnels
  - IPv4 and IPv6 tunnels

  Workaround: There is no workaround.

- CSCek35534

  Symptoms: Packet loss may occur on voice or video streams when you apply an output policy on the interface.

  Conditions: This symptom is observed on a Cisco 10000 series when traffic is sent at line rate.

  Workaround: There is no workaround.

- CSCek36747

  Symptoms: When Internet mix (IMIX) traffic is processed over an L2VPN pseudowire that is configured for shaping on a disposition PE router, shaping does not function as expected, causing packets to be dropped.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a disposition PE router.

Workaround: There is no workaround.

- CSCek41565

  Symptoms: The maximum latency of priority queueing (PQ) may be too high for some ports.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCek41755

  Symptoms: The on-demand address pool (ODAP) manager does not create the required number of subnets.

  Conditions: This symptom is observed on a Cisco router that has the DHCP ODAP Server Support feature enabled.

  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.

- CSCek43707

  Symptoms: When an interface is configured for Routed Bridge Encapsulation (RBE) and Dynamic Host Control Protocol (DHCP) and when an HA switchover occurs, routes do not synchronize on the new standby RP.

  Conditions: This symptom is observed on a Cisco 10000 series after you have performed an OIR of the interface that is configured for RBE and DHCP. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCek44091

  Symptoms: An MPLS tunnel goes down after you have changed the tunnel priority from 3 to 2 via the **tunnel mpls traffic-eng priority** command.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCek49973

  Symptoms: When Multilink PPP (MLP) is configured to use a virtual access interface as the bundle interface and when you apply a service policy with bandwidth guarantees that are higher than the bandwidth guarantees of the virtual access interface, an error message is generated because the service policy is not rejected nor enters the suspended mode.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured for MLP and QoS.

  Workaround: Add more links to the bundle interface and clear the virtual access interface.

- CSCek52663

  Symptoms: Memory failures may occur on a Cisco 10000 series when you repeatedly perform OIRs.

  Conditions: This symptom is observed very rarely on a Cisco 10000 series that runs Cisco IOS Release 12.2SB after repeated OIRs of a line card that is configured for Auto VCs and that has active PPPoA sessions.

  Workaround: There is no workaround.

- CSCek52743

  Symptoms: cRTP may become disabled on an interface when you disable and re-enable the **ip rtp header-compression** command on the interface.

  Conditions: This symptom is observed on a Cisco router that functions in an MLP configuration when the link (such as a Frame Relay link) and the MLP bundle clone from the same virtual template.

  Workaround: Reset the interface.

- CSCek53834

  Symptoms: When you repeatedly clear PPPoA sessions, memory may become fragmented, and eventually may become so low and fragmented that you cannot execute the **show running-config** command.

  Conditions: This symptom is observed on a Cisco 10000 series when you repeatedly clear PPPoA PTA sessions by entering the **clear pppatm** command.

  Workaround: There is no workaround.

- CSCek55603

  Symptoms: Spurious memory accesses may occur on a Cisco 10000 series that is configured for PPPoA.

  Conditions: This symptom is observed when you first add and then remove Variable Bit Rate (VBR) from a VC class for active PPPoA sessions.

  Workaround: There is no workaround.

- CSCek56426

  Symptoms: The police counters are not properly incremented after a class has been added or deleted.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB2 when the total number of classes crosses a power-of-2 boundary after a class has been added to or deleted from the policy that is attached to an interface.

For example, the symptom occurs under the following conditions:

- There are 2, 4, 8, or 16 classes in a policy, including the class default, and you add a class.
- There are 3, 5, 9, or 17 classes in a policy, including the class default, and you delete a class.

Workaround: Detach the service policy from the interface, add or delete a class to or from the policy, and re-attach the policy.

- 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.

- CSCsc74782

  Symptoms: The number of BECN-tagged packets that are sent by one CE router does not match the number of BECN-tagged packets that are received by another CE router. This symptom can be verified in the output of the **show frame-relay pvc** command.

  Conditions: This symptom is observed under the following conditions:

  - Both CE routers are connected to PE routers.
  - One of the PE routers is a Cisco 10000 series and the other PE router is a Cisco 7500 series.
  - There is an AToM tunnel between the PE routers and the AToM tunnel was set via Xconnect commands.
  - The AToM tunnel is configured for DLCI-to-DLCI switching.

  Workaround: There is no workaround.

- CSCsd23425

  Symptoms: QoS statistics are not reflected properly in the output of the **show policy-map session uid** *uid-number* command.

  Conditions: This Symptom is observed on a Cisco 10000 series is has a PRE2 and that functions as a LAC.

  Workaround: There is no workaround.

- CSCsd47447

  Symptoms: A router crashes when a non-VLAN user class is configured under a parent policy with an action such as the **set qos-group** command.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs because a non-VLAN user class under a parent policy is an illegal configuration.

  Workaround: Do not configure a non-VLAN user class under a parent policy. However, note that you can configure a VLAN user class under a parent policy.

- CSCsd82031

  Symptoms: I/O memory may become depleted on a Cisco 7304 because of IPC buffer usage. This situation may also cause the following error messages to be generated:

  ```
  %WSIPC-3-SYSCALL: System call for command 7 (port 4/1): ipc_send_rpc_blocked
  timed-out (Cause: timeout)
  -Traceback= 406EB43C 40924448 409245FC 40924750
  ```

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and three Port Adapter Carrier Cards (7300-CC-PAs) in which 8-port serial, X.21 port adapters (PA-8T-X21) are installed and occurs when many serial interfaces are reset.

  Workaround: Prevent the serial interfaces from being reset.

- CSCse14947

  Symptoms: A standby RP may continuously reload after you have entered the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco router that has the **atm pvp** *vpi* **l2transport** interface configuration command enabled for an AToM tunnel that functions in ATM PVP mode.

  Workaround: Disable the **atm pvp** *vpi* **l2transport** interface configuration command. When you do so, the standby RP comes back up.

- CSCse21604

  Symptoms: When a failure occurs on a CE router, the primary pseudowire switches over to the backup pseudowire. However, when the failure is corrected, the backup pseudowire does not fall back to the primary pseudowire but remains in the "UP" state.

  Conditions: This symptom is observed on a Cisco router that functions as a CE router when the ATM-to-ATM Local Switching and L2VPN Pseudowire Redundancy features are configured with an AToM (like-to-like) pseudowire class. The symptom occurs only in an ATM configuration.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that faces the PE router. Doing so forces the primary pseudowire to come up.

- CSCse29304

  Symptoms: The call setup rate on an LNS may be very slow.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an LNS.

  Workaround: There is no workaround.

- CSCse30504

  Symptoms: A CPUHOG condition may cause an interface of an OC-12 port line card to flap even though the remote link is still active.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse41607

  Symptoms: All ingress traffic into a Gigabit Ethernet (GE) SPA may be ignored.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 or NSE-150 when the following conditions are present:

  - PXF is disabled.
  - The router has an MSC-100 in which a GE SPA is installed.

  - The router processes traffic at GE rate (or, at a rate that causes the CPU usage of the NSE to be at 100 percent).
  - You perform a series (at least 5 or 6) of physical OIRs of the MSC-100.

  You must reload the router to recover proper functionality.

  Workaround: Enable PXF.

  Alternate Workaround: Do not perform a series of consecutive physical OIRs of the MSC-100 while traffic is being switched and the CPU usage of the NSE is at 99 or 100 percent.

- CSCse55371

  Symptoms: A policing error may occur on a DHCP IP session when local authorization is configured.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

  Workaround: Configure a static IP session and RADIUS authorization.

- CSCse59604

  Symptoms: The CPU of a router may spike when an empty control policy is configured on an interface and when another non-empty control policy is configured at either the global or the interface level.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

  Workaround: Do not configure an empty control policy on the interface.

- CSCse78015

  Symptoms: When you change the MTU on a virtual template, an incorrect value is used for the IP MTU.

  Conditions: This symptom is observed when the value that is set as the MTU via the **mtu** *bytes* command is automatically entered as the maximum value for *bytes* argument of the **ip mtu** *bytes* command.

  This symptom occurs only with MTU values in the range of 64 to 67 when an IP MTU is also configured. MTU values from 68 up to the interface maximum work fine. Some interfaces allow a minimum MTU value of 64 but the minimum IP MTU value is 68, therefore, MTU values in the range of 64 to 67 may cause a problem.

  For example, when you change the MTU via the **mtu** *bytes* command to a minimum value of 64 while the IP MTU has a minimum value of 68, the IP MTU is automatically changed to a maximum value of 64, which causes the IP MTU to cover an incorrect range.

  Workaround: Avoid MTU values in the range from 64 to 67.

- CSCse83462

  Symptoms: CEF convergence takes a long time in a load-balancing configuration on a Cisco 10000 series that has a PRE-3.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router in an MPLS VPN configuration and that is connected to two P routers. The symptom occurs after an interface has flapped.

  Workaround: There is no workaround.

- CSCse84099

  Symptoms: When you configure the C2 overhead byte under SONET T3 or VT controllers on a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card, the T3 or VT controllers may not come up.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse98988

  Symptoms: DHCP control messages that are sent by a DHCP relay agent and that are destined for an external DHCP server do not pass through an interface of an Intelligent Service Gateway (ISG).

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the interface is configured for IP Session Creation.

  Workaround: There is no workaround.

- CSCsf02261

  Symptoms: Multilink PPP (MLP) traffic fails when it is forwarded via a LAC (or LNS) over an PPPoA session.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC and that runs Cisco IOS Release 12.2(28)SB2. The symptom occurs when the MLP traffic comes from an ADSL router via an L2TP session and when the CPE connects to the LAC via PPPoA.

  Workaround: Configure the CPE to connect to the LAC via PPPoEoA instead of PPPoA.

- CSCsf20019

  Symptoms: When traffic is being processed at a low speed such as 56 Kbps, intermittently, traffic comes to a complete halt on a Frame Relay subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2. The symptom occurs when the PXF engine stops dequeueing packets on the Frame Relay subinterface, causing the interface output queue to become wedged.

  Workaround: Remove the service policy from the subinterface and then re-apply the service policy to the subinterface.

  Further Problem Description: Without applying the workaround, about 60 to 70 minutes after the output queue has become wedged, the output queue starts to dequeue itself.

- CSCsf20691

  Symptoms: When an unknown Change of Authorization (CoA) service policy is pushed to an active ISG session, the service policy is not acknowledged and the ISG session is terminated.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG. The following is an example of the conditions under which the symptom occurs:

  A CoA service policy is pushed in the following VSA format:

  ```
  vsa cisco generic 1 string "subscriber:policy-directive=service-policy type service
  name BOOTONE"
  ```

  The BOOTONE service does not exist in the local ISG profile database, nor in the AAA service database.

  Workaround: There is no workaround.

- 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.

- CSCsg09230

  Symptoms: When traffic is processed over a session after you have removed the standby RP, a memory leak may occur in the an “adj_allocate_setup_and_lock” process.

  Conditions: This symptom is observed on a Cisco router that is configured for PTA and L2TP sessions.

  Workaround: Do not remove the standby RP after you have booted the router.

- CSCsg10730

  Symptoms: A multicast ping packet that is sent from one CE router to another CE router may be dropped.

  Conditions: This symptom is observed on a Cisco 7304 and Cisco 10000 series that function in a Multicast VPN (MVPN) configuration with Autonomous System Border Routers (ASBRs).

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur on a Cisco 7200 series.

- CSCsg18588

  Symptoms: A router may be unable to bring up more than 36,000 sessions in a configuration with VC-classes and QoS policy maps. Memory errors may be reported and sessions may be disconnected.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG and occurs only when all of the following criteria are present:

  - There are more than 38,000 VCs configured.
  - The VCs have VC-classes.
  - The VCs have outbound policy maps configured.

  Workaround: There is no workaround.

- CSCsg22762

  Symptoms: The cache entries of Flexible NetFlow may lock up for multicast traffic.

  Conditions: This symptom is observed during normal Flexible NetFlow operation when multicast traffic enters the router.

  Workaround: There is no workaround.

- CSCsg23257

  Symptoms: Duplication or tapping does not occur on a Cisco 7301 that is configured for Lawful Intercept (LI).

  Conditions: This symptom is observed when a PPPoE session is set up at the client and when you attempt to duplicate packets at a Cisco 7301 that functions as a LAC and that is configured for LI. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg25018

  Symptoms: The working interface is not restored to the active state but remains inactive while the protect interface remains active in the following situation:

  - The working interface has the **pos ais-shut command enabled.**
  - You enter the **aps revert** command to enable a switchover from the protect interface to the working interface.
  - You enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the working interface.

  The working interface should become active but does not do so.

  Conditions: This symptom is observed on a Cisco 7304 when interfaces of an OC-3 POS line card are configured for APS and occurs only in a back-to-back bi-directional APS configuration. The symptom does not occur with an OC-3 POS port adapter.

  Workaround: Perform a soft OIR of the working interface.

  Alternate Workaround: Disable the **pos ais-shut command on the working interface.**

  Possible Workaround: Enter the **pos scramble-atm** on the active interface. Note that this workaround does not always work.

- CSCsg32170

  Symptoms: When dynamic bandwidth selection (DBS) is enabled on an ATM VC, policing on PPPoX sessions may exceed the configured policing rates.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) when the following sequence of events occurs:

  1. Configure a QoS policy in the egress direction on the ATM VC that has DBS enabled.
  2. Bring up a PPPoX session and download the QU and QD values of the account information at the start of the session.
  3. Bring up one more new session and then tear down this session.

  After you have torn down the second session, traffic flowing through the first session may exceed the policing values that have been configured.

  Workaround: Disable DBS on the interface on which the ATM VC is configured.

- CSCsg32465

  Symptoms: Incorrect police percent conversions occur in the second and third levels of a policy.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg34025

  Symptoms: A Cisco 7206VXR crashes because of a software bus error when the main interface is shut down and brought up again.

  Conditions: This symptom is observed on a Cisco 7206VXR with an NPE-G1 that runs Cisco IOS Release 12.2(28)SB5 and that has a Frame Relay map class with a QoS service policy that is applied to an MFR subinterface.

  Workaround: Remove the Frame Relay map class from the MFR subinterface.

- CSCsg38900

  Symptoms: The PXF engine on an NSE-150 may crash at PXF column 2 when a switchover occurs while traffic is being processed. When this situation occurs, no information is written to the crashinfo file.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for HA, that has 250 FEC VRFs, and that has the **ip cef** and **ip pxf** commands enabled.

  Workaround: Do not enable the **ip cef** command in an HA configuration. Rather, enable the **ip cef distributed** command.

- CSCsg38944

  Symptoms: The following error message is generated when a PVC is shut down.

  ```
  %ATM-3-FAILMODIFY VC: failed to modify messages in the log
  ```

  Conditions: This symptom is observed on a Cisco 10008 when a PVC is shut on the remote side.

  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.

  Possible 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.

- CSCsg50129

  Symptoms: The PA-CC on a Cisco 7304 that has an NSE-100 may crash when you enter the **clear interface atm** command more than once for the interface of a 1-port ATM OC-3c/STM-1 multimode, enhanced port adapter (PA-A6-OC3MM) that is installed in the PA-CC.

  Conditions: This symptom is observed on a Cisco 7304 when the PA-A6-OC3MM is configured with 500 VRFs, when traffic is passing through all the VRFs, and when not all VCs have come up after the previous **clear interface atm** command was entered while you enter the **clear interface atm** command again.

  Workaround: After you have entered the **clear interface atm** command, wait for all the VCs to come up before you enter the **clear interface atm** command again.

  Alternate Workaround: Do not enter the **clear interface atm** command. Rather, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the PA-A6-OC3MM.

- CSCsg50211

  Symptoms: A Gigabit Ethernet connection between a Gigabit Ethernet port on a Cisco 10000 series and another platform may become inoperative unexpectedly.

Conditions: This symptom is observed randomly on a Cisco 10000 series that runs Cisco IOS Release 12.2SB and that has an interface that is configured for auto-negotiation on a full-height or half-height Gigabit Ethernet line card.

Possible Workarounds: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface. If this workaround does not clear the symptoms, enter the **hw-module reset** command for the affected line card. If neither of these workarounds clear the symptoms, reload the router.

- CSCsg53878

  Symptoms: An invalid traceback address may be displayed as part of a CPUHOG error message, as in the following example:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (6/6),process
  = Virtual Exec. -Traceback= BFC30E70
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 and that runs Cisco IOS Release 12.2(31)SB2 when commands are entered from the virtual terminal.

  Workaround: There is no workaround.

  Further Problem Description: When the symptom occurs, collect the output of the **show processes cpu sorted | ex 0.00** command. Then, for the processes that have a high CPU usage as shown in the output of the **show processes cpu sorted | ex 0.00** command, enter the **show stack** *#* command and substitute the PID of the output of the **show processes cpu sorted | ex 0.00** command for the *#* argument in the **show stack** *#* command. Then, submit all output to the Cisco Technical Assistance Center (TAC) for further assistance.

- CSCsg53975

  Symptoms: An OC-3 POS interface on a Cisco 10000 series that is connected to a Cisco 7200 series remains in the down/down state after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the OC-3 POS interface.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 6-port OC-3 POS line card.

  Workaround: Reload the Cisco 10000 series.

- CSCsg58029

  Symptoms: CPU usage may be at 100 percent for more than 10 minutes, and all line cards may reboot.

  Conditions: These symptoms are observed very rarely on a Cisco 10000 series when a large number of links on the router flap while traffic is being processed.

  Workaround: There is workaround.

- CSCsg58896

  Symptoms: A Cisco 10000 series that is configured for PPP may crash because of memory corruption.

  Conditions: This symptom is observed rarely on a Cisco 10000 series when a large number of serial links flaps during a long period of time, causing multilink bundles to go up and down.

  Workaround: There is no workaround.

- CSCsg66504

  Symptoms: Traffic is lost for 10 to 15 seconds after a PRE switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series immediately after the standby PRE enters the hot standby state.

Workaround: There is no workaround.

- CSCsg68753

  Symptoms: When you configure a traffic class to classify traffic on precedence 2 with a mark probability denominator of 1/5 and on precedence 6 with a mark probability denominator of 1/10, the output of the **show policy-map interface** command shows that the mark probability denominator for both precedence values is 1/10.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(28)SB2 and that is configured for WRED.

  Workaround: There is no workaround.

- CSCsg69691

  Symptoms: When a microcode reload is performed, the router may crash and generate the following error message:

  ```
  %ERR-1-GT64120 (PCI-1): Fatal error, PCI Master abort
  ```

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **microcode reload all** command.

  Workaround: There is no workaround.

- CSCsg70687

  Symptoms: A Port Adapter Carrier Card (CC-PA) on a Cisco 7304 may crash and generate the following error messages and tracebacks in the logs:

  ```
  %WSIPC-3-SYSCALL: System call for command 7 (port 2/0) : ipc_s end_rpc_blocked
  timed-out (Cause: timeout)
  -Traceback= 406F016C 40929BC4 40929D78 40929ECC

  %LC-3-RECOVERY: Line card (slot 2) recovery in progress
  -Traceback= 406F016C 408B9028 401F3680 408C017C 4087FAE4 408645E4 407F1E64

  %LC-3-SANTAANA: Santa Ana Asic: NSE instance 0, Serial Channel A (slot 2), Error
  Status 0x9 Detected padding

  %LC-3-SANTAANA: Santa Ana Asic: Line card instance 0, Serial Channel A (slot 2), Error
  Status 0x0

  %LC-3-IOTIMEOUT: RP CI-MUX FPGA read timeout (Slot 2, Serial Channel 0)
  ```

  Conditions: This symptom is observed once every 20 hours on a Cisco 7304 that has a CC-PA that runs firmware revision 1.40.

  Workaround: There is no workaround.

- CSCsg70929

  Symptoms: A 4-port OC-3 ATM line card (ESR-4OC3-ATM) may not restart properly on a Cisco 10000 series that has a PRE-2.

  Conditions: This symptom is observed only when the router boots while the MTU of the interface on the ESR-4OC3-ATM is different from the default MTU. The symptom does not occur if you change the default MTU of the interface after the router has booted.

  Workaround: Disable the **mtu** *bytes* interface configuration command and restart the ESR-4OC3-ATM.

- CSCsg71200

  Symptoms: During dynamic VLAN class modifications, the queueing policy inheritance fails. This situation causes traffic to be dropped.

Conditions: This symptom is observed on a Cisco 10000 series that has a hierarchical queueing policy for VLAN classes and a flat shape for the class default. When the VLAN class modifications occur that shift the matching subinterfaces to the class default, then back to the original VLAN class, and then to another VLAN class, the child queues are not created, causing traffic to drop.

Workaround: Remove and re-attach the hierarchical queueing policy.

- CSCsg71247

  Symptoms: Non-Priority Queuing (PQ) traffic in a class default in a QoS policy that includes the **match vlan** command is not dequeued during oversubscription of the PQ class.

  Conditions: This symptom is observed on a Cisco 10000 series only when there are multiple VLAN classes and when there are child queueing policies in the class default and the VLAN classes. The PQ policer takes the interface bandwidth as reference, causing policing to occur at the wrong rates and starvation of non-PQ child classes in the class default. The symptom does not occur for child classes in a VLAN class.

  Workaround: There is no workaround.

- CSCsg71400

  Symptoms: Traffic stops matching to a child policy.

  Conditions: This symptom is observed on a Cisco 10000 series when an interface has a hierarchical policy defined on a PVC, when you remove the child policy, and when you re-attach the child policy to the parent policy of the hierarchical policy. In this situation, the traffic no longer matches to the child policy.

  Workaround: Detach the hierarchical policy from the PVC, modify the child policy, and re-attach the hierarchical policy to the PVC.

- CSCsg71674

  Symptoms: T1 interfaces flap intermittently, causing input, CRC, frame, and abort errors to be generated.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(28)SB4.

  Workaround: There is no workaround.

- CSCsg72950

  Symptoms: Temperature alarms on a Cisco 10000 series PRE-3 assert at lower ambient temperatures than necessary.

  Conditions: This symptom may occur in an operating environment in which the ambient temperature is in the low 30s (degrees Celsius).

  Workaround: You can reprogram the temperature alarm thresholds. The recommended thresholds are:

  ```
  inlet minor: 41 C
  inlet major: 51 C
  inlet critical: 73 C
  outlet minor: 48 C
  outlet major: 58 C
  outlet critical: 85 C
  ```

- CSCsg73099

  Symptoms: When a client attempts to establish an IP session by using an IP assignment from the DHCP server of an Intelligent Service Gateway (ISG), the IP session may not be established.

Conditions: This symptom is observed on a Cisco router that functions as an ISG when the following conditions are present:

- The ISG is configured to initiate an IP session upon receipt of the first IP packet that does not have an IP session already, that is, the **initiator unclassified mac-address** or **initiator unclassified ip** command is enabled.
- The IP session client receives its IP assignment from the DHCP server of the ISG and this DHCP server functions as a stand-alone DHCP server (that is, the IP assignment occurs without the influence of an ISG user and/or service profile).

Workaround: In addition to or instead of the **initiator unclassified mac-address** or **initiator unclassified ip** command, enter the **initiator dhcp class-aware** command on the client-facing interface.

- CSCsg75132

  Symptoms: When the standby PRE comes up, the following error message is generated on the console of the active PRE:

  ```
  REDUNDANCY-3-IPC: cannot open standby port session in use
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has dual PRE engines that function in ISSU, RPR+, or SSO mode.

  Workaround: There is no workaround.

  Further Problem Description: The error message indicates that some of the Entity MIB information such as standby PRE version, standby flash information, and standby EEPROM data has failed to synchronize to the active PRE.

- CSCsg75968

  Symptoms: When you enter the **clear counters** command, a Cisco 7304 that has an NSE-150 may crash and generate a TLB exception.

  Conditions: This symptom is observed when the Cisco 7304 is configured with 500 VRFs on an PA-A6 port adapter, when 250 VRFs are active, and when you perform a soft OIR for the PA-A6 and then enter the **clear counters** command.

  Workaround: There is no workaround.

- CSCsg76626

  Symptoms: A counter may indicate double values and packets are punted from the PXF engine to the RP and then dropped.

  Conditions: This symptom is observed on a Cisco 7304 when you apply an ACL deny statement on the egress interface.

  Workaround: There is no workaround.

- CSCsg76845

  Symptoms: Traffic loss, framing errors, CRC errors, input errors, and abort errors may occur on DS1 interfaces after an APS switchover occurs because a line card has reset.

  Conditions: This symptom is observed on the Cisco 10000 series that has a 1-port channelized OC-12 line card that is configured for channelized T3 traffic and MR-APS. The framing, CRC, input, and abort errors may occur even when traffic is not flowing.

  Workaround: There is no workaround.

- CSCsg76929

  Symptoms: The PXF engine of a Cisco 10000 series may crash.

Conditions: This symptom is observed rarely on a Cisco 10000 series when MLP is configured and when member links flap frequently.

Workaround: There is no workaround.

- CSCsg77139

  Symptoms: After you have reloaded a router, VRF routes disappear.

  Conditions: This symptom is observed when you reload a router the processes a heavy traffic flow.

  Workaround: Enter the **clear ip route vrf** *vrf-name* command.

  Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface from which the VRF routes have disappeared.

- CSCsg77753

  Symptoms: A router that has an hierarchical policy on an ATM VC may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7206VXR that is configured with an NPE-G1 but may be platform-independent.

  Workaround: There is no workaround.

- CSCsg78469

  Symptoms: A Cisco 10000 series may generate a "SW_CORRUPTION" error message when a service of the ISG Layer 4 Redirect feature is removed from a session in a broadband aggregation (BBA) configuration.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) when a service of the ISG Layer 4 Redirect feature is removed via the configuration of a service policy.

  Workaround: There is no workaround.

- CSCsg79415

  Symptoms: After you have deleted a VLAN class from a bi-level policer policy in the ingress direction, class-default traffic is not aggregately policed by the parent policer that is defined for the default class.

  Conditions: This symptom is observed on a Cisco 10000 series that has a VLAN class with a child policer policy and a class default also with a child policy when you first attach the policy to an interface and then delete the VLAN class from the policy.

  Workaround: There is no workaround.

- CSCsg79638

  Symptoms: The PXF engine of a Cisco 10000 series may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series when MLP is configured and when member links flap frequently.

  Workaround: There is no workaround.

- CSCsg81545

  Symptoms: A router may crash when you attach a Frame Relay map class to a subinterface that has already a map class attached or when you remove the DLCI from a Frame Relay subinterface that still has a map class attached.

  Conditions: These symptoms are observed on a Cisco 7200 series.

Workaround: Remove the existing map class from the subinterface before you attach a new map class or remove the DLCI.

- CSCsg81678

  Symptoms: The aggregate values of the scheduler may be incorrectly updated for high-speed links. This situation may cause delay before policy maps take effect.

  Conditions: This symptom is observed on a Cisco 10000 series under rare circumstances with high-speed links such as 100 Mbps and Gigabit Ethernet links for which a parent shaper is configured.

  Workaround: There is no workaround.

- CSCsg81708

  Symptoms: Traffic drops occur when packets with a size of 64 bytes are being processed.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2.

  Workaround: There is no workaround.

- CSCsg82134

  Symptoms: When a line card failover occurs on a router that has redundant 4-port channelized T3 half-height line cards (ESR-HH-4CT3 line cards), the following error message and a traceback may be generated:

  ```
  %C10KHHCT3-4-LINECARDFAILOVER: LC Y-Cable cutover from subslot 4/1 due to freedm xmt
  partial packet fifo underrun error
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for failover protection through Y-cables when you initiate a line card failover by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on one of the ESR-HH-4CT3 line cards or by entering the **hw-module subslot** *slot-number/subslot-number* **reset** command for one of the ESR-HH-4CT3 line cards.

  Workaround: There is no workaround.

  Further Problem Description: Because of this caveat, the “xmt partial packet error” indication is currently not enabled to initiate an automatic line card failover on a router with redundant ESR-HH-4CT3 line cards. The error message is currently for information only.

  By nature, a line card failover may produce erroneous error indications on the line card. Further investigations have lead to the belief that the line card software is reading invalid error register information just after a failover occurs, producing an erroneous error message. Error indication registers should be cleared by the line card software following any line card failover before reading these registers again for valid error indications.

  When this caveats is resolved, the “xmt partial packet error” indication will be enabled as one of the mechanisms for an automatic line card failover.

- CSCsg85690

  Symptoms: When a policy map is unconfigured from a Fast EtherChannel (FEC) interface, a Cisco 7304 may crash and generate an “ALIGN-1-FATAL” error message without a traceback.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that is configured with 250 VRFs on the FEC interface. In addition, the Cisco 7304 is configured with 250 Frame Relay links and 250 dot1q VRFs. The symptom occurs while traffic is flowing through the FEC interface.

  Workaround: There is no workaround.

- CSCsg86230

  Symptoms: A router may crash when the execution of the **show policy-map** command is at the -More- prompt via one connection while the policy map is being modified or deleted via another connection.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may not be limited to this platform.

  Workaround: There is no workaround.

- CSCsg88356

  Symptoms: A ping between a CE router that is configured for ATM and another CE router that is configured for Ethernet may fail over an AToM tunnel when the **interworking ethernet** command is enabled on a connected PE router.

  Conditions: This symptom is observed on a Cisco 7200 series that functions as a PE router and may occur because of a timing issue. The symptom may not be platform-specific.

  Workaround: Do not enter the **interworking ethernet** command on the PE router. Rather, enter the **interworking ip** command.

- CSCsg88965

  Symptoms: When you first remove the **encapsulation frame-relay** command from a serial interface and then attempt to copy the startup configuration to the running configuration, a Cisco 7304 may crash and generate the following error message:

  ```
  Data Bus Error exception, CPU signal 10, PC = 0x40A24800.
  ```

  Conditions: This symptom is observed on a Cisco 7304 with an NSE-100 that has 250 Frame Relay, 250 Fast EtherChannel, and 250 dot1q VRFs while traffic is flowing through all these VRFs. QoS is configured on the core-facing interfaces of the Cisco 7304 and on the connected PE routers.

  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.

- CSCsg90571

  Symptoms: On a Cisco 7200 series with an NPE-G1, channelized T3 links may flap. On a Cisco 7200 series with an NPE-G2, the serial interface may become wedged without the interface output queue being full.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB2 and that is configured with a 2-port multichannel T3 port adapter (PA-MC-2T3+).

  Workaround: There is no workaround.

- 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.

- CSCsg97961

  Symptoms: A router may crash when you configure it with a high number of PPP over Ethernet over VLAN (PPPoEoVLAN) sessions that are spread over hundreds of VLAN subinterfaces.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 or PRE-3.

  Workaround: There is no workaround.

- 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.

- 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.

TCP/IP Host-Mode Services

- CSCsd54305

  Symptoms: BGP sessions that are established between two route reflectors (RRs) flap continuously because TCP times out for keepalives.

  Conditions: This symptom is observed on a Cisco router that functions as an RR in an MPLS VPN Interautonomous System (InterAS) scenario and occurs when the RR receives VPNv4 prefixes from a PE router. In this situation, the BGP session between the RR and the second RR flaps.

  Workaround: There is no workaround.

Wide-Area Networking

- 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.

- 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.

  Workaround: There is no workaround.

- CSCsd06110

  Symptoms: A router may exhaust its I/O memory.

  Conditions: This symptom is observed on a Cisco router when you clear 10,000 tunnels on which about 45,000 PPP sessions are established. The symptom occurs only under extreme stress situations.

  Workaround: Clear the tunnels and sessions in stages.

- CSCsd95533

  Symptoms: PPP packets are dropped and the Network Control Programs (NCPs) are not negotiated.

  Conditions: This symptom is observed when you force a DHCP renewal of a lease for a DHCP client on a virtual-template interface.

  Workaround: Delete and reconfigure the virtual-template interface.

- CSCse19768

  Symptoms: A Cisco router crashes when you enter the **compress predictor** command to configure Predictor software compression.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100. However, the symptom is platform-independent.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for Limpel Zif Stac (LZS) software compression.

- CSCse79790

  Symptoms: When PPPoE Relay is configured, only one session comes up successfully. All successive sessions fail. The initiation of more sessions brings down the existing sessions. If there are active sessions that are already existing (not necessarily PPPoE Relay sessions), the initiation of new PPPoE Relay sessions tears down all the sessions.

  Conditions: These symptoms are observed on a Cisco router that functions in a Virtual Private Dialup Network (VPDN). The symptom occurs only for PPPoE Relay sessions and not for normal sessions.

  Workaround: There is no workaround.

- CSCse86612

  Symptoms: A router that functions as an L2TP LNS for remote-end customer PCs that function as LACs crashes during normal operation.

  Conditions: This symptom is observed on a Cisco router that functions as a LNS in a Virtual Private Dialup Network (VPDN) and that runs Cisco IOS Release 12.2(28)SB2 or Release 12.4(8).

  Workaround: There is no workaround.

- CSCsg56725

  Symptoms: When you enter **terminate-from hostname** *host-name* 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 platform-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.

- CSCsg76884

  Symptoms: A PRE may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series that is configured for PPP and occurs when many serial links flap.

  Workaround: There is no workaround.

- CSCsg79798

  Symptoms: The number of SHDB handles for PPP, SIP, and a Cisco CallManager may increase considerably on the active RP. In this situation, when a switchover occurs, many interfaces may end up in the up/down state.

  Conditions: This symptom is observed on a Cisco router that has dual RPs in a situation in which 1000 serial interfaces flap every 12 seconds for 10 hours.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(31)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Note All caveats that are resolved in Cisco IOS Release 12.2(28)SB and Release 12.2(28)SB1 through Release 12.2(28)SB5 are also resolved in Release 12.2(31)SB2. To improve the usability of the release notes documentation, these resolved caveats are documented only in the sections for Release 12.2(28)SB1 through Release 12.2(28)SB5 and are not repeated in the "Resolved Caveats—Cisco IOS Release 12.2(31)SB2" section.

Basic System Services

- 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.

- CSCek43597

  Symptoms: A memory leak may occur on a router that is configured with 11,000 PPPoA and PPPoEoA sessions.

  Conditions: This symptom is observed when AAA HA is used to synchronize the authorization data from the standby RP to the active RP and when a RADIUS server is used.

  Workaround: Use local authentication. If this is not an option, there is no workaround.

- CSCek58968

  Symptoms: A RADIUS packet that is sent to a RADIUS server may contain a corrupted attribute.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA and that has the **radius-server vsa send authentication** command enabled.

  Workaround: Disable the **radius-server vsa send authentication** command.

- CSCin98160

  Symptoms: Sessions are not properly synchronized from the active RP to the standby RP after an HA switchover has occurred.

  Conditions: This symptom is observed on a Cisco router that has the **no aaa new-model** command enabled.

  Workaround: Configure local authentication and enter the **aaa new-model** command. If this is not an option, there is no workaround.

- CSCin99788

  Symptoms: An "%AAA-3-ACCT_LOW_MEM_TRASH" error message is generated when a low-memory condition occurs. When this situation occurs, a memory leak may occur in AAA data.

  Conditions: This symptom is observed when an interface flaps and causes a very large number of sessions to go down simultaneously, in turn generating a very large number of accounting stop records. In this situation, the I/O memory may be held for a long time when accounting records are send and when an AAA server is slow or unreachable.

  Workaround: There is no workaround.

- CSCsc73699

  Symptoms: A router that is configured for NetFlow v9 may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S4 or Release 12.2(27)SBC1 when the configuration is modified while the router actively exports flows. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- 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.

- CSCse30963

  Symptoms: The following error message and a traceback may be generated on a Cisco 7200 series:

  ```
  %SYS-3-MGDTIMER: Uninitialized timer, set_exptime, timer
  ```

  Conditions: This symptom is observed when you perform an OIR of a channelized port adapter, when you configure a channel group on channelized interfaces of a channelized port adapter, or when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on any interface.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur on a Cisco 7200 series that has an NPE-G2.

- CSCse36870

  Symptoms: An ISG crashes when a Change of Authorization (CoA) is issued upon account logon.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG while the password attribute is sent in the Account-Logon request.

  Workaround: There is no workaround.

- CSCse68964

  Symptoms: When a PTA session is created with a traffic classifier (TC) service, the Parent-Session-ID attribute of the accounting packets of the TC service on the ISG does not match the Acct-Session-Id of the parent session after 16^2 (that is, 000000EE) Acct-Session-Ids have been used.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG and that is configured with QinQ subinterfaces over which PTA sessions are established.

  Workaround: There is no workaround.

- CSCse78879

  Symptoms: The **radius-server attribute 31 remote-id** command does not function. The expected value of attribute 31 in a RADIUS Access-Request and Accounting-Request is only the value of the remote ID. However, attribute 31 may contain the host name, domain name, subinterface and description, in addition to the remote ID.

  Conditions: This symptom is observed on a Cisco router that functions as a NAS and that has the **radius-server attribute 31 remote-id** command enabled.

  Workaround: There is no workaround.

- CSCsf07847

  Symptoms: Specifically-crafted CDP packets may cause a router to allocate and hold extra memory. Exploitation of this behavior by sending multiple specifically-crafted CDP packets may cause memory allocation problems on the router.

  Conditions: This symptom is observed on a Cisco router when the header length of the CDP packet is shorter than the predefined header length (which is 4 bytes) and when the router runs a Cisco IOS software image that integrates the fix for CSCse85200.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse85200. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Disable CDP on interfaces where CDP is not required.

Further Problem Description: Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

- CSCsf11826

  Symptoms: When AAA and High Availability (HA) are configured, "SHDB handles" are not properly released when the **no aaa new-model** command is enabled on the router. For each session (that is, each PPPoA or PPPoE session) that comes up, a new "SHDB handle" is allocated. However, when the session goes down, the "AAA HA code" fails to release the handle. This situation causes the router to use up all valid handle names, and, after that has occurred, to either generate tracebacks for each session that is created or to crash.

  Conditions: This symptom is observed for each session that calls the "AAA HA code" to handle redundancy.

  Workaround: Enable the **aaa new-model** command and configure local authentication. If this is not an option, there is no workaround.

- CSCsf23387

  Symptoms: After a network event such as an HA switchover or an interface failure has occurred, information for all PPP sessions may be lost, causing the router to send RADIUS account-start messages for all PPP sessions and causing the RADIUS server to be severely stressed.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat relieves the impact on the RADIUS server by enabling you to limit the maximum number of outstanding active RADIUS accounting request via the AAA accounting throttling command that is introduced below. This command is introduced not only for HA configurations but for general AAA operations.

  radius-server throttle accounting *requests*

  The *requests* argument limits the number of pending accounting start/stop requests that are sent by the router to the RADIUS server. For example, if the *requests* argument has a value of 25, the number of pending accounting start/stop requests (without a RADIUS acknowledgement) is at maximum 25. If a new accounting request must be processed and the router has already sent 25 requests, the router will attempt to send the new accounting request after a "timeout". The request will be delayed with the value in seconds that is entered in the *timeout* argument of the following command:

  radius-server timeout *timeout*

  The router does not discard these accounting request if they time-out. Only if the router has actually attempted to send the accounting request to the RADIUS server and has retransmitted it three times, the accounting request may be discarded. Note that the retransmit default is three but can be modified through the **radius-server retry** *retries* command.

  If an accounting request is throttled, statistics are not impacted in any way. The statistics are updated only if an accounting request is sent to the RADIUS server, not when it is being throttled. You can check for the active accounting requests by entering the following command:

  show aaa servers

  Note that accounting has no impact on call setups. From the perspective of a client, it is a "send-and-forget" situation. The success or failure of accounting does not impact the actual session.

- CSCsf29098

  Symptoms: When you perform an OIR of a POS port adapter, a TLB Exception error may occur and the router may reset.

Conditions: This symptom is observed on a Cisco router that has a POS port adapter with an interface that functions as an MPLS link in an AToM configuration when the POS interface has the **mpls ip** command enabled.

Workaround: First disable the **mpls ip** command on the POS interface, then remove the AToM (Xconnect) configuration from the interface, and then perform an OIR of the POS port adapter.

- 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**.

- CSCsg48183

  Symptoms: A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

  Conditions: This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

  - You reload the router.
  - A switchover of the active RP occurs.
  - You enter the **redundancy force-switchover main-cpu** command.

  Workaround: There is no workaround.

- CSCsg77508

  Symptoms: The parent session Accounting STOP record is missing RADIUS attributes 42,43, 47 and 48.

  Conditions: This symptom is observed on a Cisco router that is configured to terminate a PPP over Ethernet over L2TP session when you apply a service policy to the session. The symptom occurs only when the session is configured with at least one traffic classification with per-flow accounting.

  When the PPP over Ethernet client is terminated, the RADIUS attributes 42, 43, 47 and 48 are missing from the parent session Accounting STOP record.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsc76550

  Symptoms: The RP may crash with a watchdog timeout error for the IP input process.

  Conditions: This symptom is observed on a Cisco router when you delete a subinterface that processes traffic.

  Workaround: Shut down the subinterface before you delete the subinterface.

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.

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.

- CSCek46082

  Symptoms: A router may crash when one of its multipoint interface enters the up state.

  Conditions: This symptom is observed on a Cisco 7200 series when the multipoint interfaces are configured for AAL5SNAP encapsulation via a virtual template and occurs only when the **debug atm event** command is enabled.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCed28542

  Symptoms: A router that is configured for PAT may generate the following error message and traceback while reporting slowness in the network:

  ```
  %SYS-2-INTSCHED: 'may_suspend' at level 3
  -Process= "IP NAT Ager", ipl= 3, pid= 118
  -Traceback= 80507F58 81310988 80CC14F8 80CD4F80 80CBAD30 80CBAD90 81321684 80CBB048
  80504118 805085E0
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(4)T and that has a high number (more than 2500) of NAT entries. The symptom is not release-specific.

  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.

- CSCek48132

  Symptoms: A router that is configured for HA may crash shortly after a switchover has occurred. When this situation occurs, "%TCP-2-INVALIDTCB" error messages are generated.

  Conditions: This symptom is observed on a Cisco router that has many interfaces (1600) that are connected to BGP neighbors when some peers are configured for NSR and others for NSF. The higher the number of interfaces on the router, the more likely it is that the symptom occurs.

  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.

- 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.

- 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.

- 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.

- CSCse67198

  Symptoms: A router may hang when you send a VRF ping to an outside NAT address of a directly-connected router.

  Conditions: This symptom is observed on a Cisco router that is configured for VRF NAT.

  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.

- 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.

- CSCsf06946

  Symptoms: After you have removed a loopback interface from the configuration on the primary RP while the same loopback interface is required as part of another configuration, for example, as an update source for a BGP neighbor, the standby RP does not reload successfully when you reset it.

  Conditions: This symptom is observed on a Cisco router and occurs only in an HA environment.

  Workaround: Remove all configurations that reference the loopback interface before you remove the loopback interface.

- CSCsg27697

  Symptoms: When an RP switchover occurs or when a standby RP resets, the standby RP may enter a loop in which it reboots continuously because of a BEM error.

  Conditions: This symptom is observed on a Cisco router that has the **router rip** and **address-family ipv4** commands enabled but that does not have a **network** command as part of the address-family configuration.

  Workaround: Disable the **router rip** command.

Miscellaneous

- CSCec54103

  Symptoms: When the ifStackStatus object of an inverse multiplexing over ATM (IMA) interface is polled with an “snmpwalk,” an endless loop may occur.

  Conditions: This symptom is observed on a Cisco router that is configured with an 8-port ATM Inverse MUX E1 or T1 port adapter (PA-A3-8E1IMA or PA-A3-8T1IMA).

  Workaround: There is no workaround.

- CSCef09119

  Symptoms: CPUHOG tracebacks may be generated when you bring up 30,000 PPPoE sessions and then remove an input policy map from a virtual template on a broadband PTA.

  Conditions: This symptom is observed on a Cisco router that functions as a broadband PTA and that is configured with 31,500 ATM subinterfaces, an input policy map, an output policy map with an CBWFQ policy, and 128,000 queues.

  Workaround: There is no workaround.

- CSCeg83467

  Symptoms: A router crashes when the encapsulation is changed from AAL5SNAP to AAL0.

  Conditions: This symptom is observed when the encapsulation is changed on a private virtual circuit (PVC).

  Workaround: Do not configure AAL0.

- 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.

- 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 PAM 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
```

- CSCej77184

  Symptoms: After an SSO switchover has occurred, the following error message may be generated:

  ```
  LSD-4-LABEL_RESOURCE: label range 16-524287 exhausted
  ```

  Conditions: This symptom is observed on a Cisco router that functions in an MPLS configuration under a heavy traffic load that causes bulk synchronization to take a relatively long time. The symptom occurs when there is label allocation between the “bulk-sync-done” state and the “Standby Hot” state.

  Workaround: There is no workaround.

- CSCej78971

  Symptoms: Unicast Reverse Path Forwarding (uRPF) does not function for a PPP subscriber when the **ip portbundle** command is enabled on the interface that carries the subscriber session. The following example shows a configuration in which the symptom occurs:

  ```
  interface Serial3/0
   ip vrf forwarding vrf1
   ip address x.x.x.x y.y.y.y
   ip verify unicast source reachable-via rx  <***** uRPF enabled
   encapsulation ppp
   service-policy type control ipsub-auth
  ```

  In the above-mentioned example, if the **ip portbundle** command is enabled in the “ipsub-auth” policy map, the source address of the interface that carries the subscriber traffic is changed to one of the IP addresses of the ISG, and the reverse-path check causes the traffic to be dropped.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG.

  Workaround: Disable the uRPF.

- CSCek34307

  Symptoms: After a service policy is removed from the virtual template, the same policy is not automatically removed from the virtual-access interface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB or Release 12.2(27)SBC.

  Workaround: Clear the virtual-access interface.

- 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.

- CSCek38382

  Symptoms: The standby PRE-2 crashes because of a debug exception, and the standby PRE-2 console shows the following error messages and traceback before the crash occurs:

  ```
  %SYS-2-ASSERTION_FAILED: Assertion failed: "(*parents_ptr)->coll_magic ==
  COLL_MAGIC_VAL"
  -Process= "Deferred Adj Background", ipl= 0, pid= 167
  -Traceback= 6050CA04 604AA1B4 60362364 60362510 603630A4 6035B67C 60360598 60FFAB30
  60FF54A0 60FF5578

  %Software-forced reload
  ```

  Conditions: This symptom is observed on a Cisco 10000 series after an ATM line card is reset.

  Workaround: There is no workaround.

- CSCek38430

  Symptoms: The standby PRE reloads unexpectedly.

  Conditions: This symptom is observed on a Cisco 10000 series when either of the following events occur:

  – Multiple users simultaneously add and delete service policies.

  – Multiple users periodically enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an ATM subinterface. For example, the users enter the commands with intervals of 5 to 10 seconds during a period of 2 or 3 minutes.

  Workaround: There is no workaround.

- CSCek39134

  Symptoms: During an HA configuration synchronization a router may generate the following error message:

  ```
  %UTIL-3-TREE: Data structure error--attempt to reference an uninitialized wavl tree
  ```

  Conditions: This symptom is observed rarely on a Cisco router when auto-discovery packets are received by the router during the initialization phase after an HA switchover has occurred or after the router has reloaded for the first time.

  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.

- CSCek40657

  Symptoms: A PTA router may crash when you download a configuration with a class map, policy map, and PVC range to a point-to-point interface.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PTA router.

  Workaround: There is no workaround.

- CSCek41883

  Symptoms: An RP may hang when PPPoX sessions are brought up.

  Conditions: This symptom is observed after an HA switchovers has occurred.

  Workaround: There is no workaround.

- CSCek42581

  Symptoms: A router crashes when you modify a police in the parent policy map.

  Conditions: This symptom is observed on a Cisco 10000 series when you first remove a class with a police that is configured under a parent policy map and then re-apply the same class or any other class with a police to the parent policy map.

  Workaround: Remove the parent policy map, reconfigure the parent policy map, and the re-attach the parent policy map.

- CSCek44373

  Symptoms: The standby RP may generate "%SYS-2-MALLOCFAIL: Memory allocation" failures and may or may not reset repeatedly.

  Conditions: These symptoms are typically observed in highly scaled configurations that consist, for example, of many BGP peers or PPPOA sessions. The symptoms occur during the SSO configuration-synchronization phase and bulk-synchronization phase when the standby RP comes online, during the configuration of the router, after a switchover, or when peer interfaces and/or routing neighbors flap. The symptom is more likely to occur on an RP that does not contain so much physical I/O memory and/or operates at a relatively slow CPU speed.

  Workaround: Scale down the configuration, or reduce the number of BGP peers or PPPOA sessions. If the peer neighbors or interfaces flap, determine the root cause, and correct the flapping problem.

- CSCek45299

  Symptoms: A policer configuration may not be removable from a policy map.

  Conditions: This symptom is observed on a Cisco 10000 series when policy-map classes have a priority level configured.

  Possible Workaround: Remove the policy map, reconfigure the policy map, and then re-attach the policy map.

- CSCek45570

  Symptoms: ISSU negotiation or a bulk synchronization fails, causing the standby RP to reload.

  Conditions: This symptom is observed on a Cisco router that is configured for HA when the ISSU client or DHCP client is not present on the peer.

  Workaround: There is no workaround.

- CSCek46135

  Symptoms: There is no interception when a time-based ACL rule is inactive.

  Conditions: This symptom is observed on a Cisco 10000 series that has the Lawful Intercept feature enabled.

  Workaround: There is no workaround.

- CSCek48136

  Symptoms: A router may crash when QoS policy changes occur for a large number of VCs.

  Conditions: This symptom is observed on a Cisco router when the QoS changes are made via an automated script.

Workaround: Modify the VCs manually, one by one.

- CSCek48457

  Symptoms: A Cisco 10000 series crashes when a scaled MFR configuration is loaded.

  Conditions: This symptom is observed when you load the scaled MFR configuration by using TFTP via the **copy tftp running-config** command.

  Workaround: There is no workaround.

- CSCek48575

  Symptoms: A router may crash when you first enter the **ip portbundle** command for PPPoE sessions in a port-bundle host key (PBHK) configuration and when you then change an ACL.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and that has a configuration such as the following:

```
ip portbundle
 length 3
 match access-list 103
 source Loopback2
```

  Workaround: There is no workaround.

- 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.

- CSCek52071

  Symptoms: A Cisco 7200 series may crash when you configure an IPv6 address on an interface.

  Conditions: This symptom is observed on a Cisco 7200 series that has the Lawful Intercept feature enabled.

  Workaround: There is no workaround.

- CSCek53084

  Symptoms: Attachment circuit (AC) and AToM clients show up as compatible while they have no peer on the other side.

  Conditions: This symptom is observed on a Cisco router that is configured for In-Service Software Upgrade (ISSU) when you downgrade from Cisco IOS Release 12.2(31)SB to Cisco IOS Release 12.2(28)SB or one of it's rebuilds.

  Workaround: There is no workaround.

- CSCek53559

  Symptoms: A router may reload after receiving a malformed UDP packet on port 67.

  Conditions: This symptom is observed on a Cisco router that functions as an DHCP server.

  Workaround: There is no workaround.

- CSCek54106

  Symptoms: When you convert a non-queueing policy map to a queueing policy map and attach it to interfaces that do not support queuing, the QoS policy is removed from the interfaces and existing sessions.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Convert the non-queueing policy map to a queueing policy map before you apply it to interfaces or bring up sessions.

- CSCek54768

  Symptoms: E1 interfaces may go down when a line card is reset or removed even when the line card has APS enabled and an APS cutover is triggered. The interfaces do come back up within a few seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has a pair of 4-port channelized OC-3 line cards that are configured for SR-APS. The line cards are configured with E1 interfaces under either SONET or SDH.

  Workaround: Enter the **force** command in APS group configuration mode on both the router on which the line card is reset or removed and on the router at the far end to ensure that the line card that is reset or removed does not receive or transmit the active traffic.

  Note that the chances of the symptom occurring may be reduced when the line card that is reset or removed is not the active line card.

  Further Problem Description: This symptom occurs only when a line card is reset or removed, not when an APS switchover is triggered by a fiber cable that is removed.

  The symptom occurs because of a change in the E1 clock source that may occur when the line card is reset or removed and that causes alarms to be received. The symptom is more likely to occur when the line card has a large configuration and when the E1 interfaces are set to “clock source line.”

- CSCek55284

  Symptoms: When you upgrade the Cisco IOS software image from Cisco IOS Release 12.2(28)SB3 to Cisco IOS Release 12.2(31)SB by entering the **issu loadversion** command, the standby RP remains in the RPR mode, preventing the upgrade from proceeding.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCek55726

  Symptoms: When you reload a Cisco 10000 series that has dual PREs, the standby PRE may crash during the boot process and may or may not generate a traceback.

  Conditions: This symptom is observed on a Cisco 10000 series that has a large configuration when the standby PRE and primary PRE are out of synchronization while you enter the **reload** command.

  Workaround: There is no workaround.

- CSCek55946

  Symptoms: A Cisco 7304 series NPE-G100 may hang.

  Conditions: This symptom is observed when a cache exception occurs, which is a very rare event.

  Workaround: There is no workaround.

- CSCek56055

  Symptoms: When an IP session that was initiated by DHCP goes down, the session cannot be reconnected until the lease expires for the client.

Conditions: This symptom is observed on a Cisco Intelligent Service Gateway (ISG) when an idle-timeout occurs, when the ISG reloads, or when a client logs off without releasing the IP address.

Workaround: Manually clear the DHCP binding or just wait until the lease expires.

- CSCek56415

  Symptoms: The Hierarchal Queuing Framework (HQF) is not removed after you have removed a service policy.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 and that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek56991

  Symptoms: A Cisco 7200 series may send a corrupted packet via a 2-port T3 serial, enhanced port adapter (PA-2T3+). The rate of corrupted packets is very low.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB, Release 12.4T, or Release 12.4(4)XD3 and occurs when the router functions under high stress conditions such as a high CPU load and an oversubscribed interface of the PA-2T3+.

  Workaround: Avoid a high CPU load and oversubscription of the interface of the PA-2T3+.

- CSCek57646

  Symptoms: On a Cisco 10000 series, tracebacks and an error message that is related to the link index may be generated, and MLPoATM links continue to flap. The error message is similar to the following:

  ```
  %GENERAL-3-EREVENT: ttcm_add_mlp_member: 1926 No free link index available in
  Virtual-Access15
  ```

  Conditions: This symptom is observed when a member link of an MLPoATM bundle is modified.

  Workaround: There is no workaround.

- 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.

- CSCek59190

  Symptoms: When you reload a Cisco 10000 series, tracebacks are generated when the router comes back up.

  Conditions: This symptom is observed when the router has dual PREs that function in SSO mode and a 4-port channelized STM-1/OC-3 line card that is configured for Multi-Router APS (MR-APS).

  Workaround: There is no workaround.

- CSCek59985

  Symptoms: A traceback may be generated during the “fetch_interface_drop_stats_clrable” process on a Cisco 10000 series.

  Conditions: This symptom is observed when you enter the **clear pxf interface** command for an inactive multilink interface.

  Workaround: Enter the **clear pxf interface** command only when the multilink interface is active.

- 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.

  Workaround: There is no workaround.

- CSCek62271

  Symptoms: The output of the **show ip subscriber** command does not show the sessions.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) and occurs for IP session with a static IP address that are connected via Layer 2.

  Workaround: Do not enter the **show ip subscriber** command. Rather, enter the **show ip subscriber mac** command.

- CSCek63748

  Symptoms: When the **debug ip subscriber event** or **debug ip subscriber all** command is enabled and when a client attempts to establish an IP session, the Cisco Intelligent Service Gateway (ISG) may crash.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG under the following conditions:

  – The ISG is configured to initiate an IP session upon receipt of the first IP packet that does not have an IP session already, that is, the **initiator unclassified mac-address** or **initiator unclassified ip** command is enabled.

  – There is a DHCP relay between ISG and the client.

  – The IP session client receives its IP assignment from the DHCP server of the ISG and this DHCP server functions as a stand-alone DHCP server (that is, the IP assignment occurs without the influence of an ISG user and/or service profile).

  Workaround: Disable the **debug ip subscriber event** or **debug ip subscriber all** command.

- CSCin99827

  Symptoms: An RP may crash when PPP sessions with service policies are removed. If the router is configured with a standby RP, a switchover may occur. Then, if more PPP sessions are removed, the newly active RP may crash. These symptoms may also occur when you enter the **no policy-map** command for a policy map that is attached as a service policy to many PPP sessions.

  Conditions: These symptoms are more likely to occur with a large number of sessions (tens of thousands or more) and when the session are removed at a high rate (hundreds per second).

  Workaround: There is no workaround.

  Further Problem Description: The symptoms are caused by a race condition when internal processes, such as statistics updates, may attempt to modify data that are related to service policies that are being removed.

- CSCir00590

  Symptoms: VCs may enter an inactive state, preventing sessions from coming up over the VCs.

  Conditions: This symptom is observed on a Cisco 10000 series when you perform an OIR of the line card on which the VC are configured after at least one HA switchover has occurred.

  Workaround: Reload the router.

- CSCir00613

  Symptoms: An ATM line card may reset after when an SSO switchover occurs.

  Conditions: This symptom is observed on a Cisco 10000 series when an SSO switchover occurs while there are 32,000 active PPP over ATM (PPPoA) sessions.

  Workaround: There is no workaround.

- CSCsa92748

  Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

  ```
  Last reset from watchdog reset
  ```

  Conditions: This symptom is observed only on Cisco 7200 and Cisco 7301 series routers that are configured with an NPE-G1 Network Processing Engine.

  Workaround: There is no workaround.

- CSCsb01284

  Symptoms: Incorrect police percent conversions occur in the second and third level of a policy.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB but may also occur on other platforms and in other releases.

  Workaround: There is no workaround.

- CSCsb71154

  Symptoms: When a VC that is configured under a VP goes down, PPPoE sessions can still be established over the VC.

  Conditions: This symptom is observed on a Cisco 10000 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface or after you have reloaded the router.

  Workaround: There is no workaround.

- CSCsc14052

  Symptoms: A Cisco 10000 series may crash and generate one of the following error messages:

  ```
  PXF DMA Error - Command Packet Handle Out of Range
  ```

  or:

  ```
  PXF DMA - Small Free Packet Handle Access Out of Range
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that processes L2TP traffic and that has a heavy CPU load.

  Workaround: There is no workaround.

- CSCsc44272

  Symptoms: When a Cisco 7304 has a configuration with more than 65,536 ACEs, some of the counters do not increment correctly.

  Conditions: This symptom is observed when the entire ACE configuration is greater than 65,336 ACEs.

  Workaround: There is no workaround. Do not configure more than 65,536 ACEs.

- CSCsd35159

  Symptoms: Alignment errors may occur when you detach a shaping service policy from a QinQ subinterface.

Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: There is no workaround.

- CSCsd45936

  Symptoms: When a two-level hierarchical policy map in which the parent level has only a class default is already attached to an interface and when you configure a policer for both the parent and child levels, either of the following symptoms may occur:

  – When the child policy map is removed from the class default of the parent policy map, the traffic policing rate does not properly reflect the parent policer rate.

  – When the child policy map is attached to the class default of parent policy map, the traffic policing rate does not properly reflect the child policer rate.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

  Workaround: After the child policy is removed from or attached to the parent policy map, detach the policy map from the interface and re-attach it to the interface.

- 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.

- CSCsd60687

  Symptoms: When an RPR switchover occurs, a router may generate CPUGHOG messages or may crash because of a watchdog timeout.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB or Release 12.2SR.

  Workaround: There is no workaround.

- CSCsd65283

  Symptoms: A router may crash when you enter the **connect** command.

  Conditions: This symptom is observed when one of the VCs that is being configured in the **connect** command is down.

  Workaround: Ensure that both VCs are up when you enter the **connect** command.

- CSCsd65497

  Symptoms: When a GRE IP tunnel is configured between a CE router and a PE router and is added to the VRF table, the IP address of the tunnel on the PE router is not reachable from the CE router although the IP address of the tunnel on the CE router is reachable from the PE router.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that functions as a PE router.

  Workaround: There is no workaround.

- CSCsd82991

  Symptoms: A router crashes when you enter the **ip rtp header compression** command on a serial interface that has a service policy attached.

  Conditions: This symptom is observed on a Cisco router and occurs only when a routing protocol, such as EIGRP, has been configured.

Workaround: There is no workaround.

- CSCsd85852

  Symptoms: When a PVC is shut down on the remote side, the PVC subinterface on a router transitions from the down state to the up state within one second, but then remains in the down state after the down retry timers expire.

  Conditions: This symptom is observed on a Cisco router that is configured for Operation, Administration, and Maintenance (OAM) and Dynamic Bandwidth Selection (DBS).

  Workaround: There is no workaround.

- CSCsd85990

  Symptoms: Multilink class 0 is used for all outgoing packets, regardless of which encapsulation sequence is configured for a queue.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multiclass MLP (MC-MLP) with one member link and occurs after the PXF engine is reloaded.

  Workaround: There is no workaround.

- CSCsd92405

  Symptoms: A router crashes when receiving multiple malformed TLS and/or SSL3 finished messages. A valid username and password are not required for the crash to occur.

  Conditions: This symptom is observed when a router has HTTP secure server enabled and has an open, unprotected HTTP port.

  Workaround: There is no workaround. Minimize the chances of the symptom occurring by permitting only legitimate hosts to access HTTP on the router.

- CSCsd95631

  Symptoms: When you enter the **show atm vp** command for ATM VPs, a negative number of data VCs is displayed, which does not represent the actual number of VCs per VP.

  Conditions: This symptom is observed on a Cisco 10008 that runs Cisco IOS Release 12.3(7)XI. However, the symptom is not platform-specific, nor release-specific.

  Workaround: There is no workaround.

- 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.

- CSCse01989

  Symptoms: When you apply a channel group to a Gigabit Ethernet interface that has the **negotiation auto** command enabled, the **negotiation auto** command is unexpectedly enabled on the port-channel interface. This situation causes a synchronization failure on the standby RP, in turn, causing the standby RP to reset.

Conditions: This symptom is observed on a Cisco router that has redundant RPs in an HA configuration.

Workaround: Manually remove the auto-negotiation configuration from the port-channel interface by entering the **no negotiation auto** command.

- CSCse08652

  Symptoms: When you configure MVPN over an MLPoATM interface, multiple PXF crashes may occur.

  Conditions: This symptom is observed on a Cisco 10000 series when you first enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the MLPoATM interface and then enter the **show pxf cpu queue** *interface* command on the MLPoATM interface. After these commands, the PXF crashes start. This situation may cause the boot flash to be fully consumed.

  Workaround: There is no workaround.

- CSCse11078

  Symptoms: When you enter the **aps force** or **aps manual** command on a Cisco 10000 series router that has interfaces that are configured for Multi-Router APS (MR-APS), the standby PRE may not properly reflect the MR-APS state of the interfaces.

  Conditions: This symptom is observed in a configuration with two Cisco 10000 series routers that are configured with dual PREs that function in SSO mode.

  Workaround: There is no workaround.

- CSCse13674

  Symptoms: A session does not receive an IP address from the VRF pool.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when a VRF is configured in an automatic activation service with Transparent Auto-Logon (TAL).

  Workaround: Do not configure a VRF in an automatic activation service.

- CSCse15417

  Symptoms: When about 40,000 sessions are created, a Cisco router that functions as an Intelligent Service Gateway (ISG) may reload.

  Conditions: This symptom is observed only when auto services are used to bring up the sessions and when a low-memory condition occurs.

  Workaround: Do not use auto services to bring up the sessions.

- 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.

- CSCse23190

  Symptoms: After a forced SSO switchover has occurred, the next hop in the routing table becomes 0.0.0.0.

Conditions: This symptom is observed on a Cisco router that is configured with PPPoEoA sessions.

Workaround: There is no workaround.

- CSCse23232

  Symptoms: When a virtual template or user profile contains a service policy with class maps, the router may send not one but a number of RADIUS accounting-request packets for each PPPoE or PPPoEeoA session. The number of RADIUS accounting-request packets equals the number of class maps in the service policy. Each accounting-request packet has its own unique "acct- session-id."

  Conditions: This symptom is observed on a Cisco router that is configured with a QoS policy.

  Workaround: There is no workaround.

- 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.

  Workaround: There is no workaround.

- CSCse25431

  Symptoms: A LAC may generate an "HQF_WARN_HQF_OVERSUBSCRIPTION_DETECTED" error message when it is oversubscribed with a high number of sessions. The LAC may crash when it is severely oversubscribed.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC when you scale PPPoEoQinQ sessions with QoS configured and when you oversubscribe to a very high rate. The oversubscription is configured on a subinterface via an MQC policy that is enabled through the **shape average percent** *percent* command.

  Workaround: Do not configure the oversubscription factor above the supported factor of 50:1.

- CSCse28714

  Symptoms: Removing and re-attaching a policy to a subinterface may fail because of cleanup issues.

  Conditions: This symptom is observed on a Cisco 10000 series when a hierarchical policy with PBR in the parent policy class-default class is applied to the session that is established on the subinterface.

  Workaround: There is no workaround.

- CSCse28795

  Symptoms: When a service policy is configured on an ATM main interface that has a PVC on a subinterface (the PVC does not have its own policy), an "%C10K_QOS_GENERAL-e-EREVENT" error message and traceback are generated when the PVC is recreated.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router in an MPLS network that has the following topology:

  ```
  CE1 -- PE1 -- P -- PE2 -- CE2
  ```

  Workaround: There is no workaround. However, the error message and traceback have no functional impact.

- CSCse31706

  Symptoms: A Lawful Intercept configuration improperly shows as part of an interface configuration.

  Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: There is no workaround.

- CSCse32421

  Symptoms: A PXF buffer leak may occur when a Multilink PPP interface is shut down on the other side of a back-to-back configuration.

  Conditions: This symptom is observed on a Cisco 10000 series and is caused by packets that become stuck in the multilink bundle queue when the connected router crashes or is reloaded, or when a remote interface is shut down. When all links are removed from the multilink bundle, the packets are still queued up in the multilink bundle. Because there is no serial link to dequeue the packets, the packets remain in the queue.

  Workaround: There is no workaround.

- CSCse35684

  Symptoms: OSPF sessions do not come up at the Layer-3 level.

  Conditions: This symptom is observed when you perform an OIR of an ATM line card.

  Workaround: Reload the affected line card.

- CSCse36785

  Symptoms: Packets that are switched via CEF to a service network with DHCP-based IP subscribers may be dropped at an ISG.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when both of the following conditions occur:

  – A subscriber sets the DHCP broadcast bit in a DHCP request to zero, as a Microsoft DHCP host typically does.

  – The subscriber connection occurs via Dynamic VPN selection, that is, the subscriber connects to the ISG via a global interface but the IP address is assigned by VPN services that are selected by the subscriber.

  Workaround: If the DHCP client is a router that runs a Cisco IOS software image, enter the **ip dhcp-client broadcast** command on router. If the DHCP client runs Microsoft software, there is no workaround.

- CSCse36890

  Symptoms: Multicast packets that traverse GRE tunnels over a Gigabit EtherChannel (GEC) bundle interface may be dropped because of multicast RPF failures.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Do not use a GEC bundle. Rather, configure the GRE tunnels on regular GE interfaces.

- 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.

- CSCse41596

  Symptoms: A Cisco router does not update the IP address of a RADIUS proxy session, and the RADIUS proxy session is terminated after the IP address timer expires.

Conditions: This symptom is observed only when the router functions both as an Intelligent Service Gateway (ISG) and as a DHCP server.

Workaround: There is no workaround.

- CSCse42494

  Symptoms: A router crashes when it has more than 65,536 L2TP sessions in a multiple-hop configuration. At a multiple-hop router, an L2TP session is created inbound and outbound for each user session. This means that the number 65,536 is exceeded when more than 32,768 sessions are traversing the tunnel.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Configure less than 32,768 user sessions (half of 65,536).

- CSCse43394

  Symptoms: When traffic is sent through 250 LFI over Frame Relay interfaces, the other side does not receive any traffic. Also, no packets are dequeued on the priority queue (PQ).

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse43461

  Symptoms: The VC state remains down after and interface flap occurs on an MFR interface that has Frame Relay end-to-end keepalive (EEK) configured. The EEK state remains down although the MFR interface is up.

  Conditions: This symptom is observed on a Cisco 10000 series when the MFR interface has the following Frame Relay class map configured:

  ```
  map-class frame-relay eek
   frame-relay end-to-end keepalive mode bidirectional
  ```

  and also

  ```
  frame-relay multilink bandwidth-class c
  ```

  The symptom occurs when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the MFR interface.

  Workaround: To prevent the symptom form occurring, enter the **frame-relay end-to-end keepalive error-threshold send 3** command in the Frame Relay class map. The default value is 2.

  When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface at the other side of the MFR interface.

- CSCse44067

  Symptoms: A Cisco 7304 that has an ATM-IMA port adapter may crash.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when you configure an ATM-IMA subinterface with an IP address.

  Workaround: There is no workaround.

- CSCse45054

  Symptoms: When there is bidirectional traffic over PPPoE sessions over an Auto VC and you perform an OIR of the line card that processes this traffic, a few VCs are not cleared from the line card when the idle timeout is reached. This situation prevents sessions from coming up on the affected VCs.

  Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: Perform a second OIR of the line card.

- CSCse47905

  Symptoms: When an IP session that was initiated by DHCP goes down, the session cannot be reconnected until the lease expires for the client.

  Conditions: This symptom is observed on a Cisco Intelligent Service Gateway (ISG) when an idle-timeout occurs, when the ISG reloads, or when a client logs off without releasing the IP address.

  Workaround: Manually clear the DHCP binding or just wait until the lease expires.

- CSCse48657

  Symptoms: The active RP unexpectedly resets the standby RP.

  Conditions: This symptom is observed when you configure an Embedded Event Manager (EEM) policy and when the policy file is only available on the active RP and not on the standby RP.

  Workaround: Before you configure the EEM policy, copy the policy file to the standby RP at the same location as the policy file is located on the active RP.

- CSCse49912

  Symptoms: When end-to-end Frame Relay fragmentation (FRF.12) is configured for a Multilink Frame Relay (MFR) (FRF.16.1) bundle, the Frame Relay configuration may become lost and packets with a size that is smaller than the fragmentation size cannot pass.

  Conditions: This symptom is observed on a Cisco 10000 series when end-to-end Frame Relay fragmentation is configured on the main interface, that is, not via a Frame Relay map class and occurs when the interface flaps.

  The following configuration provides an example of an end-to-end Frame Relay configuration that is applied directly to the main interface:

```
interface MFR4
 description c10k FRF.16 test
 ip address 10.0.0.1 255.255.255.252
 load-interval 30
 no arp frame-relay
 frame-relay multilink bandwidth-class c 3
 frame-relay fragment 80 end-to-end
 frame-relay interface-dlci 17
```

  Workaround: Reconfigure end-to-end Frame Relay fragmentation by entering the following sequence of commands:

  no frame-relay fragment *fragment-size* **end-to-end**

  frame-relay fragment *fragment-size* **end-to-end**

  Alternate Workaround: Apply end-to-end Frame Relay fragmentation via a Frame Relay map class.

- CSCse50992

  Symptoms: Traffic that matches a prepaid service that consists of a traffic class and a volume monitor is matched with a default traffic class instead, causing the traffic to pass unbilled.

  Conditions: This symptom is observed on a Cisco 10000 series when traffic is sent continuously after reauthorization has occurred.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the router to restore proper functionality.

- CSCse51043

  Symptoms: A router may generate tracebacks and may crash when you bring up a Gigabit Ethernet (GE) interface.

  Conditions: This symptom is observed when you first shut down the GE interface and then bring it up with a large number of IPoQinQ VLANs.

  Workaround: There is no workaround.

- CSCse53212

  Symptoms: When a switchover occurs, a traceback may be generated on a router that is configured with a large number of PPPoE sessions, and the router may crash.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS and LDP and occurs only when the number of PPPoE sessions reaches beyond 30,000. However, the traceback (without a crash) may occur even for 500 PPPoE sessions.

  Workaround: There is no workaround.

- CSCse53669

  Symptoms: You may not be able to change the Dynamic Bandwidth Sharing (DBS) parameters for some create on-demand PVCs, and the DBS parameters for some PVCs may change when they are not supposed to change.

  Conditions: This symptom is observed on a Cisco 10000 series you enter the **dbs enable** or **no dbs enable** command for a range of ATM PVCs after VCs have been brought up. The symptom does not occur for VCs that are brought up for the first time after the DBS configuration has changed.

  Workaround: This workaround applies only to a VC that does not process traffic for a while. The purpose of this workaround is to bring down a VC connection in order to change the DBS parameters.

  Enter the **dbs enable** or **no dbs enable** command, as needed. Then, enter the **pvc-in-range** *vpi vci* command for a particular VC and enter the **idle-timeout** *seconds* command with a non-zero value for the *seconds* argument to enable the session to expire when there is no traffic on the VC. Check the output of the **show atm vc** *vcd* command until the VC goes down or disappears. Remove the **idle-timeout** *seconds* command or restore this command to its former value.

- CSCse57312

  Symptoms: The MQC output policer does not add the L2 header as part of its calculation.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only for multicast traffic on Ethernet and ATM interfaces.

  Workaround: There is no workaround.

- CSCse57808

  Symptoms: An eBGP session on the MFR interface continues to flap if one of the links in the MFR bundle is down while the bundle is up.

  Conditions: This symptom is observed only when Frame Relay EEK is enabled on the MFR interface. The symptom does not occur when Frame Relay EEK is not configured on the MFR interface.

  Workaround: Ensure that all links in the bundle are up. If you must bring down one link, do not shut the link down, but remove it from the bundle.

- CSCse59096

  Symptoms: Traffic with large packets cannot be fragmented through an MFR bundle that is configured for end-to-end Frame Relay fragmentation (FRF.12) after you have removed a service policy from the MFR interface.

  Conditions: This symptom is observed on a Cisco 10000 series when an output policy map is first added and then removed. Packets with sizes that are smaller than the fragmentation size can still be transmitted.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MFR interface.

- CSCse60008

  Symptoms: A router crashes when a packet with a PPP header that includes a bad IP version is sent over an MLP link.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SSO.

  Workaround: There is no workaround.

- CSCse61320

  Symptoms: A PRE-2 may crash when remove the last **match vlan** class-map configuration command from the last class map in a policy that is attached to an interface.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Remove the class map by entering the **no class-map** *class-map-name* command.

- CSCse65884

  Symptoms: The **atm pvp** *vpi* **l2transport** command may disappear from the configuration.

  Conditions: This symptom is observed after you have reloaded the router.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reconfigure the command.

- CSCse65966

  Symptoms: Low traffic throughput occurs when you detach a VLAN policy from an interface.

  Conditions: This symptom is observed on a Cisco 10000 series when the VLAN policy that is being detached has a child policy under a default class for non-VLAN group members.

  Workaround: There is no workaround.

- CSCse66782

  Symptoms: When RSA keys are generated at first, both the active and the standby RP receive the RSA key. However, after an HA RP switchover has occurred, the new standby RP no longer has the RSA key. When you reset the standby RP, the RSA key is not synchronized to the standby RP either. After another HA switchover has occurred, both the active and the standby RP have lost the RSA key, which then must be regenerated.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCse68044

  Symptoms: The user name that is sent to accounting and authorization servers is blank, causing prepaid services and billing to fail.

Conditions: This symptom is observed on a Cisco router when ISG is configured to perform Transparent Auto-Logon (TAL) for PPP sessions and when there is no authentication configured on the virtual template that is used for the PPP sessions.

Workaround: There is no workaround.

- CSCse68788

  Symptoms: The console hangs and there is no response to any CLI commands.

  Conditions: This symptom is observed on a Cisco 10000 series that has a large broadband configuration with 40,000 PTS sessions, each one with a QoS service policy. The symptom occurs when active sessions are disconnected at a high rate (200 disconnections per second).

  Workaround: Slow down the session disconnection rate.

  Further Problem Description: The symptom does not occur when sessions without a QoS service policy are disconnected.

- CSCse70667

  Symptoms: A router crashes during an attempt to access the interface policy-map statistics.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with invalid policy maps that have VLAN classes with invalid filter types.

  Workaround: There is no workaround.

- CSCse72235

  Symptoms: A Cisco 7200 series may crash because of an address error with corrupted program counter at “pc=0xAFACEFAD.” This precise value is repeated in the traceback and in the “EPC,” “BadVaddr,” and “ra” registers. The crash may be preceded by a “%SYS-2-GETBUF: Bad getbuffer” error message.

  Conditions: This symptom is observed on a Cisco 7200 VXR router that has an NPE-G1 and that runs Cisco IOS Release 12.2(28)SB2. The router is configured as a LAC with PPPoA and MPLS fragmentation for packets that travel from a PPPoA interface through an L2TP tunnel to an interface that is configured for MPLS.

  Workaround: Disable MPLS.

  Alternate Workaround: Disable fragmentation.

- CSCse75238

  Symptoms: A router may crash when the service-policy information of a session is displayed.

  Conditions: This symptom is observed when tens of thousands of sessions are established on a PTA router that has a service-policy instance for each session via a policy map on a virtual template.

  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.

- CSCse77804

  Symptoms: When you downgrade the Cisco IOS software image from Cisco IOS Release 12.2(33)SB to Release 12.2(28)SB, the download fails.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PREs (PRE A and PRE B) and that is configured for ISSU when the following sequence of events occurs:

  1. The active PRE is switched over from PRE A to PRE B.
  2. The **loadversion** command is issued from PRE B, which is the active PRE.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when PRE A is the active PRE and when the **loadversion** command is issued from PRE A.

- 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.

- CSCse78987

  Symptoms: The PXF engine may crash because of an invalid sequence of DMA commands.

  Conditions: This symptom is observed on a Cisco 10000 series when a multicast packet is replicated on an interface on which an Intelligent Service Gateway (ISG) session is established.

  Workaround: There is no workaround.

- CSCse79166

  Symptoms: Policing may not function on a Cisco 10000 series.

  Conditions: This symptom is observed when a parent policy map has a **police** command enabled and when a child policy map has a set action.

  Workaround: Do not configure a simple set action in the child policy map. Rather, configure a **police** command with a set action in the child policy map.

- 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.

- CSCse81528

  Symptoms: A newly active 4-port channelized T3 half-height line card (ESR-HH-4CT3) in subslot 0 may reload when a previously active ESR-HH-4CT3 is unplugged from subslot 1.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only in a configuration with a redundant Y-cable in which subslot 1 is the active ESR-HH-4CT3.

  Workaround: There is no workaround.

- CSCse83989

  Symptoms: When you reset or insert a line card while traffic is flowing, the line card may reset continuously.

Conditions: This symptom is observed on a Cisco 10000 series that has a 1-port channelized OC-12 line card and a 4-port channelized OC-3 line card.

Workaround: Stop the traffic that is destined for the line card before you reset or insert the line card.

- 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.

- CSCse87221

  Symptoms: Tracebacks are generated during an SSO switchover.

  Conditions: This symptom is observed on a Cisco router when you enter the **redundancy force-failover main-cpu** command.

  Workaround: There is no workaround.

- CSCse87499

  Symptoms: A platform that is configured for Cisco IOS Redundancy Facility (RF) may reload unexpectedly.

  Conditions: This symptom is observed when an RF client fails while the standby RP attempts to transition to the hot standby state.

  WorkAround: There is no workaround.

- CSCse88338

  Symptoms: A router crashes when you first enter the **clear subscriber session all** command and then enter the **show ip subscriber dangling** *number-of-seconds* command.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG while processing traffic.

  Workaround: Do not enter the **show ip subscriber dangling** *number-of-seconds* command or the **clear ip subscriber dangling** *number-of-seconds* command.

- 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) switchover 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.

- 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.

- CSCse91989

  Symptoms: ISSU Client 2063 (ISSU DHCPC) that is only present in Cisco IOS Release 12.2(31)SB2 shows up as compatible in a release that does not support the client.

  Conditions: This symptom is observed when you downgrade from Cisco IOS Release 12.2(31)SB2 to a release that does not yet support the client.

  Workaround: There is no workaround.

- CSCse93327

  Symptoms: A Cisco 10000 series may crash when you modify a class map.

  Conditions: This symptom is observed when the QoS configuration is scaled to a high number of VLAN classes and when you attempt to delete a child class with a WRED configuration from a policy that is attached to a VLAN group class.

  Workaround: First, remove the WRED configuration from the class. Then, delete the class.

  Alternate Workaround: Detach the service policy from the interface, delete the class, and then re-attach the service policy to the interface.

- CSCse93747

  Symptoms: When you configure QoS on an ATM PVC under a point-to-point subinterface, the router may not accept and save an output service policy when an input service policy is already present on the interface.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE-2 or PRE-3.

  Workaround: First configure the output service policy and then configure the input service policy.

- CSCse94304

  Symptoms: A PRE crashes, and CPUHOG error messages are generated.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in an MR-APS configuration with another Cisco 10000 series and that has MLP configured.

  Workaround: Disable MLP.

- CSCse94879

  Symptoms: When you upgrade from Cisco IOS Release 12.2(27)SBB5 to Release 12.2(27)SBB6 by using ISSU, a traffic interruption of about 30 seconds may occur on an OC-12 POS line card.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PRE-2 processors and one or more OC-12 POS line cards. The symptom could also occur with other releases.

  Workaround: There is no workaround.

  Further Problem Description: The upgrade should reload the OC-12 POS line card but not reset the line card. Instead, an internal error occurs on the line card, causing the line card to crash. However, the line card automatically reboots and successfully recovers, and traffic resumes after about 30 seconds of interruption.

- CSCse95010

  Symptoms: For a bi-level policy that has the **shape percent** command enabled for the parent match-vlan class and that has the **bandwidth percent** command enabled for the child class, the bandwidth is not proper computed at the child class when the *percent* argument of the **shape percent** command of the parent match-vlan class exceeds the value 50, that is, the shaper rate is more than 50 percent.

  Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: Ensure that the *percent* argument of the **shape percent** command of the parent match-vlan class does not exceed the value 50.

Further Problem Description: When the **bandwidth remaining percent** command is removed from the parent match-vlan class, the following error message is generated:

Please remove bandwidth from the child policy and re-issue command.

When you detach the parent policy from the main interface and re-attach it to the main interface, the child class miscomputes the bandwidth because it takes zero as reference rather than the shaper rate of the parent class.

- CSCse96084

  Symptoms: "Suspend/Activate service-policy" messages flood the console when there are thousands of sessions hosted on the router.

  Conditions: This symptom is observed on a Cisco 10000 series when the sessions come up or go down.

  Workaround: Disable console logging on the router.

  Further Problem Description: The messages are internal messages that should not appear on the console.

- CSCse97283

  Symptoms: ARPs may be lost. This situation may cause adjacencies to go down, which, in turn, may cause peer routers to stop responding.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only when buffer memory is extremely congested for one minute or more. For example, extreme congestion occurs when the "low buffer hdl drop(s)" counter in the output of the **show pxf cpu stat drop 1** increments at a rate that is equal to the incoming ARP traffic rate.

  Workaround: There is no workaround.

- CSCse99137

  Symptoms: A Cisco router that functions as an Intelligent Service Gateway (ISG) returns the wrong value in Cisco Vendor Specific Attribute (VSA) 250 (ssg-account-info) in a RADIUS packet.

  Conditions: This symptom is observed when the ISG responds to a service query from a Cisco Subscriber Edge Services Manager (SESM) or service provider portal server.

  Workaround: There is no workaround.

- CSCsf05044

  Symptoms: In a very large-scale MLPP configuration, that is, more than 300 MLP bundles, when a PRE-2 HA switchover occurs on a Cisco 10000 series, the following error message and/or a traceback may be generated on the connected Cisco 10000 series at the far end:

  ```
  ttcm_add_mlp_member: unable to install mlp link
  ```

  Conditions: This symptom is observed during the renegotiation of the links and line protocol of the interfaces and bundles.

  Workaround: There is no workaround.

- CSCsf05685

  Symptoms: A router that functions as a DHCP server and DHCP relay may fail to issue or renew a lease.

  Conditions: This symptom is observed after a class name is uploaded onto the DHCP server, which causes the parameters of DHCP-initiated sessions for an ISG to be changed.

Workaround: There is no workaround.

- CSCsf08208

  Symptoms: The username attribute is not present in the accounting stop records.

  Conditions: This symptom is observed when a PPP session is brought up with Transparent Auto logon (TAL).

  Workaround: There is no workaround.

- CSCsf10896

  Symptoms: The parent session ID attribute is not present in the accounting records for prepaid services.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when accounting is enabled for any prepaid service.

  Workaround: There is no workaround.

- CSCsf12056

  Symptoms: A LAC does not tap upstream packets via the CISCO-TAP2-MIB.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC and that has the Lawful Intercept feature enabled.

  Workaround: There is no workaround.

- CSCsf12124

  Symptoms: The policer conform, exceed, and violate counters (both packets and bytes) in the output of the **show policy-map interface** command may stop incrementing and freeze at a certain value.

  When this situation occurs, usually, the bytes counters freeze first, and then, after some time, the packet counters freeze too. This situation may also cause the “policer drop-rate bps counter” to become stuck at zero because the “policer drop-rate bps counter” is based on changes in the bytes counters.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and occurs when the counters are very large, that is, at or very near their limits.

  Temporary Workaround: Remove and then re-apply the policy map on the interface to reset the counters to zero.

- CSCsf13802

  Symptoms: eBGP sessions may go down when they are established on MFR subinterfaces with several VPNs between a Cisco 10000 series that functions as a PE router and a Cisco 7200 series that functions as a CE router.

  Conditions: This symptom is observed when the Cisco 10000 series has input and output service policies and Frame Relay fragmentation configured in a map class that is applied to DLCIs on the MFR subinterfaces. The symptom occurs while there is no traffic on the MFR link between the PE and CE routers.

  Workaround: Remove either the service policies or Frame Relay fragmentation from the map class.

- CSCsf15121

  Symptoms: Packets that are encapsulated via PPPoE and that are generated by a Cisco 10000 series and sent to a PPPoE client may take into account the padding of the incoming frame in the length field of the PPPoE header. This situation may cause problems for certain protocol stacks.

Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC or PTA router and that terminates PPP over Ethernet over ATM (PPPoEoA), PPP over Ethernet over Ethernet (PPPoEoE), PPP over Ethernet over Queue in Queue (PPPoEoQinQ), or PPP over Ethernet over VLAN (PPPoEoVLAN) sessions. The incoming frames are Ethernet or PPPoEoA frames, which can be padded because of the 64-byte minimum frame size requirement of Ethernet.

The symptom is caused by the fix for caveat CSCsd13298, which uses the full incoming frame size as the length field of the PPPoE header of the outgoing packet.

A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd13298. 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.

- CSCsf15164

  Symptoms: When a PRE-2 crashes and when the router is configured with a redundant PRE-2, a "PCI Retry Expire" error may occur after the crashinfo file has been generated.

  Conditions: This symptom is observed on a Cisco 10000 series and may occur even when the redundant PRE is not booted but remains in ROMmon.

  Workaround: There is no workaround.

  Further Problem Description: Note that the "PCI Retry Expire" error is not the original cause for the crash, but is a secondary issue.

- CSCsf17039

  Symptoms: A router may crash when you configure On-Demand Address Pools (ODAP) with Dynamic Host Configuration Protocol (DHCP) and when the router that requests the address pool (subnet) runs out of available addresses.

  Conditions: This symptom is observed in an MPLS-VPN network when you configure ODAPs on virtual home gateways (VHGs) and provider edge (PE) routers.

  Workaround: There is no workaround.

- CSCsf24720

  Symptoms: The PXF engine may crash when tapping is enabled.

  Conditions: This symptom is observed on a Cisco 10000 series that has the Lawful Intercept feature enabled when a truncation of the padding of a packet occurs, causing the Lawful Intercept feature to generate a replica.

  Workaround: There is no workaround.

- CSCsf25920

  Symptoms: The line protocol for an MFR interface may be up and the DLCIs may be in the active state even though the LMI is down.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB and occurs for MFR interfaces.

  Workaround: There is no workaround.

- CSCsf25978

  Symptoms: By default, a Cisco 10000 series PRE-2 should police a priority class to 95 percent of the link bandwidth to prevent other queues from starving. However, the priority class may use up to 100 percent of the link bandwidth if no policer is configured.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

Workaround: Configure a policer in the priority class.

- CSCsf27230

  Symptoms: When you configure a policy with WRED and shaping, random drops do not occur.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100.

  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 IISU. 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.

- CSCsf28159

  Symptoms: ISG accounting reports identical counter values for all services in the VSAs.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the "accounting-list" is removed from the VSAs that are included in the request from the Cisco Subscriber Edge Services Manager (SESM).

  Workaround: Configure the SESM to include the "accounting-list" in the VSAs that are sent to the ISG.

- CSCsf28725

  Symptoms: The **match cos** command does not function when it is applied to a QoS policy in the output direction.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 when the output policy map is configured on an interface that has an L2 VPN configuration.

  Workaround: There is no workaround.

- CSCsf30762

  Symptoms: When bidirectional traffic passes a 1-port Gigabit Ethernet half-height line card, the Gigabit Ethernet ingress and egress interface counters report zero packets/second and zero bits/second.

  Conditions: This symptom is observed on a Cisco 10000 series when there is a large number (at least 10,000) of interfaces and/or broadband sessions and when traffic is sent over the Gigabit Ethernet interface of a 1-port Gigabit Ethernet half-height line card.

  Workaround: There is no workaround.

- CSCsf96715

  Symptoms: The PXF engine may crash while a PPPoX session is established between a LAC and an LNS.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC and that has a QoS configuration.

Workaround: Disable the QoS configuration on the LAC.

- CSCsf98115

  Symptoms: AAA output counters for Tx bytes and octets remain zero or are incorrect for LAC sessions.

  Conditions: This symptom is observed on a Cisco 10000 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.

- CSCsg00072

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: The PXF engine may crash continuously.

     Condition 1: This symptom is observed on a Cisco 10000 series that has a PRE-2 and that is configured for LFI over ATM when IPCP is negotiated.

     Workaround 1: Disable the LFIoATM bundle interface.

  2. Symptom 2: Multilink PPP over ATM (MLPoA) member links may flap because of keepalive failures.

     Condition 2: This symptom is observed on a Cisco 10000 series that has a PRE-2 when keepalives are enabled on the bundle interface.

     Workaround 2: Disable keepalives on the bundle interface.

- CSCsg00438

  Symptoms: Some Cisco 10000 series line cards may become stuck.

  Conditions: This symptom is observed when the router functions in a redundant configuration and occurs after you have reloaded the router.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, power-cycle the affected line cards or perform an OIR of the affected line cards.

- CSCsg02980

  Symptoms: The CCM client holds up the Redundancy Framework (RF) progression.

  Conditions: This symptom is observed on a Cisco router that is configured for HA and PPP.

  Workaround: There is no workaround.

- CSCsg03916

  Symptoms: TACACS+ accounting on/off messages are not sent after a router has been reloaded.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for AAA and TACACS+ system accounting. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCsg09654

  Symptoms: After a switchover has occurred, "IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP" error messages are displayed on both the primary and standby RP, it takes while for the primary RP to come up, and the standby RP does not come up at all.

  Conditions: These symptoms are observed on a Cisco 7304 that has dual RPs that functions in SSO mode.

  Workaround: There is no workaround.

- CSCsg09825

  Symptoms: A Cisco 10000 series may crash when a PPPoE session is brought up.

  Conditions: This symptom is observed only when the VC over which the PPPoE session is brought up has both the **dbs enable** command and a queuing service policy enabled.

  Workaround: Either disable the **dbs enable** command or remove the queuing service policy before the PPPoE session is brought up.

- CSCsg11718

  Symptoms: A VRF may become stuck in the "Delete Pending" state.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and Half-Duplex VRF (HDVRF) when you delete the VRF and then associate it with an interface before it is completely deleted.

  Workaround: To ensure that the VRF is properly deleted, enter the **shutdown** interface configuration command on the interface with which the VRF is associated or remove the interface with which the VRF is associated.

- CSCsg12800

  Symptoms: A subscriber session setup fails when a VRF transfer is initiated at the start of the session.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG.

  Workaround: There is no workaround.

- CSCsg13086

  Symptoms: A router crashes when range PVCs are created on an Auto VC on a point-to-point subinterface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsg13118

  Symptoms: A Cisco 7304 crashes when you enter the **show warm-boot** command or **no warm-boot** command.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for warm reboot.

  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.

  Workaround: Remove the QoS configuration. If this is not an option, there is no workaround.

- CSCsg18289

  Symptoms: Applying a line loopback onto an ATM interface has no effect.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **loopback line** command on an ATM interface. The output of the **show interfaces atm** command shows that "loopback set" and "loopback line" appear in the configuration. However, the "loop" LED on the line card does not illuminate either. Traffic through the interface continues uninterrupted.

  Workaround: There is no workaround.

- CSCsg18894

  Symptoms: When you attempt to change or overwrite the **priority** command for a MQC priority queue, the command is rejected and the following error message is generated:

  ```
  priority not allowed in conjunction with queue-limit
  ```

  Conditions: This symptom is observed on a Cisco router that has the **queue-limit** command enabled in a MQC priority queue.

  Workaround: Remove the **queue-limit** command, modify the **priority** command, and then re-enter the **queue-limit** command.

- CSCsg19684

  Symptoms: A channel-group configuration on a physical interface is not removed when you perform an OIR of the port adapter on which the channel group is configured.

  Conditions: This symptom is observed on a cisco 7304 that is configured for Fast EtherChannel (FEC).

  Workaround: Enter the **no channel-group** *channel-number* command before you perform an OIR of the port adapter.

- CSCsg21425

  Symptoms: ACL entries that include L4 match criteria may not match properly.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 and an ACL with eight or less rules when at least one rule is a "permit" rule that specifies L4 matching criteria.

  Workaround: Add a few dummy rules to the ACL to ensure that the ACL has more than eight rules. Doing so enables the L4 match criteria to match properly.

- CSCsg24343

  Symptoms: A Cisco 7304 may crash when LFIoATM configured on a PA-A3-OC3MM port adapter that is installed in a PA-CC and when traffic starts to flow over the ATM link.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

- CSCsg24451

  Symptoms: Some line cards may be reported as deactivated when the router boots.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB and usually occurs for Gigabit Ethernet or Fast Ethernet line cards.

Workaround: Enter the **hw-mod subslot** *slot*/*subslot* **reset** command for each affected line card.

Alternate Workaround: Reload the router again.

- CSCsg27043

  Symptoms: On a 7304 series Network Services Engine (NSE), the passing of packets from the PXF engine to the RP may freeze for a period from seconds to minutes. This situation causes the router to lose its routing protocol neighbors.

  Conditions: This symptom is observed rarely on a Cisco 7304 that runs Cisco IOS Release 12.2S or Release 12.2SB.

  Temporary Workaround: If the symptom occurs repeatedly, reloading the router may help.

- CSCsg29086

  Symptoms: An ISG may crash and generate the following error messages and a traceback:

  ```
  %ALIGN-1-FATAL: Corrupted program counter 17:47:38 ESTDST Thu Oct 5 2006 pc=0x0,
  ra=0x0, sp=0x6436AB80
  %ALIGN-1-FATAL: Corrupted program counter 17:47:38 ESTDST Thu Oct 5 2006 pc=0x0,
  ra=0x0, sp=0x6436AB80
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x0 -Traceback=
  ```

  Conditions: This symptom is observed on a Cisco router that function as an ISG and that is configured for Dynamic Host Configuration Protocol (DHCP).

  Workaround: There is no workaround.

- CSCsg29539

  Symptoms: In an MPLS core that carries EoMPLS traffic, an ingress PE router that has a TE tunnel to an egress PE router may stop sending EoMPLS traffic after the TE tunnel is rerouted across a different path in the MPLS core. When you enable the **debug mpls packet** command on the first P router in the topology, the debugs show that the EoMPLS packets enter with the wrong (that is, the old) TE tunnel label.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that runs Cisco IOS Release 12.2(28)SB or one of its rebuilds.

  Workaround: Clear the interface.

- CSCsg30757

  Symptoms: The following symptoms may occur for prepaid accounting:

  – There are no gigabit word attributes 52 and 53 for prepaid service, but when you enable the **debug radius** command, attributes 52 and 53 are shown for the parent session.

  – The prepaid service always sends the rollover counters in “I” and “O” as zero although the definitions are “I<HC>;<LC>” and “O<HC>;<LC>” in which HC indicates the rollover counter and LC indicates the lower 32 bit of the input and output octets counters.

  The following is part of the debugs and shows “I0;1963039136” and “O0;1963039136” and no attributes 52 and 53 (“gigaword rollover counters”) although the amount of traffic over this service has exceeded the gigaword and has rolled over once already:

  ```
  RADIUS:   Cisco AVpair       [1]   36  "parent-session-id=0A0A440200000003"
  RADIUS:  Vendor, Cisco       [26]  21
  RADIUS:   ssg-control-info   [253] 15  "I0;1963039136"
  RADIUS:  Vendor, Cisco       [26]  21
  RADIUS:   ssg-control-info   [253] 15  "O0;1963039136"
  ```

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured with a prepaid service policy.

Workaround: There is no workaround.

- CSCsg31202

  Symptoms: A Cisco 7304 with an NSE-100 may crash and generate the following error message:

  ```
  Unexpected exception, CPU signal 10, PC = 0x4008B2EC
  ```

  Conditions: This symptom is observed very rarely when the router is configured with an input policy that marks incoming IP traffic on one interface and then uses this information for classification on an output policy on another interface.

  Workaround: There is no workaround.

- CSCsg32638

  Symptoms: The default MIR value for the priority queue is incorrectly set to the CIR value for the priority queue, causing latency and throughput problems on the priority queue.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround.

- CSCsg35305

  Symptoms: A Cisco router that functions as an Intelligent Service Gateway (ISG) reloads when you enter the **show database** command.

  Conditions: This symptom is observed when existing sessions are in the process of being disconnected and when you enter the **show database** command for these sessions.

  Workaround: Do not enter the **show database** command for sessions that are in the process of being disconnected.

- 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.

- CSCsg37423

  Symptoms: The output of the **show l2tun session l2tp** command does not include interface information.

  Conditions: This symptom is observed on a Cisco router that is configured for Xconnect.

  Workaround: There is no workaround.

- CSCsg40949

  Symptoms: The PXF engine of a Cisco 10000 series may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series when MLP is configured and when member links flap frequently.

  Workaround: There is no workaround.

- CSCsg43177

  Symptoms: Memory loss may occur when a microcode reload is being processed.

Conditions: This symptom is observed on a Cisco 10000 series that is configured as a 6PE router and occurs because of unnecessary allocation of IPv6 adjacencies.

Workaround: There is no workaround.

- CSCsg45686

  Symptoms: The following warning message may be generated when PPPoX sessions are being established:

  ```
  %C10K_BBA_SESSION-4-WRN2EVENT: Temporarily unable to add session to VC session list
  ```

  Although this warning message is a low-priority message, the number of messages may be quite high when a large number of sessions is being established.

  Conditions: This symptom is observed on a Cisco 10000 series when an operation fails during the attempt to establish a session.

  Workaround: There is no workaround. However, the error message has no system impact, and the session is established during a next attempt.

- CSCsg47298

  Symptoms: When an IP session is deleted, a Cisco 10000 series may reload because of an exception.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and that has both PBHK and police features installed for an IP session.

  Workaround: Do not configure police features for an IP session when PBHK is already configured for that IP session.

- CSCsg47598

  Symptoms: Unrecoverable memory loss may occur when you reload part or all of a configuration that has QoS policies that are active. In a large-scale configuration (that is, a configuration with many active policies), this situation may cause memory exhaustion.

  When the symptom occurs, the output of the **show processes memory sorted holding** command shows a reduction in free memory between reloads of the same configuration with QoS policies that are active.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsg47601

  Symptoms: When a Cisco router that functions as an Intelligent Service Gateway (ISG) also functions as a DHCP server or relay, the DHCP client may receive the wrong IP address or does not receive an IP address at all.

  Conditions: This symptom is observed when an IP DHCP session is terminated to a VRF via a service profile that is automatically activated during the session creation and when more than one auto service is configured in the user profile.

  Workaround: Configure only one auto service (VRF Service) in the user profile.

- CSCsg50778

  Symptoms: A Cisco 10000 series crashes because of memory violations when you attempt to set the 4096th tap.

  Conditions: This symptom is observed on a Cisco 10000 series that has the Lawful Intercept feature enabled.

  Workaround: The maximum number of taps is 4095. Do not set more than 4095 taps.

- CSCsg59671

  Symptoms: Accounting record counters are incorrect when accounting is applied to an IP Interface session.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) and occurs only for IP Interface sessions.

  Workaround: There is no workaround.

- CSCsg60122

  Symptoms: A Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) reloads when you enter the **show pxf cpu iedge ip-session vcci** *vcci id* command.

  Conditions: This symptom is observed when existing sessions are in the process of being disconnected while you enter the **show pxf cpu iedge ip-session vcci** *vcci id* command.

  Workaround: Do not enter the **show pxf cpu iedge ip-session vcci** *vcci id* command for sessions that are in the process of being disconnected when the console has a short terminal length.

- CSCsg64438

  Symptoms: When a prepaid service is unapplied from rules, the accounting stop record does not contain packet counts and octet counts.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the **service-policy type service unapply name** *policy-map-name* command (in which the *policy-map-name* argument indicates the prepaid service) is configured in the rules.

  Workaround for the packet counts: There is no workaround.

  Workaround for the octet counts: Look for the information in the following attributes that are present in the according stop record:

  ssg-control-info [253] 6 “I<high>;<low>”
  <low> indicates the input octets.

  ssg-control-info [253] 6 “O<high>;<low>”
  <low> indicates the output octets.

- 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.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reload the router.

- 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.

- CSCsg71993

  Symptoms: A DHCP client fails to receive an IP address from the DHCP server.

  Conditions: This is observed on a Cisco router that functions as an Intelligent Service Gateways (ISG) and DHCP server when the **initiator dhcp** IP subscriber configuration command is not enabled.

Workaround: Enter the **initiator dhcp** IP subscriber configuration command, either with or without the optional **class-aware** keyword.

- CSCsg72388

  Symptoms: A router crashes when a policy that uses a class map of the following form is configured in a policy map and applied to an interface:

  ```
  class-map match-any <classname>
      match <any match criteria>
      match ip rtp <odd number> 0
      <zero or more match clauses>
  ```

  Before the router crashes and enters the ROMmon prompt, the following error message is generated:

  ```
  "%ALIGN-1-FATAL: Illegal access to a low address"
  ```

  Conditions: This symptom is observed when you try to match on a range of zero UDP ports with a starting port number that is an odd number. Because the **match ip rtp** command can match only even-numbered ports, this configuration is equivalent to saying “match nothing.”

  Workaround: Specify an even-numbered starting port or a non-zero port range.

- 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.

- 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.

- CSCsg93274

  Symptoms: When a switchover occurs on the standby PRE, the router does not sent a ciscoRFSwactNotif notification.

  Conditions: This symptom is observed on a Cisco 10000 series when the CISCO-RF-MIB traps are enabled for host that are configured to receive traps, that is, for valid SNMP hosts that have the **snmp-server enable traps rf** command enabled.

  Workaround: Configure SNMPv2 “informs.”

  Alternate Workaround: Use a static ARP configuration for the trap handlers that are configured via the **snmp-server host** command to increase the chances that the first few traps that are sent by the Cisco 10000 series are received by these trap handlers.

TCP/IP Host-Mode Services

- CSCef52888

  Symptoms: Path MTU Discovery (PMTUD) may incorrectly select a higher MTU for an egress interface and may cause BGP to send packets that are larger than the size that the egress interface can support. When this situation occurs, packets are lost and the BGP session may be terminated.

Conditions: This symptom is observed when PMTUD is enabled over parallel links with different MTUs and when the paths in each direction use different links. Some other conditions may also apply, such as CEF and load-balancing being enabled.

Workaround: Enter the **ip tcp mss** command to configure the MSS to be less than the MTUs of all possible egress interfaces, or configure the MTUs of all possible egress interfaces to be same as the MSS.

- CSCse28222

  Symptoms: A router that is configured for NSR crashes and generates TCP tracebacks.

  Conditions: This symptom is observed on a Cisco router when a switchover occurs.

  Workaround: There is no workaround.

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.

- CSCek47644

  Symptoms: PPP keepalives are processed at in the slow path.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a broadband remote access server (BRAS) in an HA configuration and that has a virtual-template interface. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCek48265

  Symptoms: When you enter the **default ppp bcp tagged-frame** command, a traceback message may be generated on the console.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured for PPP.

  Workaround: There is no workaround.

- CSCek55136

  Symptoms: A Cisco 10008 router may restart because of a bus error.

  Conditions: This symptom is observed on a Cisco 10008 router that runs Cisco IOS Release 12.3(7)XI7b and that is configured for PPPoE. However, the symptom appears to be platform-independent and may also affect other releases.

  Workaround: There is no workaround.

- CSCek55209

  Symptoms: When the **ppp multilink endpoint mac** *lan-interface* command or the **ppp multilink endpoint ip** *ip-address* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual circuit is unconfigured.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink PPP.

Workaround: There is no workaround. Do not use these configuration commands in Cisco IOS Releases 12.3, 12.4 or 12.2SB without a fix for this DDTS.

- CSCek56250

  Symptoms: A router may reload while executing the **show ppp multilink** command.

  Conditions: This symptom is observed when a multilink bundle goes down while the output is being generated.

  Workaround: There is no workaround.

- CSCsc30497

  Symptoms: When NAS-port based pre-authorization fails, the PPPoE session limit per VLAN is no longer applied, that is, the local limit is no longer applied to a particular interface.

  Conditions: This symptom is observed in Cisco IOS Release 12.3YM but may also occur in other releases.

  Workaround: There is no workaround.

- CSCsd45915

  Symptoms: After a switchover has occurred, a virtual-access interface is created instead of a full virtual-access subinterface.

  Conditions: This symptom is observed on a Cisco router that is configured for PPP when a full virtual-template interface is first deleted and then reconfigured.

  Workaround: There is no workaround.

- CSCsd75854

  Symptoms: A router may generate a malformed PPPoE Active Discovery Offer (PADO) packet with two 802.1q tags. The first 802.1q tag contains the correct VLAN ID.

  Conditions: This symptom is observed on a Cisco router when the Service-Name field in the PPPoE Active Discovery Initiation (PADI) packet is empty and not equal to the one that is configured on the router.

  Workaround: Ensure that a correct Service-Name field in used in the PADI packet.

- CSCse05777

  Symptoms: A router may reload unexpectedly when you configure more multilink interfaces than the maximum number that the router can support. The router should not reload but should generate an error message.

  Conditions: This symptom is observed on any Cisco router that imposes a limit on the number of multilink interfaces.

  Workaround: Do not exceed the maximum number of multilink interfaces.

- CSCse29596

  Symptoms: PPPoA sessions cannot be brought up again after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco router when PPPoA sessions are first brought up on the active RP, then brought down by the peer, and then an SSO switchover occurs.

  Workaround: There is no workaround.

- CSCse66625

  Symptoms: A router does not accept the **pppoe max-sessions** *number* command on a subinterface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

Workaround: First configure the **pppoe max-sessions** *number* command on a BBA group, then attach this BBA group to the subinterface.

- CSCse78652

  Symptoms: The queuing mode on multilink interfaces erroneously defaults to fair-queuing instead of FIFO, causing distributed Cisco Express Forwarding (dCEF) to fail.

  Conditions: This symptom is observed on a Cisco 7500 series and occurs for all multilink interfaces. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCse78979

  Symptoms: PPPoA sessions do not synchronize to the standby PRE while VCs are recreated with a changed encapsulation type.

  Conditions: This symptom is observed on a Cisco 10000 series when you change the encapsulation type on the interface from MUX to SNAP and then back to MUX while PPPoA sessions are coming up. The symptom may be platform-independent.

  Workaround: There is no workaround.

- 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.

- CSCsf12042

  Symptoms: PPP over Ethernet over Ethernet (PPPoEoE) and PPPoE over Q-in-Q (PPPoEoQ-in-Q) sessions fail to be established.

  Conditions: This symptom is observed on a Cisco router when the connections are made via Fast Ethernet or Gigabit Ethernet interfaces. Note that the symptom does not affect PPP over Ethernet over ATM (PPPoEoA) sessions.

  Workaround: There is no workaround.

- CSCsg31095

  Symptoms: Per-user DNS and WINS attributes are ignored.

  Conditions: This symptom is observed on a Cisco router when RADIUS returns per-user DNS and WINS attributes that are the last attributes for the user profile.

  Workaround: Move the DNS and WINS attributes to a position in the RADIUS profile that ensures that they are not the last attributes.

- CSCsg34400

  Symptoms: A Cisco router that functions as a LAC may crash.

  Conditions: This symptom is observed when a PPPoE session is cleared by the client.

  Workaround: There is no workaround.

- CSCsg38412

  Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

Open Caveats—Cisco IOS Release 12.2(28)SB6

Cisco IOS Release 12.2(28)SB6 is a rebuild release for Cisco IOS Release 12.2(28)SB. This section describes a severity 3 caveat that is open in Cisco IOS Release 12.2(28)SB6. There are other open caveats in Cisco IOS Release 12.2(28)SB6. However, open caveats are normally listed only for maintenance releases, and the listing of CSCsg97961 is an exception.

Miscellaneous

- CSCsg97961

  Symptoms: A router may crash when you configure it with a high number of PPP over Ethernet over VLAN (PPPoEoVLAN) sessions that are spread over hundreds of VLAN subinterfaces.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 or PRE-3.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(28)SB6

Cisco IOS Release 12.2(28)SB6 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB6 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsc73699

  Symptoms: A router that is configured for NetFlow v9 may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S4 or Release 12.2(27)SBC1 when the configuration is modified while the router actively exports flows. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- 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.

- CSCse68964

  Symptoms: When a PTA session is created with a traffic classifier (TC) service, the Parent-Session-ID attribute of the accounting packets of the TC service on the ISG does not match the Acct-Session-Id of the parent session after 16^2 (that is, 000000EE) Acct-Session-Ids have been used.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG and that is configured with QinQ subinterfaces over which PTA sessions are established.

  Workaround: There is no workaround.

- CSCsf29098

  Symptoms: When you perform an OIR of a POS port adapter, a TLB Exception error may occur and the router may reset.

  Conditions: This symptom is observed on a Cisco router that has a POS port adapter with an interface that functions as an MPLS link in an AToM configuration when the POS interface has the **mpls ip** command enabled.

  Workaround: First disable the **mpls ip** command on the POS interface, then remove the AToM (Xconnect) configuration from the interface, and then perform an OIR of the POS port adapter.

- CSCsg48183

  Symptoms: A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

  Conditions: This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

  – You reload the router.

  – A switchover of the active RP occurs.

  – You enter the **redundancy force-switchover main-cpu** command.

  Workaround: There is no workaround.

- CSCsg77508

  Symptoms: The parent session Accounting STOP record is missing RADIUS attributes 42, 43, 47 and 48.

  Conditions: This symptom is observed on a Cisco router that is configured to terminate a PPP over Ethernet over L2TP session when you apply a service policy to the session. The symptom occurs only when the session is configured with at least one traffic classification with per-flow accounting.

  When the PPP over Ethernet client is terminated, the RADIUS attributes 42,43, 47 and 48 are missing from the parent session Accounting STOP record.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsc76550

  Symptoms: The RP may crash with a watchdog timeout error for the IP input process.

  Conditions: This symptom is observed on a Cisco router when you delete a subinterface that processes traffic.

  Workaround: Shut down the subinterface before you delete the subinterface.

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

- CSCed28542

  Symptoms: A router that is configured for PAT may generate the following error message and traceback while reporting slowness in the network:

  ```
  %SYS-2-INTSCHED: 'may_suspend' at level 3
  -Process= "IP NAT Ager", ipl= 3, pid= 118
  -Traceback= 80507F58 81310988 80CC14F8 80CD4F80 80CBAD30 80CBAD90 81321684 80CBB048
  80504118 805085E0
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(4)T and that has a high number (more than 2500) of NAT entries. The symptom is not release-specific.

  Workaround: There is no workaround.

- CSCsc98835

  Symptoms: OSPF and BGP change their state unexpectedly.

  Conditions: This symptom is observed on a Cisco router when a modification of a shared access control list (ACL) that is called from more than 300 route maps causes a CPUHOG condition in the Virtual Exec Process.

  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 the 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.

Miscellaneous

- CSCef43197

  Symptoms: A router may crash when you enter the **no ip routing** command.

  Conditions: This symptom is observed on a Cisco router that has the **set ip next-hop** command enabled in a policy-based routing configuration and occurs when the router attempts to access freed adjacencies.

Workaround: Remove the **set ip next-hop** command from the route map before you enter the **no ip routing** command.

- CSCei22697

  Symptoms: Some MVPN tunnels are mapped to an incorrect VRF forwarding table.

  Conditions: This symptom is observed on a Cisco router that is configured for data MDT groups.

  Workaround: There is no workaround.

- 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 PAM 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
```

- CSCek38382

  Symptoms: The standby PRE-2 crashes because of a debug exception, and the standby PRE-2 console shows the following error messages and traceback before the crash occurs:

```
%SYS-2-ASSERTION_FAILED: Assertion failed: "(*parents_ptr)->coll_magic ==
COLL_MAGIC_VAL"
-Process= "Deferred Adj Background", ipl= 0, pid= 167
-Traceback= 6050CA04 604AA1B4 60362364 60362510 603630A4 6035B67C 60360598 60FFAB30
60FF54A0 60FF5578

%Software-forced reload
```

  Conditions: This symptom is observed on a Cisco 10000 series after an ATM line card is reset.

  Workaround: There is no workaround.

- CSCek40657

  Symptoms: A PTA router may crash when you download a configuration with a class map, policy map, and PVC range to a point-to-point interface.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PTA router.

  Workaround: There is no workaround.

- CSCek54106

  Symptoms: When you convert a non-queueing policy map to a queueing policy map and attach it to interfaces that do not support queuing, the QoS policy is removed from the interfaces and existing sessions.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Convert the non-queueing policy map to a queueing policy map before you apply it to interfaces or bring up sessions.

- CSCek54768

  Symptoms: E1 interfaces may go down when a line card is reset or removed even when the line card has APS enabled and an APS cutover is triggered. The interfaces do come back up within a few seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has a pair of 4-port channelized OC-3 line cards that are configured for SR-APS. The line cards are configured with E1 interfaces under either SONET or SDH.

  Workaround: Enter the **force** command in APS group configuration mode on both the router on which the line card is reset or removed and on the router at the far end to ensure that the line card that is reset or removed does not receive or transmit the active traffic.

  Note that the chances of the symptom occurring may be reduced when the line card that is reset or removed is not the active line card.

  Further Problem Description: This symptom occurs only when a line card is reset or removed, not when an APS switchover is triggered by a fiber cable that is removed.

  The symptom occurs because of a change in the E1 clock source that may occur when the line card is reset or removed and that causes alarms to be received. The symptom is more likely to occur when the line card has a large configuration and when the E1 interfaces are set to “clock source line.”

- CSCek57646

  Symptoms: On a Cisco 10000 series, tracebacks and an error message that is related to the link index may be generated, and MLPoATM links continue to flap. The error message is similar to the following:

  ```
  %GENERAL-3-EREVENT: ttcm_add_mlp_member: 1926 No free link index available in
  Virtual-Access15
  ```

  Conditions: This symptom is observed when a member link of an MLPoATM bundle is modified.

  Workaround: There is no workaround.

- CSCek65046

  Symptoms: After a microcode reload has occurred, traffic is dropped for all users that have a per-user ACL configured and for which the user IP address is specified in the ACL.

  Conditions: This symptom is observed on a Cisco 10000 series when a per-user ACL is applied to each session and when an ACL Template is enabled.

  Workaround: After you have performed a microcode reload, disconnect and reconnect all sessions. Note that it is very likely that a user will reconnect a session after traffic has dropped.

- CSCir01277

  Symptoms: A Cisco 7304 may reload unexpectedly because of a watchdog reset condition, which can be seen in the output of the **show version** command.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

- CSCsa92748

  Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

  ```
  Last reset from watchdog reset
  ```

  Conditions: This symptom is observed only on Cisco 7200 and Cisco 7301 series routers that are configured with an NPE-G1 Network Processing Engine.

  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.

- CSCsd08862

  Symptoms: A router may crash because of a bus error when you enter the **show interface** command or another command that displays the virtual-access information for a virtual-access interface or subinterface.

  Conditions: This symptom is observed while a session that is associated with the virtual-access interface or subinterface is being cleared.

  Workaround: There is no workaround.

- CSCsd19951

  Symptoms: When you attach a service policy to a POS interface and enter the **show policy-map interface** command, a spurious memory access and traceback are generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x6184E5E8 reading 0x4
  %ALIGN-3-TRACE: -Traceback= 6184E5E8 6183E7C4 6184144C 6083B758 6083AF40 608416B4
  60841724 60841D80
  ```

  Conditions: This symptom is observed on a Cisco router only when a service policy has LLQ configured.

  Workaround: There is no workaround.

- CSCsd40153

  Symptoms: An ASBR has “No Label” as its outgoing label for a peer ASBR interface address.

  Conditions: This symptom is observed when the following conditions occur:

  – An ISP network (ISP network A) has two ASBRs that peer with one ASBR in another ISP network (ISP network B).

  - IGP routing (OSPF or any other IGP) is configured between the ASBRs in ISP network A.
  - A BGP session between one ASBR in ISP network A and the ASBR in ISP network B flaps.

  After about 5 minutes, all routes that are reachable via the ASBRs in ISP network A and the ASBR in ISP network B have "No Label" as their outgoing label.

  Workaround: Enter the **clear ip route** *network* command.

- CSCsd45936

  Symptoms: When a two-level hierarchical policy map in which the parent level has only a class default is already attached to an interface and when you configure a policer for both the parent and child levels, either of the following symptoms may occur:

  - When the child policy map is removed from the class default of the parent policy map, the traffic policing rate does not properly reflect the parent policer rate.
  - When the child policy map is attached to the class default of parent policy map, the traffic policing rate does not properly reflect the child policer rate.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

  Workaround: After the child policy is removed from or attached to the parent policy map, detach the policy map from the interface and re-attach it to the interface.

- CSCsd51309

  Symptoms: A platform may pause indefinitely or reload unexpectedly when you disable the MPLS Traffic Engineering AutoTunnel Mesh Groups feature.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series but is platform-independent.

  Workaround: There is no workaround.

- CSCse23232

  Symptoms: When a virtual template or user profile contains a service policy with class maps, the router may send not one but a number of RADIUS accounting-request packets for each PPPoE or PPPoEeoA session. The number of RADIUS accounting-request packets equals the number of class maps in the service policy. Each accounting-request packet has its own unique "acct- session-id."

  Conditions: This symptom is observed on a Cisco router that is configured with a QoS policy.

  Workaround: There is no workaround.

- 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.

  Workaround: There is no workaround.

- CSCse57312

  Symptoms: The MQC output policer does not add the L2 header as part of its calculation.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only for multicast traffic on Ethernet and ATM interfaces.

  Workaround: There is no workaround.

- CSCse72235

  Symptoms: A Cisco 7200 series may crash because of an address error with corrupted program counter at “pc=0xAFACEFAD.” This precise value is repeated in the traceback and in the “EPC,” “BadVaddr,” and “ra” registers. The crash may be preceded by a “%SYS-2-GETBUF: Bad getbuffer” error message.

  Conditions: This symptom is observed on a Cisco 7200 VXR router that has an NPE-G1 and that runs Cisco IOS Release 12.2(28)SB2. The router is configured as a LAC with PPPoA and MPLS fragmentation for packets that travel from a PPPoA interface through an L2TP tunnel to an interface that is configured for MPLS.

  Workaround: Disable MPLS.

  Alternate Workaround: Disable fragmentation.

- CSCsf04423

  Symptoms: On a Cisco platform that is configured for MPLS and NetFlow, all traffic that leaves an interface may be process-switched, causing high CPU usage under the IP Input process. The symptom can be verified in the output of the **show interface statistic** command.

  Conditions: This symptom is observed when the **ip flow ingress** command is enabled on any interface on the platform and when MPLS is also enabled.

  Workaround: Enable MPLS-Aware NetFlow by entering the **ip flow-cache mpls label-positions** *label-position-1* command. Doing so prevents traffic from being process-switched, but note that additional MPLS fields are added to the NetFlow export records.

- CSCsf05044

  Symptoms: In a very large-scale MLPP configuration, that is, more than 300 MLP bundles, when a PRE-2 HA switchover occurs on a Cisco 10000 series, the following error message and/or a traceback may be generated on the connected Cisco 10000 series at the far end:

  ```
  ttcm_add_mlp_member: unable to install mlp link
  ```

  Conditions: This symptom is observed during the renegotiation of the links and line protocol of the interfaces and bundles.

  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.

- CSCsf19731

  Symptoms: The newly active PRE crashes immediately after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series when an SSO switchover is triggered via SNMP.

Workaround: Do not trigger an SSO switchover via SNMP. Rather use the CLI to trigger an SSO switchover.

- CSCsf27230

  Symptoms: When you configure a policy with WRED and shaping, random drops do not occur.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsf28159

  Symptoms: ISG accounting reports identical counter values for all services in the VSAs.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the "accounting-list" is removed from the VSAs that are included in the request from the Cisco Subscriber Edge Services Manager (SESM).

  Workaround: Configure the SESM to include the "accounting-list" in the VSAs that are sent to the ISG.

- 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.

- CSCsf97199

  Symptoms: High CPU usage may occur during the "XDR mcast" and "XDR RP" background processes. Each of these processes uses more than 30 percent of the CPU while no data traffic passes through the router.

  Conditions: This symptom is observed on a Cisco 10000 series but is platform-independent.

  Workaround: Reload the router.

- CSCsg11718

  Symptoms: A VRF may become stuck in the "Delete Pending" state.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and Half-Duplex VRF (HDVRF) when you delete the VRF and then associate it with an interface before it is completely deleted.

  Workaround: To ensure that the VRF is properly deleted, enter the **shutdown** interface configuration command on the interface with which the VRF is associated or remove the interface with which the VRF is associated.

- 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.

- CSCsg27043

  Symptoms: On a 7304 series Network Services Engine (NSE), the passing of packets from the PXF engine to the RP may freeze for a period from seconds to minutes. This situation causes the router to lose its routing protocol neighbors.

Conditions: This symptom is observed rarely on a Cisco 7304 that runs Cisco IOS Release 12.2S or Release 12.2SB.

Temporary Workaround: If the symptom occurs repeatedly, reloading the router may help.

- CSCsg29539

  Symptoms: In an MPLS core that carries EoMPLS traffic, an ingress PE router that has a TE tunnel to an egress PE router may stop sending EoMPLS traffic after the TE tunnel is rerouted across a different path in the MPLS core. When you enable the **debug mpls packet** command on the first P router in the topology, the debugs show that the EoMPLS packets enter with the wrong (that is, the old) TE tunnel label.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that runs Cisco IOS Release 12.2(28)SB or one of its rebuilds.

  Workaround: Clear the interface.

- CSCsg30757

  Symptoms: The following symptoms may occur for prepaid accounting:

  – There are no gigabit word attributes 52 and 53 for prepaid service, but when you enable the **debug radius** command, attributes 52 and 53 are shown for the parent session.

  – The prepaid service always sends the rollover counters in “I” and “O” as zero although the definitions are “I<HC>;<LC>” and “O<HC>;<LC>” in which HC indicates the rollover counter and LC indicates the lower 32 bit of the input and output octets counters.

  The following is part of the debugs and shows “I0;1963039136” and “O0;1963039136” and no attributes 52 and 53 (“gigaword rollover counters”) although the amount of traffic over this service has exceeded the gigaword and has rolled over once already:

```
RADIUS:   Cisco AVpair       [1]   36  "parent-session-id=0A0A440200000003"
RADIUS:  Vendor, Cisco       [26]  21
RADIUS:   ssg-control-info   [253] 15  "I0;1963039136"
RADIUS:  Vendor, Cisco       [26]  21
RADIUS:   ssg-control-info   [253] 15  "O0;1963039136"
```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured with a prepaid service policy.

  Workaround: There is no workaround.

- CSCsg31202

  Symptoms: A Cisco 7304 with an NSE-100 may crash and generate the following error message:

```
Unexpected exception, CPU signal 10, PC = 0x4008B2EC
```

  Conditions: This symptom is observed very rarely when the router is configured with an input policy that marks incoming IP traffic on one interface and then uses this information for classification on an output policy on another interface.

  Workaround: There is no workaround.

- CSCsg35305

  Symptoms: A Cisco router that functions as an Intelligent Service Gateway (ISG) reloads when you enter the **show database** command.

  Conditions: This symptom is observed when existing sessions are in the process of being disconnected and when you enter the **show database** command for these sessions.

  Workaround: Do not enter the **show database** command for sessions that are in the process of being disconnected.

- CSCsg37423

  Symptoms: The output of the **show l2tun session l2tp** command does not include interface information.

  Conditions: This symptom is observed on a Cisco router that is configured for Xconnect.

  Workaround: There is no workaround.

- CSCsg40949

  Symptoms: The PXF engine of a Cisco 10000 series may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series when MLP is configured and when member links flap frequently.

  Workaround: There is no workaround.

- CSCsg64438

  Symptoms: When a prepaid service is unapplied from rules, the accounting stop record does not contain packet counts and octet counts.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the **service-policy type service unapply name** *policy-map-name* command (in which the *policy-map-name* argument indicates the prepaid service) is configured in the rules.

  Workaround for the packet counts: There is no workaround.

  Workaround for the octet counts: Look for the information in the following attributes that are present in the according stop record:

  ssg-control-info [253] 6 “I<high>;<low>” <low> indicates the input octets.

  ssg-control-info [253] 6 “O<high>;<low>” <low> indicates the output octets.

- 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.

- CSCsg93274

  Symptoms: When a switchover occurs on the standby PRE, the router does not sent a ciscoRFSwactNotif notification.

  Conditions: This symptom is observed on a Cisco 10000 series when the CISCO-RF-MIB traps are enabled for host that are configured to receive traps, that is, for valid SNMP hosts that have the **snmp-server enable traps rf** command enabled.

  Workaround: Configure SNMPv2 “informs.”

  Alternate Workaround: Use a static ARP configuration for the trap handlers that are configured via the **snmp-server host** command to increase the chances that the first few traps that are sent by the Cisco 10000 series are received by these trap handlers.

Wide-Area Networking

- CSCek55209

  Symptoms: When the **ppp multilink endpoint mac** *lan-interface* command or the **ppp multilink endpoint ip** *ip-address* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual circuit is unconfigured.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink PPP.

  Workaround: There is no workaround. Do not use these configuration commands in Cisco IOS Releases 12.2SB, 12.3, and 12.4 without a fix for this DDTS.

- CSCek56250

  Symptoms: A router may reload while executing the **show ppp multilink** command.

  Conditions: This symptom is observed when a multilink bundle goes down while the output is being generated.

  Workaround: There is no workaround.

- CSCse66625

  Symptoms: A router does not accept the **pppoe max-sessions** *number* command on a subinterface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: First configure the **pppoe max-sessions** *number* command on a BBA group, then attach this BBA group to the subinterface.

- CSCsg38412

  Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

  Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

  Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

- CSCsg39977

  Symptom: When dialer interfaces are used in conjunction with Multilink PPP (MLP), a router may crash because of a corrupted program counter.

  Conditions: This symptom is observed on a Cisco router when a dialer interface, including interfaces such as ISDN BRI and PRI interfaces, is configured to use MLP and when the queueing mode on the dialer interface is configured for Weighted Fair Queuing (WFQ). Note that WFQ is the default for some types of dialer interfaces.

  Workaround: There is no workaround.

- CSCsg56725

  Symptoms: When you enter the **terminate-from hostname** *host-name* 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 platform-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.

Resolved Caveats—Cisco IOS Release 12.2(28)SB5

Cisco IOS Release 12.2(28)SB5 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB5 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCef29931

  Symptoms: When a Telnet connection to a router that is configured for secure login fails, memory corruption may occur on the router, and the router may reload.

  Conditions: This symptom is observed when the **login block-for** *seconds* **attempts** *tries* **within** *seconds* command is enabled on the router and when a user enters an incorrect password for the *tries* argument.

  When the Telnet connection fails, the router enters the quiet mode. When the router leaves the quiet mode, the router is able to accept Telnet connections. However, when the Telnet connections fails again, memory corruption occurs before the router enter the quite mode, and the router reloads.

  Workaround: There is no workaround.

- CSCeg52893

  Symptoms: Several tty lines may become stuck in the “Carrier Dropped” modem state. You can verify this situation by entering the **show line** *line-number* EXEC command for an individual line. However, when you enter the show line EXEC command (that is, you do not enter a value for the *line-number* argument), the output shows that the same tty lines are active (that is, they are in the “*” state):

```
......
I   2/47 Digital modem - DialIn  -  -  -   7   0   0/0   -  Idle
I   2/48 Digital modem - DialIn  -  -  -   7   0   0/0   -  Idle
*   2/49 Digital modem - DialIn  -  -  -   5   0   0/0   -  Carrier Dropped
I   2/50 Digital modem - DialIn  -  -  -   7   0   0/0   -  Idle
I   2/51 Digital modem - DialIn  -  -  -  13   0   0/0   -  Idle
I   2/52 Digital modem - DialIn  -  -  -  10   0   0/0   -  Idle
......
```

  In addition, both the output of the **show users** EXEC command and the output of the **show caller** EXEC command do not show a user or caller name or show an incorrect user or caller name. The output of the **show caller** EXEC command does show that the service is “TTY.”

  Conditions: These symptoms are observed on a Cisco AS5400 that is configured for modem dial-in with PPP and EXEC connectivity and for login authentication via a TACACS+ server. The symptom is platform-independent.

  Workaround: To clear the stuck line, enter the **clear port** *slot*/*port* EXEC command.

- 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.

- CSCsc29669

  Symptoms: A bulk synchronization mismatch may occur when a switchover occurs on a Cisco 10000 series, or when you reload the router. This situation prevents the router from reaching the STANDBY HOT redundancy state in a timely manner.

  Conditions: This symptom is observed when you first define ann AAA attribute list and then force a switchover to occur. Just before the newly active PRE is supposed to enter the STANDBY HOT redundancy state, the following error messages are generated:

  ```
  Config Sync: Bulk-sync failure due to BEM mismatch. Please check the full list of BEM
  failures via:
    show issu config-sync failures bem
  Config Sync: Starting lines from BEM file:
    -aaa attribute list xxxxx
  ```

  Note that the symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCse09594

  Symptoms: A router crashes during the AAA authentication process for interfaces that are configured for PPP.

  Conditions: This symptom is observed on a Cisco router when the memory is exhausted. For example, the symptom may occur on a router that attempts to bring up more PPP sessions while its memory usage is already higher than 99 percent of the capacity because of existing configuration and sessions.

  Workaround: There is no workaround.

- CSCse70574

  Symptoms: RADIUS attributes for Acct-Input-Gigawords and Acct-Output-Gigawords counters are not present in per-service accounting on an ISG. Octets counters overflow, but the Gigawords attributes are not included in the accounting records for the service, preventing the RADIUS billing server from being notified that the input and output counters have rolled over.

  Conditions: This symptom is observed on a Cisco 10000 that runs Cisco IOS Release 12.2(28)SB2 and that functions as an ISG. The symptom may be platform-independent.

  Workaround: There is no workaround.

  Further Problem Description: RADIUS attributes for Acct-Input-Gigawords and Acct-Output-Gigawords counters are being counted and function properly for parent PPP sessions on an ISG.

Interfaces and Bridging

- CSCsa87986

  Symptoms: A router may intermittently transmit corrupt PPP packets. When you enter the **debug ppp nego** and **debug ppp errors** commands, it appears that "protocol reject" packets are received from the remote end.

  Conditions: This symptom is observed on a Cisco 7500 series that has only one OC-3 POS port adaptor per VIP and that is configured for PPP encapsulation.

  Workaround: Configure an outbound policy on the interfaces of the OC-3 POS port adaptors.

IP Routing Protocols

- CSCec12299

  Symptoms: EIGRP-specific Extended Community 0x8800 is corrupted and shown as 0x0:0:0.

  Conditions: This symptom is observed when EIGRP-specific Extended Community 0x8800 is received via an IPv4 EBGP session. This occurs typically in the following inter-autonomous system scenario:

  ```
  ASBR/PE-1 <----> VRF-to-VRF <----> ASBR/PE-2
  ```

  Workaround: Disable propagation of extended communities across autonomous systems.

- 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.

- CSCei77227

  Symptoms: A Cisco router that functions in a multicast VPN environment may crash.

  Conditions: This symptom is observed when you check the unicast connectivity and then unconfigure a VRF instance.

  Workaround: There is no workaround.

- CSCek33991

  Symptoms: A router may reset unexpectedly when it is in the midst of output of the results of the **show interface dampening** command, and the interface is deleted from another vty connection.

  Conditions: This symptom can be encountered if concurrent connections are opened to a router, and the **show interface dampening** command is issued while interface(s) are deleted.

Workaround: Ensure interfaces with **dampening** configured are not deleted while the **show interface dampening** command can be possibly issued on another vty.

- 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.

- CSCsb09852

  Symptoms: The number of networks in the BGP table and the number of attributes increases, and a slower convergence may occur for members of a BGP update group.

  Conditions: This symptom is observed on a Cisco router when the members of a BGP update group go out of synchronization with each other in such a way that they have different table versions, preventing the BGP Scanner from freeing networks that do not have a path.

  To check if the members of the BGP update group are in synchronization with each other, enter the **show ip bgp update-group summary** command and look at the table version for each member. If they have the same table version, they are in synchronization with each other; if they do not, they are out of synchronization with each other.

  Workaround: To enable the members of the BGP update group to synchronize with each other, enter the **clear ip bgp * soft out** command. Doing so does not bounce the sessions but forces BGP to re-advertise all prefixes to each member.

- CSCsb36755

  Symptoms: When BGP receives an update that has a worse metric route than the previously received route for equal-cost multipath, the BGP table is updated correctly but the routing table is not, preventing the old path from being deleted from the routing table.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP multipath.

  Workaround: Enter the **clear ip route** *network* command.

- CSCsb50606

  Symptoms: Memory utilization 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.

- 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.

- CSCsd59023

  Symptoms: ARP entries that are associated with the default interface (of the default route or network) are refreshed when they should not be refreshed.

  Conditions: This symptom is observed on a Cisco router when other interfaces change their state or when the IP configuration of other interfaces is changed.

  Workaround: There is no workaround.

- CSCsd67591

  Symptoms: A router may crash when you modify parameters of the **route-map** command for a redistribution statement.

  Conditions: This symptom is observed when you modify the parameters of the **route-map** command for a redistribution statement of an OSPF process that was deleted.

  Workaround: Delete the redistribution statement before you delete the OSPF process.

- CSCse41600

  Symptoms: A router may crash when VRFs and BGP configurations are removed quickly.

  Conditions: This symptom is observed on a Cisco router that has many VRFs and BGP configurations.

  Workaround: Remove the VRFs and BGP configurations slowly to avoid timing issues.

- CSCse51629

  Symptoms: A router may crash when use the **copy tftp:** *filename* **system:running-config** command for bulk unconfiguration of subinterfaces.

  Conditions: This symptom is observed on a Cisco router that has a large number of PVCs (that is, more than 200) and many subinterfaces, that is configured for OSPF, and that is processing traffic from 40,000 IP source addresses.

  Workaround: Do not use the **copy tftp:** *filename* **system:running-config** command for bulk unconfiguration of subinterfaces.

- 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.

- 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.

Miscellaneous

- CSCeb80947

  Symptoms: Disconnecting VPDN users via the CISCO-AAA-SESSION-MIB does not work.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(13)T or a later release of Release 12.2T. The symptom may also occur in other Cisco IOS software release trains.

  Workaround: There is no workaround.

- CSCeg26728

  Symptoms: BGP may fail to establish a peer with another router when an output service policy is configured on an interface and the output service policy limits the bandwidth to 199 kbps for packets that have the IP precedence value set to 6.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(14)S9. However, the symptom is not platform- and release-specific.

  Workaround: Remove the output service policy from the interface.

- CSCei38741

  Symptoms: Tracebacks are generated on a Cisco 10000 series that is configured with serial interfaces.

  Conditions: This symptom is observed when you change the encapsulation on a serial interface from PPP to Frame Relay.

  Workaround: Before you change the encapsulation from PPP to Frame Relay, enter the **no encapsulation ppp** command.

- CSCei80699

  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 PIM and MDT multicast tunnels.

  Workaround: There is no workaround.

- CSCej87817

  Symptoms: Policing does not drop any packets after the packets are sent or received at a rate that is much higher than the committed information rate (CIR).

  Conditions: This symptom is observed on a Cisco 7500 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCek25192

  Symptoms: When you configure traffic policing in percentages, the following error message floods the console:

  ```
  Maximum rate for the policer is 0. Conform action is drop.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for Control Plane Policing (CoPP).

  Workaround: There is no workaround.

- CSCek27377

  Symptoms: A Cisco 7304 that is configured for QoS may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 when you apply or remove a policy map on an egress interface and occurs only when the policy map invalidly has a **shape** command at both the parent and child levels.

  Workaround: There is no workaround.

- CSCek32110

  Symptoms: A Cisco 7304 may crash because of a bus error when you perform an OIR of an ATM line card while traffic is passing through the line card.

  Conditions: This symptom is observed when the ATM line card is configured with many VCs and when traffic is switched while the PXF engine is disabled.

  Workaround: There is no workaround.

- CSCek33894

  Symptoms: When an HA switchover occurs, the standby RP resets continuously.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when service policy maps access traffic class maps.

  Workaround: There is no workaround.

- CSCek40192

  Symptoms: Traffic convergence takes more than 50 ms after an Automatic Protection Switching (APS) switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCek42178

  Symptoms: An APS switchover does not occur at the far end when you enter the **hw-module slot reset** command at the near end.

  Conditions: This symptom is observed on a Cisco 10000 series

  Workaround: There is no workaround.

- CSCek42422

  Symptoms: SNMP MIB entries for the following GBIC/SFPs are missing from Cisco OS Release 12.2(28)SB and later releases:

  - CWDM-1470
  - CWDM-1490
  - CWDM-1510
  - CWDM-1530

  - CWDM-1550
  - CWDM-1570
  - CWDM-1590
  - CWDM-1610

  Conditions: This symptom is observed on a Cisco 7304 when you issue a SNMP Get command for the ENTITY-MIB.

  Workaround: There is no workaround.

- CSCek43620

  Symptoms: A bulk synchronization may fail because of a “best-effort method” mismatch, causing the standby PRE to reset unexpectedly.

  Conditions: This symptom is observed on a Cisco 10000 series when APS is configured for an ATM line card and when one or more ports are administratively down.

  Workaround: Either remove the APS configuration from the ATM line card or bring up all the ports by entering the **no shutdown** interface configuration command before the standby PRE is loaded. Then, after the standby PRE has loaded, you may return the port(s) to the administratively down state.

- CSCek46087

  Symptoms: Interprocessor communication within line cards that are installed in a router chassis may not function properly.

  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.

- CSCek47252

  Symptoms: A Cisco 7304 may reload unexpectedly when you enter the **show diag** *slot-number* command for a Port Adapter Carrier Card (7300-CC-PA).

  Conditions: This symptom is observed rarely on a Cisco 7304 and occurs only when the **show diag** *slot-number* command causes the 7300-CC-PA to reset unexpectedly.

  Workaround: To prevent the symptom from occurring, do not enter the **show diag** *slot-number* command or the **show tech-support** command, which includes the **show diag** *slot-number* command.

- CSCek49488

  Symptoms: When a Cisco IOS software image is loaded onto a Cisco 7304 that has a Port Adapter Carrier Card (7300-CC-PA), the error messages similar to the following may be generated and the 7300-CC-PA may reload unexpectedly:

  ```
  %LC-3-LCI2C_ERROR: PA Carrier Card Linecard I2C bus access failed at slot 4, status
  = 0x1
  -Traceback= 4056860C 407A2D10 4072F8C0 40737FE8 406DC95C 4066A304

  %LC-3-CLFPGAERROR: Line card common logic fpga (slot 4) error: Egress data fifo
  controller error

  %LC-3-CLFPGAERROR: Line card common logic fpga (slot 4) error: Bad control code
  (0x8888) from egress data port o

  %LC-3-RECOVERY: Line card (slot 4) recovery in progress
  -Traceback= 4056860C 407310F0 407388D0 401F38E8 40736F48 407373D8 406D3498 406268B4
  4056FEDC 40570270 40648F04 40648EF0

  %LC-6-VIRTUALINIT: Line card (slot 4) - initialization in virtual mode
  ```

The same symptom may occur when you enter the **hw-module slot** *slot-number* **stop** command followed by the **hw-module slot** *slot-number* **start** command to stop and restart the 7300-CC-PA.

Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB, 12.2(28)SB1, 12.2(28)SB2, 12.2(28)SB3, or 12.2(28)SB4.

Workaround: There is no workaround. However, the 7300-CC-PA recovers automatically.

- CSCek49580

  Symptoms: The configuration may become lost, the standby PRE may crash, the active PRE may crash, and other problems may occur.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for RPR+ when you enter the **bert t3** command from the controller menu or when you abort the **bert t1** command during execution.

  Workaround: Only enter the **bert t3** command from the interface menu, and do not abort the **bert t1** command during execution.

- CSCek51309

  Symptoms: A router may reload when a QoS policy is attached to a number of PPPoL2TP sessions on an LNS and when the physical link or sessions are flapping. The QoS policy contains a shaping and queuing configuration.

  Conditions: This symptom is observed on a Cisco router that functions as an LNS when there are many route changes, either because a physical interface flaps or because the PPPoL2TP sessions flap.

  Workaround: There is no workaround.

  Further Problem Description: The symptoms are specific to L2TP sessions and queuing features in the policy map.

- CSCek52915

  Symptoms: A router may lock up and all forwarding may stop after a priority statement is first removed and then returned into an LLQ policy map.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with 100 ATM VCs and that processes voice and data traffic.

  Workaround: There is no workaround.

- CSCek57494

  Symptoms: All packets may be dropped across a T1 or E1 link on which class-based shaping is configured.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 and that runs Cisco IOS Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCin99687

  Symptoms: An SNMP walk of the dsx1IntervalTable results in an infinite loop.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MCX-8TE1 or PA-MC-2T3+ port adapter.

  Workaround: There is no workaround.

- CSCin99753

  Symptoms: When you enter the **test pppoe** command on the PPPoE client, the PPPoE client or PPPoE server crashes.

Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that functions as a PPPoE client or PPPoE server. When the Cisco 7304 functions as a server and you enter the **test pppoe** command on another Cisco 7304 that functions as a PPPoE client, the PPPoE server crashes. When another router functions as the PPPoE server and a Cisco 7304 functions as the PPPoE client, the PPPoE client crashes.

Workaround: There is no workaround.

- CSCir00106

  Symptoms: IPC timeout messages may be generated on a Cisco 7304 that has an NSE-100.

  Conditions: This symptom is observed when the CPU usage of the router is at 100 percent, when the PXF engine is switched off, and when there is a heavy traffic that is punted to the RP.

  Workaround: Enable PXF switching by entering the **ip pxf** command.

- 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.

  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.

- CSCsc42938

  Symptoms: A router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) may crash when LDP is configured globally or on an interface.

  Conditions: This symptom is observed when you enter the **show mpls ldp neighbor** command while LDP sessions are coming up or going down.

  Workaround: There is no workaround.

- CSCsc60242

  Symptoms: ATM subinterfaces may flap unexpectedly and cause the routing protocol neighbor to flap.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 and occurs when the OAM queue depth is not set correctly.

  Workaround: There is no workaround.

- CSCsd11815

  Symptoms: The **random-detect precedence** *precedence min-threshold max-threshold* Interface is not accepted. This situation prevents the packets that match the value of *precedence* argument from being dropped.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

Workaround: There is no workaround.

- CSCsd15575

  Symptoms: Packets are not forwarded via a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **no service pxf** command.

  Workaround: Do not disable the PXF engine.

- CSCsd44362

  Symptoms: After a switchover has occurred, a watchdog timeout crash that occurs because of a CPUHOG condition may prevent the secondary RP from becoming the primary RP.

  Conditions: This symptom is observed on a Cisco 7304 when a few OIRs are performed before the switchover occurs. The router has an ATM line card on which a few PVCs are configured.

  Workaround: There is no workaround. However, after the watchdog timeout crash gas occurred, the secondary RP comes up as the primary RP.

- CSCsd45416

  Symptoms: An interface on a SPA-2GE-7304 or SPA-4FE-7304 may become stuck after a few HA switchovers have occurred.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsd56598

  Symptoms: When a switchover occurs, an interface remains down.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for SSO when the following events occur:

  1. You remove a port adapter or line card via an OIR.
  2. An SSO switchover occurs.
  3. You insert the port adapter or line card via an OIR.

  After these events, the interface remains down.

  Workaround: There is no workaround.

- CSCsd73865

  Symptoms: When you log off from a service, a router may generate the following error message and then crash:

  ```
  %SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
  [ADJ:TC:61470] - hardware platform error.
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG when you first change a locally defined service profile, then activate the service, and then log off from the service.

  After you have activated the service, the output of the **show subscriber session all** command indicates that the service has both previously applied profile features and currently applied profile features.

  Workaround: There is no workaround.

- CSCsd82072

  Symptoms: A CPUHOG error message and tracebacks may be generated on a Cisco 10000 series.

  Conditions: This symptom is observed when a 4-port channelized T3 half-height comes up with a large configuration.

  Workaround: There is no workaround.

- CSCsd98739

  Symptoms: The policer stops functioning when you remove classes for which no police action is configured and when these classes are defined before a class that does have a police action configured.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Remove and re-apply the service policy to the affected interfaces.

- CSCse11694

  Symptoms: When you bring up ISG sessions with the L4 Redirect feature under a high traffic load, translations may not be successfully created for all ISG sessions.

  Conditions: This symptom is observed on a Cisco router when you bring up more than 8000 ISG sessions and send IP packets at 4800 pps.

  Workaround: There is no workaround.

- CSCse16519

  Symptoms: A service policy is not applied to LAC sessions.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB and that functions as a LAC.

  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.

- CSCse26583

  Symptoms: When you enter the **shape average percent** *percentage* command to change a shaper policy with a shaper rate in bits per second (bps) to a shaper rate in percentage, the rate change is not reflected properly.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs with any type of policy (that is, with a single-level policy without a child policy or a two-level policy with a child policy attached to the parent policy and with a user-class or a class-default class).

  Workaround: Remove and re-attach the policy.

  Further Problem Description: The following changes in the shaper rate are not affected:

  - percentage to percentage
  - bps to bps
  - percentage to bps

- 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.

  Workaround: There is no workaround.

- CSCse28363

  Symptoms: A Cisco 10000 series may crash when you remove a POS interface.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **shutdown** interface configuration command an interface of a 1-port OC-12 POS line card.

  Workaround: There is no workaround.

- CSCse29953

  Symptoms: When a large number of PPPoE sessions come up on a Cisco 10000 series that functions as an LNS, some formerly established sessions may disconnect.

  Conditions: This symptom is observed on a Cisco 10000 series when the number of sessions approaches or exceeds 50,000 and when a keepalive value is set on the virtual template that is applied to the tunnel. This symptom occurs when the CPU usage is high while the PPPoE sessions are brought up.

  Workaround: Enter the **no keepalive** command on the virtual template that is applied to the tunnel.

  Further Problem Description: PPP keepalive timeouts cause the PPPoE sessions to disconnect because they time-out prematurely.

- CSCse30164

  Symptoms: The environment monitor checksum value in the IDPROM of a 4-port 10/100 Fast Ethernet SPA (SPA-4FE-7304) is incorrect.

  Conditions: This symptom is observed on a Cisco 7304 and is specific to the SPA-4FE-7304.

  Workaround: There is no workaround.

- CSCse34799

  Symptoms: Are router that processes Label Distribution Protocol (LDP) traffic for a sustained period of time may generate the following error messages and tracebacks, and the CPU usage may become high:

  ```
  %GENERAL-3-EREVENT: HWCEF: Failed to allocate HW mac rewrite
  -Traceback=

  %GENERAL-2-CRITEVENT: Bad RP 2 XCM address conversion
  -Traceback=
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for MPLS and LDP when continuous LDP link flapping occurs.

  Workaround: There is no workaround.

- CSCse37573

  Symptoms: The NPE-G100 in a Cisco 7304 crashes after the PA-CC has crashed.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S10 or Release 12.2SB and that is configured with a PA-CC in which an 8-port ATM IMA port adapter is installed.

  Workaround: There is no workaround.

- CSCse37614

  Symptoms: Qos preclassification on a GRE tunnel may not function.

  Conditions: This symptom is observed on a Cisco 7200 series and a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

- CSCse49552

  Symptoms: ATM ports may stop sending and receiving traffic when the ATM VCs are no longer synchronized between the Cisco IOS software and the ATM line card.

  Conditions: This symptom is observed on a Cisco 10000 series when an MTU change or a hold-queue length change cause the SAR of the ATM line card to reset.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, enter the no shutdown command on all ATM ports or reset the ATM line card by entering the **hw-module slot** *slot-number* **reset** command to enable the ATM VCs on multiple ports to synchronize properly between the Cisco IOS software and the ATM line card.

- CSCse54482

  Symptoms: A parser error and configuration synchronization error may occur when you enter a **banner** command that contains a carriage return. This situation causes the standby NSE-100 to fall back to RPR mode.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB or Release 12.2(28)SB1 and that has dual NSE-100 processors that function in SSO mode.

  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.

- CSCse62630

  Symptoms: When L2VPN circuits (that is, either AToM or L2TPv3 circuits) are configured for Ethernet interworking on an NSE-100, loss of connectivity may occur.

  Conditions: This symptom is observed on a Cisco 7304 and occurs only when there are more than 255 L2VPN circuits configured.

  Workaround: There is no workaround.

- CSCse73032

  Symptoms: Multicast routes fail, CEF routes fail, NAT translations fail, MPLS routes over an EtherChannel fail, or the router reloads unexpectedly.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100 processor that runs Cisco IOS 12.2(25)S or a rebuild of this release up to and including Release 12.2(25)S10. The symptoms occurs under stress conditions when NAT and multicast are used (but not necessarily for the same traffic flows).

In Release 12.2(28)SB or one of its rebuilds, the symptoms may occur when a Cisco 7304 that has an NSE-100 processor functions under stress conditions and when the following combinations of features are in use (but not necessarily for the same traffic flows):

- NAT and multicast
- MPLS over EtherChannel and large CEF tables
- Multicast and large CEF tables

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

- CSCse78349

  Symptoms: A Cisco 7304 that is configured for multicast may drop packets from its PXF engine.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NSE-100 and occurs when the router is at the transition of the sparse-mode and dense-mode regions and when the following events take place:

  1. A stream from the dense-mode side halts, causing the (s,g) entry to time out.
  2. The stream restarts before the corresponding (*,g) entry times out.

  This situation causes the packets to be dropped from the PXF engine and occurs because the output list interface for the (*,g) entry points toward the source in the dense-mode region.

  Workaround: Enter the **no ip mroute-cache** command on the input interface in dense mode.

- 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.

- CSCse85435

  Symptoms: A temporary loss of connectivity may occur on a 4-port channelized T3 half-height line card. The line card recovers automatically in 10 to 20 seconds for a small configuration, or potentially a longer time for very large configuration. For a small configuration without Frame Relay connections, the loss of connectivity may not even cause a line flap.

  Conditions: This symptom is observed on a Cisco 10000 series immediately after an SSO switchover has occurred. The symptom can occur with both a PRE-2 and a PRE-3.

  Workaround: There is no workaround.

- CSCse98421

  Symptoms: When a Cisco 7304 that functions in an MPLS environment as a P router receives MPLS traffic that is forwarded as pure IP traffic, the router may incorrectly apply an MPLS string rather than an IP string, causing the next PE router to drop packets that have a size larger than 1496 bytes.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that runs Cisco IOS Release 12.2(28)SB1 or Release 12.2(28)SB2, that has PXF enabled, and that has MPLS configured on the connecting interfaces.

  Workaround: Disable PXF, downgrade to Cisco IOS Release 12.2(25)S8, or disable MPLS. However, if none of these solutions is an option, there is no workaround.

Further Problem Description: The same symptom is observed irrespective of the FPGA microcode that is used. The connecting interfaces have the **mtu 1512** and **ip mtu 1500** commands enabled so the MPLS MTU is the same as the interface MTU and the IP MTU is a bit less than the interface MTU to accommodate for two labels.

- CSCsf03188

  Symptoms: A router crashes when you use TFTP to download a configuration to the running configuration and when the downloaded configuration clears the controllers.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsf08287

  Symptoms: After a PRE failover as occurred, the Multi-Router APS (MR-APS) state is mismatched between the active PRE and the standby PRE.

  Conditions: This symptom is observed on a Cisco 10000 series when the PREs function in SSO mode and when a 1-port OC-12 ATM line card or 4-port OC-3 ATM line card is connected to an ADM and is configured for MR-APS.

  Workaround: There is no workaround.

- CSCsf19377

  Symptoms: A Cisco 10000 series that is configured for MPLS AToM may crash.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround.

- CSCsf26075

  Symptoms: When a service policy with random-detect is attached to a physical interface, the logical subinterfaces may ignore the policy.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NSE-100. The physical interfaces that are affected are Ethernet and Frame Relay interfaces. For example, when there is an interface with two Frame Relay virtual circuits and a service policy with random-detect on the main interface, then none of the traffic that passes through the VCs is subjected to WRED.

  Workaround: There is no workaround.

- CSCsg06445

  Symptoms: A PRE-2 may crash because of an “Illegal Opcode” exception.

  Conditions: This symptom is observed rarely on a Cisco 10000 series that functions as an LNS that processes L2TP traffic.

  Workaround: There is no workaround.

- CSCsg07004

  Symptoms: IP header compression does not function. The output of the **show ip tcp header compression** command shows that no frames have been compressed.

  Conditions: This symptom is observed on a Cisco 7304 with an NPE-G100 when CEF is enabled on the interface on which header compression is also enabled.

  Workaround: Disable CEF on the interface on which header compression is enabled.

Wide-Area Networking

- CSCeg82698

  Symptoms: PPTP tunnels do not come up.

  Conditions: This symptom is observed when VPDN is configured.

  Workaround: There is no workaround.

- CSCek31721

  Symptoms: A router may not release the memory when sessions are freed. This situation may prevent PPP interfaces from coming up or initializing.

  Conditions: This symptom is observed on a Cisco router that is configured for HA when PPP interfaces flap.

  Workaround: There is no workaround.

- CSCek39651

  Symptoms: A TERMREQ packet that is sent from an LNS may not reach a PPP client, causing the PPP client connection to be disconnected because of a “missed keepalives” or “lower layer disconnected” message instead of a “peer disconnected” message.

  Conditions: This symptom is observed on a Cisco router that functions as an LNS when a PPP call that is forwarded over an L2TP or L2F VPDN tunnel is disconnected at the LNS.

  Workaround: There is no workaround.

- CSCek40618

  Symptoms: A router may crash by address error (load or instruction fetch) exception during normal operation.

  Conditions: This symptom has been observed when the router is configured with VPDN and Multilink PPP, using Virtual-Template interfaces.

  Workaround: There is no workaround.

- CSCsd01816

  Symptoms: Multilink interfaces do not recover after a T1 link in a bundle flaps.

  Conditions: This symptom is observed when two Cisco router are connected back-to-back via two channelized OC-3 connections with 168 T1 links and when the multilink bundles are created with two T1 links each.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected multilink interfaces.

- CSCsd44299

  Symptoms: Tracebacks may be generated when you change the MTU size of a bundle link on a physical serial interface. After you have reloaded or power-cycled the router, the tracebacks continue to be generated. The router crashes when you remove the **frame-relay fragment** *fragment-size* **end-to-end** command from the MFR interface.

  Conditions: These symptoms are observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB and occurs only for MFR interfaces that have interface-level FRF.12 fragmentation enabled.

  Workaround: Do not configure interface-level FRF.12 fragmentation. Rather, configure FRF.12 fragmentation in a map class with traffic shaping.

- CSCsd75377

  Symptoms: PPP links may not come up after an RPR+ switchover has occurred. You can compare the output of the **show ip interface brief | in up down** command before and after the RPR+ switchover to see which PPP interfaces are down.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for RPR+ but may also occur other platforms that are configured for RPR+.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interfaces.

- CSCse40960

  Symptoms: PPP keepalives may be processed at the process level (that is, in the slow path), and LCP negotiation may fail, causing links to flap repeatedly.

  Conditions: This symptom is observed on a Cisco 10000 series that has PPP keepalives enabled. However, the symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCse70647

  Symptoms: A router that functions as a BRAS or LNS crashes and generates one of the following error messages (or an error message that is similar to one of the following error messages):

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x607C0374
  ```

  or

  ```
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 206BCF18, data 21CD607D.
  -Process= "PPPoA Manager", ipl= 0, pid= 220
  ```

  or

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

  Conditions: This symptom is observed during PPP negotiations with a Microsoft PPP client that requests WINS or DNS data. Note that the symptom does not occur on a router that functions as a LAC.

  Workaround: There is no workaround. However, entering the **ppp max-failure 100** command may reduce the chances that the symptom occurs.

- CSCse81359

  Symptoms: After you have shut down a Frame Relay over MPLS (FRoMPLS) connection, the **xconnect** command is unexpectedly removed from the standby PRE, preventing the FRoMPLS connection from coming up after an HA switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: When you enter the **connect** command on the active PRE, also enter the **xconnect** command and any other configuration from the connect submode on the standby PRE to ensure that the complete configuration is retained on the standby PRE after an HA switchover has occurred.

- CSCse96387

  Symptoms: In a large scale Broadband Access Aggregation (BBA) environment, PPP negotiation may become stuck in a state in which one side is closed and the other side is constantly attempting to request options. This situation may cause all sessions to become stuck in a bad state that you must manually clear in order to recover from the state.

  Conditions: This symptom is observed on a Cisco router when a large volume of sessions comes up all at once as is common in an PPPoA BBA environment.

Workaround: If you think you are encountering this caveat, please contact Cisco Technical Support Services for assistance and possible configuration tuning to minimize the chance that the symptom occurs again.

Further Problem Description: If this is an option for your configuration, you can also reduce the rate of the incoming sessions to minimize the chance that the symptom occurs again.

- CSCse98867

  Symptoms: A router may reload when a multilink bundle goes down while packets are flowing.

  Conditions: This symptom is observed on a router that is configured for Multilink PPP (MLP) with hardware compression.

  Workaround: There is no workaround.

- CSCsf98296

  Symptoms: PPP keepalives fail because there are an extra 4 bytes added to an LCP echo reply.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBB or Release 12.2(28)SB. The symptom occurs when the Cisco router is connected to certain third-party vendor routers that strictly validate the received echo replies; the Cisco router adds an extra 4 bytes to the echo replies, causing them to be ignored by the third-party vendor routers.

  Workaround: Disable keepalives on the third-party vendor routers. If this is not an option, there is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(28)SB4

Cisco IOS Release 12.2(28)SB4 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB4 but may be open in previous Cisco IOS releases.

EXEC and Configuration Parser

- CSCsd72511

  Symptoms: When TACACS+ command accounting is enabled, SNMPv3 community strings may not be encrypted.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2.(25)SEE. The symptom also affects other releases.

  Workaround: There is no workaround.

Miscellaneous

- CSCek51309

  Symptoms: A router may reload when a QoS policy is attached to a number of PPPoL2TP sessions on an LNS and when the physical link or sessions are flapping. The QoS policy contains a shaping and queuing configuration.

  Conditions: This symptom is observed on a Cisco router that functions as an LNS when there are many route changes, either because a physical interface flaps or because the PPPoL2TP sessions flap.

  Workaround: There is no workaround.

Further Problem Description: The symptoms are specific to L2TP sessions and queuing features in the policy map.

- CSCse71784

  Symptoms: When you configure an IP address as the tunnel source and the tunnel interface has been disconnected, shut down, or reconfigured, the tunnel interface line protocol can no longer come up.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S or Release 12.2SB.

  Workaround: Do not configure an IP address as the tunnel source. Rather, at both ends of the tunnel, configure the source interface or the interface name as the tunnel source.

Wide-Area Networking

- CSCse70647

  Symptoms: A router that functions as a BRAS or LNS crashes and generates one of the following error messages (or an error message that is similar to one of the following error messages):

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x607C0374
  ```

  or

  ```
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 206BCF18, data 21CD607D.
  -Process= "PPPoA Manager", ipl= 0, pid= 220
  ```

  or

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

  Conditions: This symptom is observed during PPP negotiations with a Microsoft PPP client that requests WINS or DNS data. Note that the symptom does not occur on a router that functions as a LAC.

  Workaround: There is no workaround. However, entering the **ppp max-failure 100** command may reduce the chances that the symptom occurs.

- CSCse96387

  Symptoms: In a large scale Broadband Access Aggregation (BBA) environment, PPP negotiation may become stuck in a state in which one side is closed and the other side is constantly attempting to request options. This situation may cause all sessions to become stuck in a bad state that you must manually clear in order to recover from the state.

  Conditions: This symptom is observed on a Cisco router when a large volume of sessions comes up all at once as is common in an PPPoA BBA environment.

  Workaround: If you think you are encountering this caveat, please contact Cisco Technical Support Services for assistance and possible configuration tuning to minimize the chance that the symptom occurs again.

  Further Problem Description: If this is an option for your configuration, you can also reduce the rate of the incoming sessions to minimize the chance that the symptom occurs again.

- CSCsf06190

  Symptoms: Some PPP sessions do not properly synchronize to the standby RP.

  Conditions: This symptom is observed on a Cisco router that is configured for HA when many PPP interfaces flap at the same time.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(28)SB3

Cisco IOS Release 12.2(28)SB3 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB3 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 contains the fix for caveat CSCeh31423. See the information in the Bug Toolkit:

  http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh31423

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeh83666

  Symptoms: A router may crash or fail to allocate a port.

  Conditions: This symptom is observed on a Cisco router that is configured for NAT Overload and occurs because the “prev_block” pointer may be dereferenced when it is NULL.

  Workaround: There is no workaround.

Miscellaneous

- CSCsb72921

  Symptoms: A QoS policy map that includes the **priority** and **police** commands in the same class may be rejected.

  Conditions: This symptom is observed on a Cisco router when you migrate from Cisco IOS Release 12.2S to either Release 12.2SB or Release 12.2SBC.

  Workaround: Edit the policy manually; enter the **police** command before you enter the **priority** command, and save the configuration.

  Further Problem Description: The symptom occurs because the bandwidth allocations are checked while the policy is being configured. In earlier Cisco IOS releases such as Release 12.2(25)S, the bandwidth allocations are checked only when the complete policy is attached to the interface. Because the **police** command provides the bandwidth limit for the **priority** command in this configuration, you must enter the **police** command before you enter the **priority** command.

- CSCsd44856

  Symptoms: A Cisco 10000 series crashes when you unconfigure MLP.

  Conditions: This symptom is observed when you first remove the controller and then remove a member of a bundle that belongs to the controller.

  Workaround: First remove all the bundles from the controller before you remove the controller.

- CSCsd80857

  Symptoms: An LFIB entry in the PXF engine may become corrupted, preventing from forwarding traffic.

  Conditions: This symptom is observed on a Cisco 10000 series when first a VRF is removed and then a link flap occurs.

  Workaround: Clear the affected route.

- CSCse25130

  Symptoms: IPCP renegotiations of an MLP interface may time out during renegotiation after an MR-APS failure has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in an MR-APS configuration with another Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse39760

  Symptoms: A PA-CC does not recover when you perform a soft or hard OIR of the standby RP.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with dual RPs after a switchover has occurred that causes the standby RP to become the active RP. In this situation, when you perform a soft or hard OIR of the standby RP, the PA-CC does not recover because the PA-CC fails to initialize.

  Workaround: There is no workaround.

- CSCse47922

  Symptoms: WRED random drops that occur in different ToS and DSCP classes do not correlate with the configured thresholds as you would expect.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCse61834

  Symptoms: When you modify an ATM PVC by entering the **pvc** *vpi/vci* command, any subsequent modifications in the VC class that is assigned to this PVC do not take effect.

  Conditions: This symptom is observed when the PVC is preconfigured with a VC class when the following events occur:

  1. You make a configuration change in the PVC.
  2. You change the configuration in the VC class.

  The configuration change in the VC class does not take effect.

  Workaround: First complete the configuration changes in the VC class. Then, change the configuration in the PVC.

Resolved Caveats—Cisco IOS Release 12.2(28)SB2

Cisco IOS Release 12.2(28)SB2 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB2 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeg63395

  Symptoms: A large latency may occur when packets are forwarded by a router.

  Conditions: This symptom is observed on a Cisco router when a DoS attack is launched from another router towards a POS interface of the Cisco router.

  Workaround: There is no workaround. Although the symptom causes performance degradation, it does not cause loss of functionality.

- 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.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

- CSCsd27777

  Symptoms: When you enter the **clear subscriber session all** command while traffic is being processed, the CPU usage of the router increases to 99 percent and sessions go down gradually. At the same time, the router automatically reinitiates sessions, and "%SSSMGR-3-MEMORY_LOW" and "%IDMGR-3-INVALID_ID:" error messages are generated. Eventually, the router generates "%TCP-6-NOBUFF:" and "%SYS-2-MALLOCFAIL" errors messages, and either resets all its interfaces or reloads.

  Conditions: This symptom is observed on a Cisco 10000 series that runs 16,000 PTA sessions with ISG features and 16,000 plain L2TP sessions. On all sessions, stateless traffic is being processed. The symptom is not specific to a Cisco 10000 series and may occur on other platforms that function in a similar configuration.

  Workaround: Do not clear all sessions at once via the **clear subscriber session all** command.

- CSCse11615

  Symptoms: When you enter the **enable** privileged EXEC command, an "Access Denied" message is generated.

Conditions: This symptom is observed on a Cisco router when you have configured AAA authentication and when the **enable password** global configuration command is configured.

Workaround: Configure the password for the **enable password** global configuration command to be no more than two characters.

Alternate Workaround: Remove the **enable password** global configuration command from the startup configuration.

Miscellaneous

- CSCef82084

  Symptoms: Spurious memory accesses occur on a Cisco 7200 series and ALIGN-3-SPURIOUS error messages are generated.

  Conditions: This symptom is observed on a Cisco 7200 series that processes traffic through a serial interface.

  Workaround: There is no workaround.

- CSCeh40183

  Symptoms: A router reloads unexpectedly when the **show policy interface** EXEC command is entered.

  Conditions: This symptom is observed on a Cisco router when two users are connected to the router and simultaneously enter the **show policy interface** EXEC command.

  Workaround: Ensure that only one user at a time enters the command.

- CSCei27448

  Symptoms: A router may crash while displaying the output of the **show ip pim mdt bgp** command.

  Conditions: This symptom is observed when withdraws for a MDT source group are received by PIM from BGP while you enter the **show ip pim mdt bgp** command.

  Workaround: There is no workaround. To reduce the chance of the router crashing, change the *screen-length* argument in the **terminal length** *screen-length* command to 0. Doing so prevents the router from pausing between multiple output screens. (The default of the *screen-length* argument is 24.)

- 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.

- CSCek20952

  Symptoms: The following error message may be generated when you configure a police statement in a policy map:

  ```
  Maximum rate for the policer is 0, conform action is drop
  ```

  Conditions: This symptom is observed on a Cisco router that functions in a L2VPN configuration with QoS features.

  Workaround: There is no workaround.

- CSCek25822

  Symptoms: A PRE crashes when you enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs whether or not the router processes traffic.

  Workaround: Do not enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Further Documentation: The above-mentioned configuration is not supported on the Cisco 10000 series.

- CSCek30152

  Symptoms: When a T3/E3 Serial SPA is configured in Kentrox mode with a small bandwidth between 22 kbps and 250 kbps, either in T3 or E3 mode, the firmware miscalculates the bandwidth allocation and allows up to 24M of traffic to pass through.

  Conditions: This symptom is observed on a Cisco 7304 and a Cisco 12000 series.

  Workaround: Do not configure such a small bandwidth when the T3/E3 Serial SPA is configured in Kentrox mode. The minimal bandwidth on a T3/E3 Serial SPA that is configured in Kentrox mode is either 1500 kbps in T3 mode or 1000 kbps in E3 mode.

- CSCek35146

  Symptoms: When you remove and re-insert an MSC-100 card in which one or two SPAs are installed, the SPAs may become disabled for 10 to 12 minutes, after which they recover automatically.

  Conditions: This symptom is observed on a Cisco 7304 when you perform either a physical OIR or a soft-OIR by entering the **hw-module slot** *slot-number* **stop** command followed by the **hw-module slot** *slot-number* **start** command. The symptom occurs only when the time between the removal and the re-insertion is 2 to 3 seconds.

  Workaround: Do not re-insert the MSC-100 card too quickly after you have removed it. Wait at least 10 seconds before you re-insert the card.

- CSCek37011

  Symptoms: A line card may crash when you attempt to remove the child policy from the HQoS parent.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the line card has an interface that is configured as follows:

  - The interface faces the MPLS core.
  - The interface has an HQoS policy with a child policy.
  - The HQoS policy has a classification that is based on the MPLS EXP bits.

  Workaround: There is no workaround.

- CSCek39877

  Symptoms: A 4-port OC-3 ATM line card may not perform an APS switchover when a signal degrade (SD) or signal fail (SF) condition is present.

  Conditions: This symptom is observed on a Cisco 10000 series when bit errors occur on the on the 4-port OC-3 ATM line card.

  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.

- CSCin96524

  Symptoms: Control plane traffic may be dropped from a multilink interface.

  Conditions: This symptom is observed only when the multilink interface is oversubscribed and does not occur under normal traffic conditions.

  Workaround: Reduce the traffic rate.

  Alternate Workaround: Apply some type of queueing mechanism on the interface.

- CSCin97726

  Symptoms: On a Cisco 7500 router, the console of the active RSP may hang.

  Conditions: This symptom is observed when the router functions in RPR mode and when you attempt to access the standby RSP file system from the console of the active RSP, for example, by entering the **write memory** command or the **dir slavedisk0:** command.

  Note that the symptom is not specific to the Cisco 7500 series and may also occur on other platforms.

  Workaround: There is no workaround.

  Further Problem Description: Normal operation of the router is not affected, but the console becomes inaccessible.

- CSCsb01043

  Symptoms: When a Turbo ACL classification table grows beyond a certain size, a memory allocation failure may occur or the router may crash.

  If the router runs Cisco IOS Release 12.1E or 12.3, memory corruption may occur, causing the router to crash. If the router runs Cisco IOS Release 12.2S, an error message similar to the following may appear during a Turbo ACL compilation, the compilation will fail, and a recompilation is forced:

  ```
  %SYS-2-CHUNKBADELESIZE: Chunk element size is more than 64k for TACL Block -Process=
  "TurboACL", ipl= 0, pid= 82
  ```

  These symptoms do not occur because of an out-of-memory condition.

  Conditions: This symptom is observed on a Cisco router that is configured for Turbo ACL. The Cisco 10000 series is not affected.

  Workaround: Monitor the output of the **show access-lists compiled** command and force the Turbo ACL tables to be cleared if a table is at risk of growing large enough to trigger the symptoms.

  The tables that have significant sizes are the first and third tables shown next to "L1:" and the first table shown next to "L2:". When the number after the slash for one of these tables is greater than 16384 for the "L1" tables or greater than 32768 for the "L2" table, the table is already too large and the symptom may occur any moment.

When the number is in the range from 10924 to 16384 inclusive for the "L1" tables or the range from 21846 to 32768 inclusive for the "L2" tables, the table size will be too large on the next expansion. An expansion occurs when the number to the left of the slash reaches 90 percent of the value to the right of the slash. When the value to the left of the slash approaches 90 percent of the value to the right, enter the **no access-list compiled** command followed by the **access-list compiled** command to disable and re-enable Turbo ACL. Doing so causes the tables to be cleared and, therefore, delay the expansion. This workaround may be impractical when there is a high rate of incoming packets and when entries are added frequently to the tables.

Alternative Workaround: Disable Turbo ACL by entering the **no access-list compiled** command.

Note that neither of these workarounds are supported on a Cisco 7304 that is configured with an NSE-100: there is no workaround for this platform.

- CSCsb13836

  Symptoms: A Cisco 7304 may crash because of a bus error during normal operation when a external flash card is present.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2(20)S4 or Release 12.2(20)S8. The symptom may also occur in other releases.

  Workaround: Do not use an external flash card. Rather, use an internal flash card.

- CSCsb33258

  Symptoms: An RP crashes during BGP convergence when MVPNs are configured.

  Conditions: This symptom is observed on a Cisco router after a duplicate BGP MDT extended community message is received that specifies a different Route Descriptor (RD) for an MDT that already exists for the specified MDT source and group address.

  Workaround: There is no workaround.

- CSCsb64858

  Symptoms: A switch or router may crash while processing a longest match lookup in the CEF table.

  Conditions: This symptom is observed on a Cisco platform when a packet is punted because of an exception such as the occurrence of an ICMP redirect message while a longest match lookup is performed in the CEF table.

  Workaround: Disable ICMP redirect messages by entering the **no ip redirects** interface configuration command on all interfaces of the router.

- CSCsb83990

  Symptoms: All on-demand VCs may become stuck in the inactive state because of insufficient bandwidth on one ATM interface.

  Conditions: This symptom is observed on a Cisco 10000 series when the creation of a VC fails because there are no more VCCIs, a line card failure occurs, or a toaster failure occurs. Each of these situations cause the ATM bandwidth to be depleted, and, in turn, prevent bandwidth from being available for any other ATM subinterfaces.

  Workaround: There is no workaround.

- CSCsc08491

  Symptoms: A virtual-access subinterface may not forward any traffic.

  Conditions: This symptom is observed on a Cisco router with a virtual-access application that causes virtual-access subinterface to be created.

  Workaround: There is no workaround.

- CSCsc37472

  Symptoms: The output rate counters for a member link of a multilink interface do not increment when you look at the output of the **show interfaces** command.

  Conditions: This symptom is observed on a Cisco 10000 series when packets are properly delivered through the member link of the multilink interface.

  Workaround: Look at the PXF counters in the output of the **show pxf cpu queue multilink** *interface* or **show pxf cpu subblock multilink** *interface* commands.

- 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.

- CSCsc86262

  Symptoms: When you configure OAM on an ATM subinterface in an AToM configuration, the ATM subinterface goes down.

  Conditions: This symptom is observed on a Cisco 7304 that has a NSE-100 and that functions as a PE router in an MPLS backbone.

  Workaround: There is no workaround. Note that the symptom does not occur when you disable the PXF engine.

- CSCsc90843

  Symptoms: A router that is configured with a multilink bundle may reload unexpectedly with the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions: This symptom is observed on a Cisco router when you attempt to remove a service policy from a multilink interface.

  Workaround: There is no workaround.

- CSCsd00354

  Symptoms: The output of the **show policy-map interface** command shows the output queue packets and bytes counters as zero.

  Conditions: This symptom is observed on a Cisco 10000 series on queues for which a policer is applied.

  Workaround: Use the policer's counters in the output of the **show policy-map interface** command to determine the number of forwarded and dropped packets and bytes for the queue.

- CSCsd14277

  Symptoms: A ping does not pass through a Fast Ethernet interface that functions in AToM port mode.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that has the **xconnect** interface configuration command enabled on the interface of a 1-port Fast Ethernet port adapter (PA-FE) that is installed in a port adapter carrier card (7300-CC-PA).

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

Alternate Workaround: Enter the **shutdown** interface configuration command, the **xconnect** interface configuration command, and then the **no shutdown** interface configuration command on the affected interface.

- CSCsd25699

  Symptoms: MLP traffic fails during a PRE failover of the protect router.

  Conditions: This symptom is observed on a Cisco 10000 series when a PRE failover occurs on the protect router because of an MR-APS cable break failover from the protect router to the working router.

  Workaround: If the active controller is brought up after the MR-APS failover, manually reverse APS.

- CSCsd35958

  Symptoms: A Cisco 7304 that is configured with an NPE-G100 processor and ATM VCs may reload unexpectedly.

  Conditions: This symptom is observed when a hierarchical policy on an ATM VC has the **shape average** command enabled.

  Workaround: Do not use a hierarchical policy on an ATM VC.

- CSCsd44475

  Symptoms: A ping may fail when packets pass from an MPLS VPN into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that functions as a PE router, and that is connect to the MPLS core via a serial interface.

  Possible Workaround: Do not use a serial interface to connect the PE router to the MPLS core. Rather, use another type of interface.

  Further Problem Description: The symptom occurs because the tunnel adjacency is not complete in the PXF engine, preventing packets from being correctly punted and the adjacency from becoming complete.

- CSCsd49072

  Symptoms: The output of the **show policy-map interface** command shows incorrect statistics for a DSCP-based WRED policy. Also, when the class-map parameters are dynamically changed, the WRED statistics are lost.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsd49196

  Symptoms: After you have configured ingress NetFlow on an interface, the output of the **show ip cache verbose flow** command may show incorrect values in the “Active” seconds column.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S9, Release 12.2(20)S10, or Release 12.2(25)S8 when the **ip flow ingress** command is configured on an interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsd58203

  Symptoms: The output of the **show ip cache flow** command, may shows some flows with a size of 4294M, which is the maximum size that can fit in a 32-bit value (2^32). Note that you can view the flows more easily in the output of the **show ip cache flow | i M|Pkts** command.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(25)S7. The symptom may occur in other releases.

Workaround: There is no workaround.

Further Problem Description: The symptom is of a cosmetic nature. Proper operation of the router is not affected.

- CSCsd62942

  Symptoms: The PXF engine on a Cisco 7304 that functions as a PE router may crash when traffic passes from the MPLS core to a CE router.

  Conditions: This symptom is observed when the traffic from the MPLS core is de-aggregated on the PE router into CE-facing interfaces that are configured into a VRF and that perform IP load-sharing and occurs while the PXF engine is active on the PE router.

  Workaround: Disable IP-load-sharing on any interfaces that are configured into a VRF, such as the CE-facing interfaces.

  Alternate Workaround: Disable PXF packet-processing on the PE router.

- 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:

a. 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

b. 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*

c. Apply the service policy (“my-class-default”) to the dot1q subinterface.

- CSCsd68659

  Symptoms: When you change the **atm dsx3mode** command for the framing of one port of a 8-port E3/DS3 ATM line card (ESR-8E3/DS3-ATM), all ports on the line card are affected.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsd69402

  Symptoms: Pre-classification on a GRE tunnel does not function.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 processor.

  Workaround: There is no workaround.

- CSCsd71131

  Symptoms: A service policy may be suspended when you enter the **clear interface** command for a multilink interface that has six members.

  Conditions: This symptom is observed on a Cisco router that is configured for dLFIoLL and QoS.

  Workaround: There is no workaround.

- CSCsd76528

  This caveat consists of two symptoms, two conditions, and two workarounds:

  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.

  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.

- CSCsd83503

  Symptoms: NetFlow updates only MPLS-related egress records but not IPv4 ingress records.

  Symptoms: This symptom is observed on a Cisco 10000 series that has an PRE-2 and that has the **ip route-cache flow** command enabled on its main ATM and GE interfaces and the **mpls netflow egress** command enabled on its ATM subinterfaces (on which PVCs are configured) and GE subinterfaces.

  Note that the **ip route-cache flow** command is automatically converted into the **ip flow ingress** command and the **mpls netflow egress** command is automatically converted into the **ip flow egress** command, and these commands are stored in NVRAM. The symptom occurs after you have reloaded the PRE-2.

  Workaround: Disable and re-enable the **ip flow ingress** command on the main interfaces.

- CSCsd88288

  Symptoms: Packet loss may occur on a GRE tunnel on which CEF is enabled.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs the c7300-js-mz image of Cisco IOS Release 12.2(25)S8. The symptom may also occur in Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: Disable PXF on the Cisco 7304. If this is not an option, there is no workaround.

- CSCsd91238

  Symptoms: The success rate of pings decreases when you increase the packet size of the pings, and the output of the **show ip traffic** command shows increasing ICMP checksum errors.

  Conditions: This symptom is observed on a Cisco 7304 that has a an NSE-100, that runs Cisco IOS Release 12.2(28)SB, and that is configured with a 2-port OC-3 ATM line card (7300-2OC3ATM-SMI) when MLP and VRF are enabled on a virtual template that automatically configures the ATM PVC bundle on the line card.

  Workaround: Disable VRF forwarding on the virtual template.

  Alternate Workaround: Disable PPP on the ATM PVC bundle.

- CSCsd93728

  Symptoms: A router that functions as an LNS may crash while processing traffic over L2TP connections, and the following error message is generated:

  ```
  Cause 00000010 (Code 0x4): Address Error (load or instruction fetch) exception
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(28)SB and that is configured for QoS. The symptom occurs during normal operation.

  Workaround: There is no workaround.

- CSCsd98928

  Symptoms: A router may crash when you enter the **show policy-map interface** command while an automated script completes the policy map and then removes the policy map during cleanup.

  Conditions: This symptom is observed on a Cisco router when you enter the **show policy-map interface** command while, at the same time, the automated script removes the policy map.

  Workaround: There is no workaround.

- CSCse00469

  Symptoms: When you boot the router, the SuperACL process causes a high CPU usage for an extended time, and not all configured policy maps are compiled.

Conditions: This symptom is observed on a Cisco 10000 series when there are hundreds (or more) policy maps in the configuration.

Workaround: Reduce the number of policy maps. If this is not an option, there is no workaround.

- CSCse00609

  Symptoms: Serial interfaces go down after an RP switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that has serial interfaces configured on either a channelized OC-3 or channelized OC-12 line card.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred. Bring the serial interfaces back up by resetting the line card.

- CSCse01030

  Symptoms: When an ATM interface has a QoS policy, locally generated traffic such as OSPF DPP traffic may not be transmitted.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCse06387

  Symptoms: A Cisco 7304 may reload unexpectedly after two HA switchovers have occurred.

  Conditions: This symptom is observed when 4000 virtual circuits are configured on the router.

  Workaround: There is no workaround.

- CSCse20029

  Symptoms: A router that is configured for MPLS and NetFlow may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco router that has the **vpdn enable** and **ip vrf** commands enabled.

  Workaround: There is no workaround.

- CSCse51608

  Symptoms: When you enter the **xconnect** command, the command is not accepted.

  Conditions: This symptom is observed on a Cisco 7200 series, irrespective of which interface the command is entered for.

  Workaround: There is no workaround.

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml.

TCP/IP Host-Mode Services

- CSCek01499

  Symptoms: When a CE router that is configured for MPLS reloads, a software-forced crash may occur on the connected PE router because of memory corruption.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has two RPs that function in SSO mode. The symptom does not occur when the router has only a single RP.

  Workaround: There is no workaround.

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml.

Wide-Area Networking

- CSCeh58376

  Symptoms: A serial interface on a channelized port adapter may stop forwarding traffic through the router but traffic to and from the router over the interface may still go through. The Tx accumulator "value" counter in the output of the **show controllers cbus** Exec command does not exceed the value 2, as is shown in the following example:

  ```
  Router#sh controllers cbus | include Serial5/1/0.1/2/6/2:0
  Serial5/1/0.1/2/6/2:0, txq E8001B40, txacc E8000412 (value 2), txlimit 26
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S when QoS is configured on at least one interface on the VIP in which the channelized port adapter is installed. The symptom occurs after the affected interface has flapped very frequently because of OSI layer 1 errors. The symptom may also occur in other releases.

  Workaround: Remove and reconfigure the controller of the affected interface.

- CSCek24091

  Symptoms: A PPP session fails to come up, and the following debug message is generated:

  ```
  PPP SSS: stale named authen method list "default"
  ```

  Conditions: This symptom is observed only when a service policy is applied and when the default PPP authentication method list is used.

  Workaround: Use a PPP authentication method list other than the PPP authentication default method list.

- CSCek32043

  Symptoms: cRTP may become disabled on an interface when you disable and re-enable the **ip rtp header-compression** command on the interface.

  Conditions: This symptom is observed on a Cisco router that functions in an MLP configuration when the link (such as a Frame Relay link) and the MLP bundle clone from the same virtual template.

  Workaround: Reset the interface.

- CSCsc28120

  Symptoms: A Cisco 7301 may crash when a service policy is removed from an interface that is configured for Frame Relay encapsulation.

  Conditions: This symptom is observed when a service policy is configured on an interface before the encapsulation is changed to Frame Relay. When the service policy is then removed, the router crashes.

  Workaround: Remove the service policy before you change the encapsulation to Frame Relay.

- CSCsd71360

  Symptoms: PPP Multilink fragment loss occurs as the result of premature lost fragment timeouts. This can be seen in the lost fragment count in the output of the **show ppp multilink** command, as well as debug traces produced by the **debug ppp multilink events** command.

  Conditions: This symptom has been observed with Cisco IOS Release 12.2(28)SB and Release 12.4(6)T, but not with Cisco IOS Release 12.2(27)SBC2 or Release 12.4(4)T.

  Workaround: Configure the **ppp timeout multilink lost-fragment 1** command under the Multilink interface or the Virtual-Template interface corresponding to the multilink bundle.

Resolved Caveats—Cisco IOS Release 12.2(28)SB1

Cisco IOS Release 12.2(28)SB1 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB1 but may be open in previous Cisco IOS releases. Cisco IOS Release 12.2(28)SB1 support the Cisco 7304 only.

IP Routing Protocols

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml.

Miscellaneous

- CSCek35146

  Symptoms: When you remove and re-insert an MSC-100 card in which one or two SPAs are installed, the SPAs may become disabled for 10 to 12 minutes, after which they recover automatically.

  Conditions: This symptom is observed on a Cisco 7304 when you perform either a physical OIR or a soft-OIR by entering the **hw-module slot** *slot-number* **stop** command followed by the **hw-module slot** *slot-number* **start** command. The symptom occurs only when the time between the removal and the re-insertion is 2 to 3 seconds.

  Workaround: Do not re-insert the MSC-100 card too quickly after you have removed it. Wait at least 10 seconds before you re-insert the card.

- CSCsb13836

  Symptoms: A Cisco 7304 may crash because of a bus error during normal operation when a external flash card is present.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2(20)S4 or Release 12.2(20)S8. The symptom may also occur in other releases.

  Workaround: Do not use an external flash card. Rather, use an internal flash card.

- CSCsc86262

  Symptoms: When you configure OAM on an ATM subinterface in an AToM configuration, the ATM subinterface goes down.

  Conditions: This symptom is observed on a Cisco 7304 that has a NSE-100 and that functions as a PE router in an MPLS backbone.

  Workaround: There is no workaround. Note that the symptom does not occur when you disable the PXF engine.

- CSCsd44475

  Symptoms: A ping may fail when packets pass from an MPLS VPN into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that functions as a PE router, and that is connect to the MPLS core via a serial interface.

  Possible Workaround: Do not use a serial interface to connect the PE router to the MPLS core. Rather, use another type of interface.

  Further Problem Description: The symptom occurs because the tunnel adjacency is not complete in the PXF engine, preventing packets from being correctly punted and the adjacency from becoming complete.

- CSCsd49072

  Symptoms: The output of the **show policy-map interface** command shows incorrect statistics for a DSCP-based WRED policy. Also, when the class-map parameters are dynamically changed, the WRED statistics are lost.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsd49196

  Symptoms: After you have configured ingress NetFlow on an interface, the output of the **show ip cache verbose flow** command may show incorrect values in the “Active” seconds column.

Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S9, Release 12.2(20)S10, or Release 12.2(25)S8 when the **ip flow ingress** command is configured on an interface. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCsd58203

  Symptoms: The output of the **show ip cache flow** command, may shows some flows with a size of 4294M, which is the maximum size that can fit in a 32-bit value (2^32). Note that you can view the flows more easily in the output of the **show ip cache flow | i M|Pkts** command.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(25)S7. The symptom may occur in other releases.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is of a cosmetic nature. Proper operation of the router is not affected.

- CSCsd62942

  Symptoms: The PXF engine on a Cisco 7304 that functions as a PE router may crash when traffic passes from the MPLS core to a CE router.

  Conditions: This symptom is observed when the traffic from the MPLS core is de-aggregated on the PE router into CE-facing interfaces that are configured into a VRF and that perform IP load-sharing and occurs while the PXF engine is active on the PE router.

  Workaround: Disable IP-load-sharing on any interfaces that are configured into a VRF, such as the CE-facing interfaces.

  Alternate Workaround: Disable PXF packet-processing on the PE router.

- CSCsd69402

  Symptoms: Pre-classification on a GRE tunnel does not function.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 processor.

  Workaround: There is no workaround.

- CSCsd88288

  Symptoms: Packet loss may occur on a GRE tunnel on which CEF is enabled.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs the c7300-js-mz image of Cisco IOS Release 12.2(25)S8. The symptom may also occur in Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: Disable PXF on the Cisco 7304. If this is not an option, there is no workaround.

- CSCsd91238

  Symptoms: The success rate of pings decreases when you increase the packet size of the pings, and the output of the **show ip traffic** command shows increasing ICMP checksum errors.

  Conditions: This symptom is observed on a Cisco 7304 that has a an NSE-100, that runs Cisco IOS Release 12.2(28)SB, and that is configured with a 2-port OC-3 ATM line card (7300-2OC3ATM-SMI) when MLP and VRF are enabled on a virtual template that automatically configures the ATM PVC bundle on the line card.

  Workaround: Disable VRF forwarding on the virtual template.

  Alternate Workaround: Disable PPP on the ATM PVC bundle.

- CSCse01030

  Symptoms: When an ATM interface has a QoS policy, locally generated traffic such as OSPF DPP traffic may not be transmitted.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCse06387

  Symptoms: A Cisco 7304 may reload unexpectedly after two HA switchovers have occurred.

  Conditions: This symptom is observed when 4000 virtual circuits are configured on the router.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(28)SB

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(28)SB. All the caveats listed in this section are open in Cisco IOS Release 12.2(28)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsc17888

  Symptoms: FRoMPLS traffic does not pass through the first port of an 8-port multichannel T1/E1 8PRI (PA-MC-8TE1+).

  Conditions: This symptom is observed on a Cisco router that functions as a CE router in an AToM environment when the ports of the PA-MC-8TE1+ are configured for E1. Note that the symptom does not occur for IP traffic and L3 traffic on the first port of the PA-MC-8TE1+, nor for the remaining seven E1 ports.

  Workaround: There is no workaround.

- CSCsd27777

  Symptoms: When you enter the **clear subscriber session all** command while traffic is being processed, the CPU usage of the router increases to 99 percent and sessions go down gradually. At the same time, the router automatically reinitiates sessions, and "%SSSMGR-3-MEMORY_LOW" and "%IDMGR-3-INVALID_ID:" error messages are generated. Eventually, the router generates "%TCP-6-NOBUFF:" and "%SYS-2-MALLOCFAIL" errors messages, and either resets all its interfaces or reloads.

  Conditions: This symptom is observed on a Cisco 10000 series that runs 16,000 PTA sessions with ISG features and 16,000 plain L2TP sessions. On all sessions, stateless traffic is being processed. The symptom is not specific to a Cisco 10000 series and may occur on other platforms that function in a similar configuration.

  Workaround: Do not clear all sessions at once via the **clear subscriber session all** command.

- CSCsd38237

  Symptoms: The active RP or PRE may reload in the "db_record_set_field" function when the router runs out of memory resources.

Conditions: This symptom is observed on a Cisco router that is configured with many sessions and occurs because the ID manager cannot not enqueue the “db_field” to the “db_record” when the router runs out of memory resources.

Workaround: Limit the number of sessions on the router to ensure that there are sufficient memory resources.

IP Routing Protocols

- CSCeh91717

  Symptoms: When IPv4 routes are imported into a VRF, the routes in the VRF CEF table are marked as “unusable” and “no label”.

  Conditions: This symptom is observed on a Cisco router when the “BGP Support for IP Prefix Import from a Global Table into a VRF Table” feature is enabled and when you enter the **import ipv4 unicast** command under a VRF.

  Workaround: There is no workaround.

- CSCej72829

  Symptoms: Some BGP SSO peers become disabled.

  Conditions: This symptom is observed after an SSO switchover occurs on a Cisco router.

  Workaround: There is no workaround. Note that after five minutes the BGP SSO peers are automatically re-enabled.

- CSCsc37461

  Symptoms: A PE router that functions in an MPLS VPN configuration may take a long time to converge.

  Conditions: This symptom is observed when an interface goes down and when an MP-BGP next hop that points to this interface is no longer reachable. This MP-BGP next hop remains unreachable until the Interior Gateway Protocol (IGP) finds an alternate path. If the BGP scanner runs while the MP-BGP next hop is unreachable, VRF routes that use this MP-BGP next hop may be removed from the VRF routing table. However, usually, when the next BGP scanner runs, these VRF routes are updated and then re-imported into VRF routing table.

  Workaround: The probability for the symptom to occur depends on the elapse time between the interface going down and the IGP convergence and can be decreases by tuning the IGP parameters for a faster convergence.

- CSCsd17747

  Symptoms: When you enter the **ip pim vrf register-source** command on an interface and then delete the interface or its IP address, the command remains in the configuration. This situation causes the bulk synchronization to fail and the standby RP to reset continuously after an RP switchover has occurred. Then, because the register source (the interface) cannot be found, a BEM failure occurs.

  Conditions: These symptoms are observed when the interface forwards traffic from a nondefault VRF and when the interface has a register source configured.

  Workaround: Remove the **ip pim vrf register-source** command from the interface before you delete the interface or its IP address.

Miscellaneous

- CSCef47220

  Symptoms: A path trace buffer value may be displayed as UNSTABLE in the output of the **show controllers** command when you enter this command for an AU-3 port and look for the overhead bytes.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 4-port channelized OC-3 line card with an E1 interface that is configured for AU-3. The E1 interface has the **overhead j1 length 16 transmit-message** *string* command enabled.

  Workaround: There is no workaround.

- CSCef47280

  Symptoms: A T1 interface that is configured for AU-4 mapping on a 4-port channelized OC-3 line card does not come up.

  Conditions: This symptom is observed on a Cisco 10000 series when the T1 interface interoperates with a third-party vendor test analyzer device.

  Workaround: There is no workaround.

- CSCeg11769

  Symptoms: When class-based weighted fair queueing (CBWFQ) is configured, the router may not match the input packet rate.

  Conditions: This symptom is observed on a Cisco router that is configured for ATM and Frame Relay.

  Workaround: There is no workaround.

- CSCeg69418

  Symptoms: You cannot re-enable Home Agent (HA) functionality on a router after you have first unconfigured it.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured for mobile IP.

  Workaround: There is no workaround.

- CSCeg88253

  Symptoms: Loss of packets may occur on video queues.

  Conditions: This symptom is observed on a Cisco 10000 series that has Class-Based Weighted Fair Queueing (CBWFQ) configured on a PPP over Ethernet over ATM (PPPoEoA) link and occurs when traffic is being processed.

  Workaround: There is no workaround.

- CSCeh54607

  Symptoms: On a router that processes a high traffic rate, the output of the **show processes cpu** command shows 100 percent CPU usage.

  Conditions: This symptom is observed on a Cisco router when the following conditions are present:

  - The router processes 70 PTA PPPoE sessions.
  - There are 70,000 packets per second with 120 bytes per packet upstream.
  - There are 5600 packets per second with 1500 bytes per packet downstream.

  Workaround: Reduce the traffic rate.

- CSCei38741

  Symptoms: Tracebacks are generated on a Cisco 10000 series that is configured with serial interfaces.

  Conditions: This symptom is observed when you change the encapsulation on a serial interface from PPP to Frame Relay.

  Workaround: Before you change the encapsulation from PPP to Frame Relay, enter the **no encapsulation ppp** command.

- CSCei54002

  Symptoms: A QoS group that is set through QoS Policy Propagation via BGP (QPPB) may not function.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE2.

  Workaround: Use QPPB to set the IP precedence.

- CSCej02774

  Symptoms: When you use the **BREAK** key to interrupt the image boot process and then enter the **dir** command from the ROMmon prompt, a recurring "Arithmetic Overflow Exception" may occur.

  Conditions: This symptom is observed on a Cisco 10000 series that has 104480 Kbytes of main memory and occurs only when a file system device driver is recursively loaded because you used the **BREAK** key to interrupt the image boot process and then entered the **dir** command without first resetting the ROMmon.

  Workaround: Let the image boot and then enter the **dir** command. If you must interact with the file system via the ROMmon when the boot process has been interrupted, enter the **reset** command. If autoboot is enabled, use the **BREAK** key immediately after the banner line appears on screen.

- CSCej46675

  Symptoms: A ping over an MLP connection may fail.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 336 bundles with 3 links each. Note that the symptom does not occur when the router has 100 bundles with 10 links each or 126 bundles with 8 links each.

  Workaround: There is no workaround.

- CSCej63166

  Symptoms: A router that is configured as an LSR may generate a "%LSD-4- LABEL_RESOURCE" error message when you attempt to extend the label range.

  Conditions This symptom is observed when the LSR is configured with a limited label range when you attempt to extend the label range.

  Workaround: Enter the **no mpls label range** command and reconfigure the extended label range.

- CSCej87817

  Symptoms: Policing does not drop any packets after the packets are sent or received at a rate that is much higher than the committed information rate (CIR).

  Conditions: This symptom is observed on a Cisco 7500 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCek00986

  Symptoms: A configuration does not synchronize to the standby RP and a traceback is generated.

Conditions: This symptom is observed on a Cisco router that has dual RPs and that has the **crypto key zeroize rsa** command enabled.

Workaround: There is no workaround.

- 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.

- CSCek11664

  Symptoms: A forwarded packet may be lost on a PPPoE session.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCek21091

  Symptoms: PPPoX multicast traffic is process-switched by default. This is improper behavior.

  Conditions: This symptom is observed when the **no ip mroute-cache** command is enabled for virtual-template interfaces, causing IP multicast traffic to be process-switched.

  Workaround: Enter the **ip mroute-cache** command for each virtual-template interface.

- CSCek25123

  Symptoms: When you apply a HQoS policy that has a shape parameter of 1 Gb in its parent policy to a subinterface, a traceback is generated. When there are more than 112 subinterfaces, you cannot apply the policy map to interfaces that exceed the 112th subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series when you apply or remove a HQoS policy to or from a subinterface and when the bandwidth in the parent policy map is 1 Gb.

  Workaround: There is no workaround.

- CSCek25822

  Symptoms: A PRE crashes when you enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs whether or not the router processes traffic.

  Workaround: Do not enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Further Documentation: The above-mentioned configuration is not supported on the Cisco 10000 series.

- CSCek27708

  Symptoms: A 1-port channelized OC-12 or 4-port channelized OC-3 line card may reset.

  Conditions: This symptom is observed on a Cisco 10000 series when you run a script that configures the line card with 768 E1 or T1 interfaces with either SDH or SONET framing.

  Workaround: There is no workaround.

- CSCek31331

  Symptoms: Gigabit Ethernet line cards flap and go down.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with multiple pairs of Gigabit Ethernet line cards when traffic flows at or is approaching the line rate.

Workaround: Either turn on or turn off negotiation on the affected pair of line cards and the point of traffic generation.

- CSCek34834

  Symptoms: Input drops or packet drops may occur when a 1-port Gigabit Ethernet half-height line card is processing IMIX traffic.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port Gigabit Ethernet half-height line card.

  Workaround: There is no workaround.

- CSCek36080

  Symptoms: A Cisco router that functions as an Intelligent Services Gateway (ISG) may reload when an error condition occurs in the control plane.

  Conditions: This symptom is observed under a rare conditions when an error occurs while a session that contains auto services is brought up or while a service profile that contains auto services is activated. The symptom occurs because of a timing issue.

  Workaround: Do not use auto services in the user profile.

- CSCek56991

  Symptoms: A Cisco 7200 series may send a corrupted packet via a 2-port T3 serial, enhanced port adapter (PA-2T3+). The rate of corrupted packets is very low.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB, Release 12.4T, or Release 12.4(4)XD3 and occurs when the router functions under high stress conditions such as a high CPU load and an oversubscribed interface of the PA-2T3+.

  Workaround: Avoid a high CPU load and oversubscription of the interface of the PA-2T3+.

- CSCin97726

  Symptoms: On a Cisco 7500 router, the console of the active RSP may hang.

  Conditions: This symptom is observed when the router functions in RPR mode and when you attempt to access the standby RSP file system from the console of the active RSP, for example, by entering the **write memory** command or the **dir slavedisk0:** command.

  Note that the symptom is not specific to the Cisco 7500 series and may also occur on other platforms.

  Workaround: There is no workaround.

  Further Problem Description: Normal operation of the router is not affected, but the console becomes inaccessible.

- CSCsa56416

  Symptoms: In order for Ethernet over MPLS (EoMPLS) to function properly in either port mode or VLAN mode, the Ethernet controller must operate in promiscuous mode, that is, all MAC address filtering must be disabled. On the 8-port Fast Ethernet (FE) line card, there is one single register that controls the enabling and disabling of address filtering for the whole line card. Therefore, if even one single EoMPLS circuit is created on any of the eight ports of the line card, address filtering is disabled for all eight ports, that is all eight ports operate promiscuous mode. This situation is not desirable.

Conditions: This symptom is observed on a Cisco 10000 series that is configured for EoMPLS when you create an AToM circuit by entering the **xconnect** command on an Ethernet controller of the 8-port FE line card. In this situation, promiscuous mode is automatically enabled on the Ethernet controller and remains enabled for all eight ports of the line card until the last AToM circuit is removed from the Ethernet controller by entering the **no xconnect** command.

Workaround: There is no workaround.

- CSCsb10347

  Symptoms: Multilink interfaces remain down after an SSO switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for LFIoFR and occurs only when traffic is flowing while an SSO switchover occurs. When there is no traffic, the interfaces come up normally.

  Workaround: There is no workaround.

- CSCsb32888

  Symptoms: Forcing **release** or **renew** commands on a BVI interface fails.

  Conditions: The symptom has been observed on the Cisco 7200 platform.

  Workaround: There is no workaround.

- CSCsb36094

  Symptoms: Policing in the outward direction is not performed for IP packets with an “IP Options” payload.

  Conditions: This symptom is observed on a Cisco 10000 series that processes incoming IP packets with the “IP Options” field. The policing actions are ignored for the outgoing IP packet.

  Workaround: There is no workaround.

- CSCsb79060

  Symptoms: A T1 interface that is configured on a channelized OC-3 line card or OC-12 line card may send a Loss of Framing (LoF) alarm, causing the T1 interface to enter the down/down state. Even after you have entered the **loopback local** command, have configured HDLC encapsulation, and have configured the clock source as internal, the T1 interface does not transition to the up state.

  Another symptom is that the framing may be good, but the TX data path is not good, causing the T1 interface to enter the up/down state. The output counters on the PRE increment, but the packets never actually leave the channelized line card.

  Conditions: These symptoms are observed on a Cisco 10000 series.

  Workaround: Reload the channelized line card by entering the **hw-module slot** *slot-number* **reset** command.

- CSCsb97334

  Symptoms: After you reload the router, a glean adjacency is not resolved if the prefix is a tunnel destination.

  Conditions: This symptom is observed on a Cisco 7304 that has a tunnel configured when the destination is another tunnel.

  Workaround: Ping the tunnel interface of the destination to resolve the adjacency.

- CSCsc18999

  Symptoms: When you enter the **clear subscriber sessions all** command, the router reloads.

Conditions: This symptom is observed when Transparent Autologon (TAL) is used with ISG for control over DHCP addressing and when the router is using nearly all available CPU cycles and RAM.

Workaround: Do not you enter the **clear subscriber sessions all** command.

- CSCsc27712

  Symptoms: An ATM Permanent Virtual Path (PVP) goes down after a couple of minutes of non-activity.

  Conditions: This symptom is observed on a Cisco router when you enter the **atm pvp** command and leave the connection idle for a couple of minutes.

  Workaround: There is no workaround.

- CSCsc37472

  Symptoms: The output rate counters for a member link of a multilink interface do not increment when you look at the output of the **show interfaces** command.

  Conditions: This symptom is observed on a Cisco 10000 series when packets are properly delivered through the member link of the multilink interface.

  Workaround: Look at the PXF counters in the output of the **show pxf cpu queue multilink** *interface* or **show pxf cpu subblock multilink** *interface* commands.

- CSCsc48372

  Symptoms: The police function stops working when a PQ class map is removed and redefined for a policy map and when any class that is defined above the PQ class map is deleted. In this situation, all packets that match the PQ classes are marked as violated packets.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Remove the service policy and re-apply the service policy to the affected interfaces.

- CSCsc58937

  Symptoms: When you run the CISCO-FLASH-MIB, various traps are missing even though the operation is reported as successfully completed.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SNMP.

  Workaround: There is no workaround.

- CSCsc60444

  Symptoms: A “PXF DMA Toaster Stall Error” may occur, the microcode may unexpectedly be reloaded onto the PXF engine, and the reusable bandwidth may be incorrectly shaped.

  Conditions: These symptoms are observed on a Cisco 10000 series when a hierarchical policy map is attached to a Gigabit Ethernet interface and when the hierarchical policy map has a shaped rate that exceeds the link rate.

  Workaround: Do not attach a policy map that has a shaped rate that exceeds the link rate.

- CSCsc71353

  Symptoms: The **xconnect** command is not accepted.

  Conditions: This symptom is observed on a Cisco 7304 when you attempt to configure the **xconnect** command on an IMA port adapter that is configured for AAL0 encapsulation.

  Workaround: There is no workaround.

- CSCsc84834

  Symptoms: An adjacency is not established when a GRE tunnel is configured.

Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100.

Workaround: Ping the next hop through the GRE tunnel.

- CSCsc97102

  Symptoms: When you create or delete an PPPoX session, the address conversion from the RP to the eXternal Column Memory (XCM) is incorrect, as is shown by a traceback that is displayed on the console of the standby PRE.

  Conditions: This symptom is observed randomly on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsd00354

  Symptoms: The output of the **show policy-map interface** command shows the output queue packets and bytes counters as zero.

  Conditions: This symptom is observed on a Cisco 10000 series on queues for which a policer is applied.

  Workaround: Use the policer's counters in the output of the **show policy-map interface** command to determine the number of forwarded and dropped packets and bytes for the queue.

- CSCsd08662

  Symptoms: A Cisco 7200 series may crash when you apply a service policy with a priority action on a control plane.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

  Workaround: There is no workaround.

  Further Problem Description: A service policy with a priority action is not supported on a control plane. See the following Cisco document:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide0 9186a008052446b.html

- CSCsd14277

  Symptoms: A ping does not pass through a Fast Ethernet interface that functions in AToM port mode.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that has the **xconnect** interface configuration command enabled on the interface of a 1-port Fast Ethernet port adapter (PA-FE) that is installed in a port adapter carrier card (7300-CC-PA).

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

  Alternate Workaround: Enter the **shutdown** interface configuration command, the **xconnect** interface configuration command, and then the **no shutdown** interface configuration command on the affected interface.

- CSCsd25699

  Symptoms: MLP traffic fails during a PRE failover of the protect router.

  Conditions: This symptom is observed on a Cisco 10000 series when a PRE failover occurs on the protect router because of an MR-APS cable break failover from the protect router to the working router.

  Workaround: If the active controller is brought up after the MR-APS failover, manually reverse APS.

- CSCsd25713

  Symptoms: A Cisco 7304 crashes because of an address error (load or instruction fetch) exception when you remove a virtual template that is applied to at least one ATM subinterface by entering the **no interface virtual-template** command.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(27)SBC1 and may also occur in Release 12.2(28)SB.

  Workaround: Dot no apply a virtual template to an ATM interface.

- CSCsd38522

  Symptoms: Very high CPU usage may occur on a Cisco 10000 series when several thousand PPPoX PTA sessions are established and when the Port-Bundle Host Key (PBHK) feature is enabled. This situation can be observed in the output of the **show processes cpu** command.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured as an Intelligent Service Gateway (ISG) and that has the PBHK feature enabled with the default traffic class.

  Workaround: Apply an explicit traffic class to the port bundle, that is, apply an IP ACL that has the IP address of the Subscriber Edge Services Manager (SESM) as its destination IP address. Doing so reduces the CPU usage considerably.

- CSCsd39557

  Symptoms: Non-priority traffic is dropped, and priority traffic is sent at a very low rate.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when hierarchical shaping is configured on an ATM VC with a priority class in the next layer, as in the following example:

  ```
  policy-map atm-pri600 class From2_0 priority 150
  policy-map hiershape class class-default shape average 1000000 service-policy atm-pri600
  interface ATM4/0.401 point-to-point pvc 1/401 vbr-nrt 600 600 service-policy out hiershape
  ```

  Workaround: There is no workaround to prevent the symptom from occurring. You can restore the flow by first removing the policy from the interface and then by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCsd41107

  Symptoms: A Cisco 10000 series that functions as an LNS with a highly scaled configuration may reload unexpectedly.

  Conditions: This symptom is observed when the router runs very low on available processor memory. When this situation occurs, the following error messages are generated:

  ```
  GENERAL-2-CRITEVENT: Unable to malloc current_if_info C10K_BBA_SESSION-3-ERREVENT: No VCCI found for LNS session (26831)
  ```

  Workaround: Reduce or limit the number of L2TP tunnels and/or the number of PPP sessions that are being terminated on the LNS.

- CSCsd44475

  Symptoms: A ping may fail when packets pass from an MPLS VPN into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that functions as a PE router, and that is connect to the MPLS core via a serial interface.

  Possible Workaround: Do not use a serial interface to connect the PE router to the MPLS core. Rather, use another type of interface.

Further Problem Description: The symptom occurs because the tunnel adjacency is not complete in the PXF engine, preventing packets from being correctly punted and the adjacency from becoming complete.

- CSCsd49072

  Symptoms: The output of the **show policy-map interface** command shows incorrect statistics for a DSCP-based WRED policy. Also, when the class-map parameters are dynamically changed, the WRED statistics are lost.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsd51700

  Symptoms: A serial interface that is connected to an OSPP neighbor may flap during an SSO switchover, causing OSPF NSF to terminate during the switchover.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for NSF and occurs after multiple (10 or more) SSO switchovers.

  Workaround: There is no workaround.

- CSCsd52476

  Symptoms: Some members of a multilink interface may flap when you enter the **write memory** command on the PRE. Flapping occurs randomly each time the router reloads.

  Conditions: There symptoms are observed on a Cisco 10000 series that is configured for SSO, MR-APS, and MLP with Link Fragmentation Interleave (LFI).

  Workaround: There is no workaround.

- CSCsd57076

  Symptoms: A router crashes when you attach a service policy at the PVC level on an ATM interface.

  Conditions: This symptom is observed on a Cisco 7200 series when a bandwidth action is configured in the service policy and when traffic is passing through the interface.

  Workaround: There is no workaround.

- CSCsd64632

  This caveat consists of two symptoms, two conditions, and two workarounds:

  3. Symptom 1: After one or two switchovers have occurred, SSH services become disabled because the RSA key is lost.

     Condition 1: This symptom is observed on a Cisco router that functions in either RPR+ or SSO mode.

     Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the lost settings via the console or a vty connection.

  4. Symptom 2: After one or two switchovers have occurred, the encrypted SNMP information or private setting becomes lost.

     Condition 1: This symptom is observed on a Cisco router that functions in RPR+ mode.

     Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the lost settings via the console or a vty connection.

- CSCsd87487

  Symptoms: Multilink interfaces remain down after an SSO switchover.

Conditions: This symptom is observed on a Cisco 10000 series that is configured for LFIoATM or MLPoATM and occurs only when traffic is flowing while an SSO switchover occurs. When there is no traffic, the interfaces come up normally.

Workaround: There is no workaround.

- CSCsd93555

  Symptoms: On a Cisco 7304 that has an NSE-100, it is possible to configure Link Fragmentation and Interleaving (LFI) over MLP and an egress QoS policy on a multilink interface. This is an inappropriate configuration because neither of these features can work effectively in the NSE-100 architecture.

  Conditions: This symptom is observed on a Cisco 7304 with an NSE-100. Note that LFI over MLP and an egress QoS policy on a multilink interface is an appropriate configuration on a Cisco 7304 with an NPE-G100 and works fine on a Cisco 7304 with an NPE-G100.

  Workaround: Disable LFI over MLP by entering the **no ppp multilink interleave** command. Disable QoS on a multilink interface by entering the **no service-policy output** *policy-map-name* command.

TCP/IP Host-Mode Services

- CSCek01499

  Symptoms: When a CE router that is configured for MPLS reloads, a software-forced crash may occur on the connected PE router because of memory corruption.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has two RPs that function in SSO mode. The symptom does not occur when the router has only a single RP.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCej58338

  Symptoms: A ping may fail across an ISDN BRI channel even though the ISDN B channel is up.

  Conditions: This symptom is observed on a Cisco router when routing protocols are enabled on the ISDN BRI channel.

  Workaround: Clear the BRI B channel.

- CSCek24091

  Symptoms: A PPP session fails to come up, and the following debug message is generated:

  ```
  PPP SSS: stale named authen method list "default"
  ```

  Conditions: This symptom is observed only when a service policy is applied and when the default PPP authentication method list is used.

  Workaround: Use a PPP authentication method list other than the PPP authentication default method list.

- CSCsb71154

  Symptoms: When a VC that is configured under a VP goes down, PPPoE sessions can still be established over the VC.

Conditions: This symptom is observed on a Cisco 10000 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface or after you have reloaded the router.

Workaround: There is no workaround.

- CSCsc28120

  Symptoms: A Cisco 7301 may crash when a service policy is removed from an interface that is configured for Frame Relay encapsulation.

  Conditions: This symptom is observed when a service policy is configured on an interface before the encapsulation is changed to Frame Relay. When the service policy is then removed, the router crashes.

  Workaround: Remove the service policy before you change the encapsulation to Frame Relay.

- CSCsd01322

  Symptoms: A PPP session is created with an IP address that is 0.0.0.0.

  Conditions: This symptom is observed on a Cisco router when a RADIUS profile uses the "ip:addr-pool" attribute to assign an IP address and when AAA authorization fails because there is no IP address available in the address pool.

  Workaround: Enter the **ppp ipcp address required** command to prevent a PPP session from being created with an IP address of 0.0.0.0.

- CSCsd06110

  Symptoms: A router may exhaust its I/O memory.

  Conditions: This symptom is observed on a Cisco router when you clear 10,000 tunnels on which about 45,000 PPP sessions are established. The symptom occurs only under extreme stress situations.

  Workaround: Clear the tunnels and sessions in stages.

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 12.2SB. 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, page 273
- Platform-Specific Documents, page 275
- Feature Modules, page 276
- Cisco Feature Navigator, page 276
- Cisco IOS Software Documentation Set, page 277

Release-Specific Documents

This section provides information about release-specific documents.

Cisco IOS Release 12.2SB

For detailed information about release-specific documents for Cisco IOS Release 12.2SB, see the *Cisco IOS Release 12.2SB Documentation Roadmap*:

http://www.cisco.com/en/US/products/ps6566/products_documentation_roadmap09186a00806786c3.html

Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents for Cisco IOS Release 12.2SB are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

On Cisco.com at

Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2SB**

On http://www.cisco.com/univercd/home/index.htm at

Cisco IOS Software: **Release 12.2**: **All IOS Releases**: **Cisco IOS Release 12.2SB**

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**

Platform-Specific Documents

Platform-specific information and documents for the platforms that are supported in Cisco IOS Release 12.2SB are available at the locations listed below:

- Cisco 7200 Series Routers
  - Cisco 7200 series home page on Cisco.com at

    Products & Services: **Products: Routers and Routing Systems**: **7200 Series Routers**
  - Cisco 7200 series technical documentation on Cisco.com at

    Products & Services: **Products: Routers and Routing Systems**: **7200 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7200 Series Routers**

    For Cisco 7200 series technical documentation on http://www.cisco.com/univercd/home/index.htm, select a Cisco 7200 series router from the **Routers** pull-down menu on the top left of the page.
- Cisco 7301 Router
  - Cisco 7300 series home page on Cisco.com at

    Products & Services: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 7300 Series Routers**
  - Cisco 7300 series technical documentation on Cisco.com at

    Products & Services: Routers & Routing Systems: **All Routers & Routing Systems**: **Cisco 7300 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7300 Series Routers**
  - Cisco 7301 technical documentation on http://www.cisco.com/univercd/home/index.htm at

    Routers: **Cisco 7301**

- Cisco 7304 Router
  - Cisco 7300 series home page on Cisco.com at

    Products & Services: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 7300 Series Routers**
  - Cisco 7300 series technical documentation on Cisco.com at

    Products & Services: Routers & Routing Systems: **All Routers & Routing Systems**: **Cisco 7300 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7300 Series Routers**
  - Cisco 7304 technical documentation on http://www.cisco.com/univercd/home/index.htm at

    Routers: **Cisco 7304**
- Cisco 10000 Series Routers
  - Cisco 10000 series home page on Cisco.com at

    Products & Services: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 10000 Series Routers**
  - Cisco 10000 series technical documentation on Cisco.com at

    Products & Services: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 10000 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 10000 Series Routers**
  - Cisco 10000 series technical documentation on http://www.cisco.com/univercd/home/index.htm at

    Routers: **Cisco 10000 ESR**

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2SB 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 12.2SB are available at the following locations:

- Release 12.2(31)SB2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/index.htm
- Release 12.2(28)SB

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

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/fn

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 16 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 16 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 16 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 16 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, Obtaining Support, and Security Guidelines

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 273.