Cross-Platform Release Notes for Cisco IOS Release 12.2(27)SBA and Release 12.2(27)SBB

September 24, 2008

Cisco IOS Release 12.2(27)SBA6 and Release 12.2(27)SBB9

OL-7672-01 Rev. F1

These release notes support Cisco IOS Release 12.2(27)SBA up to and including Release 12.2(27)SBA6 and Cisco IOS Release 12.2(27)SBB up to and including Release 12.2(27)SBB9. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and related documents.

Note Cisco IOS Release 12.2(27)SBA and its rebuilds support only the Cisco 7200 series, Cisco 7301, and Cisco 7500 series. Cisco IOS Release 12.2(27)SBB and its rebuilds support only the Cisco 10000 series.

Cisco IOS Release 12.2(27)SBA is tailored for service provider and large-scale enterprise networks. One of the main purposes of Release 12.2(27)SBA is to introduce the Intelligent Service Gateway (ISG) and its Intelligent Service Architecture (ISA).

Cisco IOS Release 12.2(27)SBB is tailored for service provider networks. One of the main purposes of Release 12.2(27)SBB is to introduce greater scalability for Multiprotocol Label Switching (MPLS) provider edge (PE) applications with the introduction of advanced High Availability (HA) capabilities.

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 61 and the *Caveats for Cisco IOS Release 12.2* document. The caveats document is updated for every maintenance release and is located on Cisco.com.

Use these release notes in conjunction with the *Cross-Platform Release Notes for Cisco IOS Release 12.2* document located on Cisco.com.

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.

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

Contents

Introduction

Cisco IOS Release 12.2SB is based on Cisco IOS Release 12.2(25)S. 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, Cisco 7301, and Cisco 7500 series, all features that are in Release 12.2(25)S are also in Release 12.2SB. In addition, Release 12.2SB includes many features from Cisco IOS Release 12.2T.

Cisco IOS Release 12.2(27)SBA is a limited-availability release of Release 12.2SB that supports the Cisco 7200 series, Cisco 7301, and Cisco 7500 series. Cisco IOS Release 12.2(27)SBB is a limited-availability release of Release 12.2SB that supports the Cisco 10000 series. 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 14 and the "Caveats" section on page 61.

Early Deployment Releases

These release notes describe the Cisco 7200 series routers, Cisco 7301 router, Cisco 7500 series routers, and Cisco 10000 series routers for Cisco IOS Release 12.2SB, which is an early deployment (ED) release based on Cisco IOS Release 12.2S and Release 12.2T. 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 7500 Series, and Cisco 10000 Series

Cisco IOS ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(27)SBA6	No new software features.	No new hardware features.	06/16/2006
12.2(27)SBA5	No new software features.	No new hardware features.	02/16/2006
12.2(27)SBA4[1]	No new software features.	No new hardware features.	11/15/2005
12.2(27)SBA2	No new software features.	No new hardware features.	06/22/2005
12.2(27)SBA1	See the "New Software Features in Cisco IOS Release 12.2(27)SBA1" section on page 34.	No new hardware features.	05/09/2005
12.2(27)SBA	See the "New Software Features in Cisco IOS Release 12.2(27)SBA" section on page 36.	No new hardware features.	04/28/2005
12.2(27)SBB9	No new software features.	No new hardware features.	12/14/2006
12.2(27)SBB8	No new software features.	No new hardware features.	12/11/2006
12.2(27)SBB7	No new software features.	No new hardware features.	08/23/2006
12.2(27)SBB6	No new software features.	No new hardware features.	06/30/2006
12.2(27)SBB5	No new software features.	No new hardware features.	05/05/2006
12.2(27)SBB4	No new software features.	No new hardware features.	03/29/2006
12.2(27)SBB3	No new software features.	No new hardware features.	02/02/2006
12.2(27)SBB2	No new software features.	No new hardware features.	11/10/2005
12.2(27)SBB1	No new software features.	No new hardware features.	10/03/2005
12.2(27)SBB	See the "New Software Features in Cisco IOS Release 12.2(27)SBB" section on page 14.	No new hardware features.	06/23/2005

1. Cisco IOS Release 12.2(27)SBA4 follows Release 12.2(27)SBA2. Release 12.2(27)SBA3 is not a public release.

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. However, Cisco IOS Release 12.2(27)SBA, Release 12.2(27)SBB, and the rebuilds of these releases are not supported in Cisco Feature Navigator. Later releases of Release 12.2SB will be supported in Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). 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.

To access Cisco Feature Navigator, 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

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

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, enter your Cisco.com login, 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 7202, Cisco 7204, Cisco 7204VXR, Cisco 7206, and Cisco 7206VXR routers)
- Cisco 7301 router
- Cisco 7500 series routers (including the Cisco 7505, Cisco 7507, and Cisco 7513 routers)
- Cisco 10000 series routers (the Cisco 10008)

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 14.

Table 2 describes the supported platforms for Cisco IOS Release 12.2SBA and Release 12.2SBB 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 12.2SBA and Release 12.2SBB

Cisco IOS Release	Cisco 7200 Series	Cisco 7301 Router	Cisco 7500 Series	Cisco 10000 Series
12.2(27)SBA6	Yes	Yes	Yes	No
12.2(27)SBA5	Yes	Yes	Yes	No
12.2(27)SBA4	Yes	Yes	Yes	No
12.2(27)SBA2	No	No	Yes	No
12.2(27)SBA1	No	No	Yes	No
12.2(27)SBA	Yes	Yes	No	No
12.2(27)SBB9	No	No	No	Yes
12.2(27)SBB8	No	No	No	Yes
12.2(27)SBB7	No	No	No	Yes
12.2(27)SBB6	No	No	No	Yes

Table 2 Supported Platforms for Cisco IOS Release 12.2SBA and Release 12.2SBB (continued)

Cisco IOS Release	Cisco 7200 Series	Cisco 7301 Router	Cisco 7500 Series	Cisco 10000 Series
12.2(27)SBB5	No	No	No	Yes
12.2(27)SBB4	No	No	No	Yes
12.2(27)SBB3	No	No	No	Yes
12.2(27)SBB2	No	No	No	Yes
12.2(27)SBB1	No	No	No	Yes
12.2(27)SBB	No	No	No	Yes

Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, and Cisco 7500 Series

Table 3 lists the port adapters that are supported for the Cisco 7200 series routers, Cisco 7301 router, and Cisco 7500 series routers 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 number in the "In" column indicates the Cisco IOS 12.2SB release in which the port adapter was introduced. For example, (27) would mean that a port adapter was introduced in Cisco IOS Release 12.2(27)SBA. 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 7500 Series

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7500 Series
ATM Port Adapters					
PA-A1-OC3SM	1-port ATM OC3 single mode (IR)	—	No	No	Yes
PA-A1-OC3MM	1-port ATM OC3 multimode	—	No	No	Yes
PA-A2-4T1C-OC3SM=	ATM CES, 4 T1 CES ports, 1 OC3 ATM SM port	—	Yes	No	No
PA-A2-4T1C-T3ATM=	ATM CES, 4 T1 CES ports, 1 T3 ATM port	—	Yes	No	No
PA-A2-4E1XC-OC3SM=	CES OC3, 4 E1 ports, 120 ohms	—	Yes	No	No
PA-A2-4E1XC-E3ATM=	CES E3/E1, 120 ohms	—	Yes	No	No
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	Yes

Table 3 Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, and Cisco 7500 Series (continued)

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7500 Series
PA-A3-OC12SMI	1-port ATM Enhanced OC12/STM4 single mode (IR)	—	No	No	Yes
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
Channel Port Adapters					
PA-4C-E=	1-port Enhanced ESCON Channel	—	Yes	No	No
Dynamic Packet Transport (DPT) Port Adapters					
PA-SRP-OC12MM=	DPT-OC12 multimode (Cisco 7200 series only)	—	Yes	No	No
PA-SRP-OC12SMI=	DPT-OC12 single mode (IR) (Cisco 7200 series only)	—	Yes	No	No
PA-SRP-OC12SML=	DPT-OC12 single mode (LR) (Cisco 7200 series only)	—	Yes	No	No
PA-SRP-OC12SMX=	DPT-OC12 single mode extended reach (Cisco 7200 series only)	—	Yes	No	No
SRPIP-OC12MM=	DPT-OC12 multimode (Cisco 7500 series only)	—	No	No	Yes
SRPIP-OC12SMI=	DPT-OC12 single mode (IR) (Cisco 7500 series only)	—	No	No	Yes
SRPIP-OC12SML=	DPT-OC12 single mode (LR) (Cisco 7500 series only)	—	No	No	Yes
SRPIP-OC12SMX=	DPT-OC12 single mode extended reach (Cisco 7500 series only)	—	No	No	Yes
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-5EFL	5-port Ethernet 10BASE-FL	—	Yes	Yes	Yes
PA-8E	8-port Ethernet 10BASE-T	—	Yes	Yes	Yes
PA-FE-FX	1-port Fast Ethernet 100BASE-FX	—	Yes	Yes	Yes
PA-FE-TX	1-port Fast Ethernet 100BASE-TX	—	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	No

Table 3 Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, and Cisco 7500 Series (continued)

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7500 Series
FDDI Port Adapters					
PA-F/FD-MM	1-port FDDI Full Duplex multimode	—	Yes[2]	No	Yes
PA-F/FD-SM	1-port FDDI Full Duplex single mode	—	Yes[2]	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-8T1	8-port multichannel T1, integrated CSU/DSUs	—	Yes	Yes	Yes
PA-MC-8E1/120	8-port multichannel E1, G.703 120-ohm interface	—	Yes	No	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
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
Service Adapters					
SA-ENCRYPT=	Encryption Service Adapter	—	No	No	Yes
SA-ISA	Integrated Services Adapter for IPSec or MPPE encryption	—	Yes	No	No
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

Table 3 Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, and Cisco 7500 Series (continued)

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7500 Series
PA-POS-OC3SML	1-port Packet over SONET OC3c/STM1 single mode (LR)	—	Yes	Yes	Yes
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, T3 DSUs	—	Yes	Yes	Yes
PA-T3+	1-port T3 Serial, Enhanced	—	Yes	Yes	Yes
PA-2T3	2-port T3 Serial, T3 DSUs	—	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
Token Ring Port Adapters					
PA-4R-DTR	4-port Dedicated Token Ring, 4/16Mbps, HDX/FDX	—	Yes	No	Yes
Voice Port Adapters					
PA-MCX-2TE1=	2-port MIX-enabled multichannel T1/E1, CSU/DSU	—	Yes	No	No
PA-MCX-4TE1=	4-port MIX-enabled multichannel T1/E1, CSU/DSU	—	Yes	No	No
PA-MCX-8TE1-M=	8-port multichannel T1/E1, Signaling System 7 over IP (SS7oIP)	—	Yes	No	No
PA-MCX-8TE1=	8-port MIX-enabled multichannel T1/E1, CSU/DSU	—	Yes	No	No
PA-VXA-1TE1-24+	1-port T1/E1 Digital Voice, 24 Channels	—	Yes	No	Yes
PA-VXA-1TE1-30+	1-port T1/E1 Digital Voice, 30 Channels	—	Yes	No	Yes
PA-VXB-2TE1+	2-port T1/E1 moderate capacity, Enhanced	—	Yes	Yes	Yes
PA-VXC-2TE1+	2-port T1/E1 high capacity, Enhanced	—	Yes	Yes	Yes

1. For a spare product number, append an equal sign (=) to the product number. If a product number is listed as a spare product, only a spare product is available. 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 7500 series: http://www.cisco.com/en/US/products/hw/routers/ps359/prod_eol_notices_list.html
2. The FDDI port adapters are supported on non-VXR routers.

For troubleshooting and alerts information about port adapters, 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(27)SBB 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, (27) means that a line card was introduced in Cisco IOS Release 12.2(27)SBB. 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(27)SBB.

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	—
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	—
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	—
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	—

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

Common Abbreviation	Cisco Product Number[1]	Line Card Description	In
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.
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.

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(27)SBA, 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 7500 series routers, 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

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 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.

Note Cisco IOS Release 12.2(27)SBA, Release 12.2(27)SBB, and the rebuilds of these releases are not supported in Cisco Feature Navigator. Later releases of Release 12.2SB will be supported in Cisco Feature Navigator.

To access Cisco Feature Navigator, 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

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

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

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. However, Cisco IOS Release 12.2(27)SBA, Release 12.2(27)SBB, and the rebuilds of these releases are not supported in Cisco Feature Navigator. Later releases of Release 12.2SB will be supported in Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). 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.

To access Cisco Feature Navigator, 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

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

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, enter your Cisco.com login, 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, enter your Cisco.com login, 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 A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. However, Cisco IOS Release 12.2(27)SBA, Release 12.2(27)SBB, and the rebuilds of these releases are not supported in Cisco Feature Navigator. Later releases of Release 12.2SB will be supported in Cisco Feature Navigator.
To access Cisco Feature Navigator, 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://www.cisco.com/register.

New Hardware Features in Cisco IOS Release 12.2(27)SBB

Cisco IOS Release 12.2(27)SBB does not introduce new hardware features. For information about supported platforms, see the "Supported Hardware" section on page 5.

New Software Features in Cisco IOS Release 12.2(27)SBB

This section describes new and changed features in Cisco IOS Release 12.2(27)SBB. 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(27)SBB. 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 5 lists the features that have never been introduced in any other Cisco IOS software release for the Cisco 10000 series; these features are introduced for the Cisco 10000 series in Cisco IOS Release 12.2(27)SBB for the first time.

Table 5 New Features for the Cisco 10000 Series

Feature Name
Any Transport over MPLS (AToM): Frame Relay over MPLS (FRoMPLS)
Cisco BGP Nonstop Routing
Hierarchical Input Policing
IGMPv3
IP SLAs - LSP Health Monitor
In Service Software Upgrade (ISSU)
Layer 2 Local Switching
Link Fragmentation Interleave over Frame Relay (FRF.12)
MLP Connections
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: • MPLS High Availability: Overview • MPLS LDP: SSO/NSF Support and Graceful Restart • MPLS VPN: SSO/NSF Support • 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
Multicast-VPN: Multicast Support for MPLS VPN
Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services
Two-Rate Policer (this feature may also be known as Dual Rate Three Color Policer)

For information about new commands and command changes in Cisco IOS Release 12.2(27)SBB, see "Chapter 1" of the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/10000_c//bba_sbb.pdf

ACL Authentication of Incoming rsh and rcp Requests

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbtauth.htm

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

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/software/ios122s/122snwft/release/122sb/122sbb27/10000_c//bba_sbb.pdf

ARP Optimization

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbarpop.htm

ATM Features

Cisco IOS Release 12.2(27)SBB supports the following ATM features.

ATM Bulk VC Configuration

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/software/ios122s/122snwft/release/122sb/122sbb27/10000_c//bba_sbb.pdf

ATM PVCs

The ATM line cards support the full range of VPI//VCI pairs (unidirection only)—8-bit VPI range and 16 bit VCI range. Table 6 lists the maximum number of active VCs supported on ATM line cards for Cisco IOS Release 12.2(27)SBB.

Table 6 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 of them 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 of them 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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/dtatmpvr.htm

BGP Features

Cisco IOS Release 12.2(27)SBB supports the following Border Gateway Protocol (BGP) features.

BGP 4 MIB Support for per-Peer Received Routes

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/ios122s/122snwft/release/122s14/fsbgpmib.htm

BGP Conditional Route Injection

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/ftbgpri.htm

BGP Convergence Optimization

BGP Convergence Optimization introduces a new algorithm for update generation that reduces the amount of 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 may also be known as BGP: Reduction in Transient Memory Usage.

BGP Configuration Using Peer Templates

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/120s24/s_bgpct.htm

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

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

BGP Dynamic Update Peer-Groups

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/120s24/s_bgpdpg.htm

BGP Hide Local-Autonomous System

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11bhla.htm

BGP Hybrid CLI Support

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/ftbhycli.htm

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/ftiaaspa.htm

BGP Link Bandwidth

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11b_lb.htm

BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11bmpl.htm

BGP Named Community Lists

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftbgpncl.htm

BGP Next Hop Propagation

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

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a008045afd9.html

BGP Policy Accounting

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/ft_bgppa.htm

BGP Prefix-Based Outbound Route Filtering

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11borf.htm

BGP Route-Map Continue

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/gt_brmcs.htm

BGP Route-Map Policy List Support

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/ftbgprpl.htm

BGP Support for Dual AS Configuration for Network AS Migrations

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/fsbgpdas.htm

BGP Support for TTL Security Check

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_btsh.htm

Cisco BGP Nonstop Routing

For detailed information about this feature, see the *BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO)* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_bnsr.htm

Bit Error Rate Test (BERT)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_bert.htm

CEF/dCEF - Cisco Express Forwarding

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/software/ios122s/122snwft/release/122sb/122sbb27/10000_c//bba_sbb.pdf

Crashinfo Support

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.

EIGRP MPLS VPN PE-CE Site of Origin (SoO)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/s_mvesoo.htm

Globalized Channelizations for SONET/SDH

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

ICMP Rate Limiting

The ICMP Rate Limiting feature is used to rate-limit ICMP echo-reply traffic in order to protect hosts against Denial of Service (DoS) attacks.

IEEE 802.1p Support

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 local-area networks (LANs). Network managers can begin to migrate to 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 Features

Cisco IOS Release 12.2(27)SBB supports the following Internet Group Management Protocol (IGMP) features.

IGMP State Limit

The IGMP State Limit feature provides protection against denial of service attacks caused by Internet Group Management Protocol (IGMP) packets. The new command-line interface (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.

IGMPv3

For detailed information about this feature, see the "Configuring IGMP Version 3" section in the "Configuring IP Multicast Routing" chapter of "Part 3: IP Multicast" of the Cisco IOS IP Configuration Guide, Release 12.2 document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfmulti.htm#wp1046118

IGMP Version 3—Explicit Tracking of Hosts, Groups, and Channels

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/fs_xtrc.htm

In Service Software Upgrade (ISSU)

The In Service Software Upgrade (ISSU) feature includes support for the following features:

- ARP for ISSU
- ATM HA/ISSU Support
- FHRP—HSRP ISSU support
- Frame Relay Support for High Availability ISSU
- HDLC HA ISSU Support
- ISSU for PPP/MLP
- SNMP Support for ISSU

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/ios122s/122snwft/release/122sb/122sbb27/sbb_issu.htm

The In Service Software Upgrade (ISSU) feature includes support for the following MPLS features:

- MPLS - ISSU Support for LDP
- MPLS - SSO/NSF and ISSU for MPLS QoS
- MPLS VPN - ISSU Support for IPv4 VPNs

For detailed information about these features, see the *ISSU MPLS Clients* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/isclimpl.htm

The In Service Software Upgrade (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

IP Event Dampening

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/fsipevdp.htm

IPMROUTE-STD-MIB

The IPMROUTE-STD-MIB, as defined in RFC 2932, is a module for management of 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

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/software/ios122s/122snwft/release/122sb/122sbb27/10000_c//bba_sbb.pdf

IP Multicast MIB Enhancements

The IP Multicast MIB Enhancements feature enhances the IP multicast routing protocol in Cisco IOS software by adding MIB variables to query the number of (S, G) and (*, G) entries. It also adds support for high-speed interface counters.

IP SLAs - LSP Health Monitor

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_lsph.htm

IS-IS Features

Cisco IOS Release 12.2(27)SBB supports the following Intermediate System-to-Intermediate System (IS-IS) features.

Integrated IS-IS Global Default Metric

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/gtisglob.htm

Integrated IS-IS Point-to-Point Adjacency over Broadcast Media

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/fissp2p.htm

Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

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/gtisprot.htm

IS-IS Caching of Redistributed Routes

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/isredrib.htm

IS-IS Fast-Flooding of LSPs Using the fast-flood Command

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/fstfld.htm

IS-IS Incremental Shortest Path First (i-SPF) Support

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

http://www.cisco.com/univercd/td/doc/product/software/ios120/120newft/120limit/120s/120s24/isisispf.htm

IS-IS Limit on Number of Redistributed Routes

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/120s25/fsiredis.htm

IS-IS Support for Priority-Driven IP Prefix RIB Installation

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/fslocrib.htm

Layer 2 Local Switching

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/software/ios122s/122snwft/release/122sb/122sbb27/10000_c//bba_sbb.pdf

MLP Connections

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/software/ios122s/122snwft/release/122sb/122sbb27/10000_c//bba_sbb.pdf

MPLS Features

Cisco IOS Release 12.2(27)SBB supports the following Multiprotocol Label Switching (MPLS) and MPLS-related features.

MPLS (Multiprotocol Label Switching)

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/software/ios122s/122snwft/release/122sb/122sbb27/10000_c//bba_sbb.pdf

MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_mlpt.htm

MPLS LDP MD5 Global Configuration

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_md5.htm

MPLS QoS—DiffServ Tunnel Mode Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbdftnl.htm

MPLS HA Features

Cisco IOS Release 12.2(27)SBB supports the following Multiprotocol Label Switching (MPLS) High Availability (HA) features.

MPLS High Availability: Overview

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbhaov.htm

MPLS LDP: SSO/NSF Support and Graceful Restart

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbldpgr.htm

MPLS VPN: SSO/NSF Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbvpngr.htm

Command Changes in Relation to MPLS HA

For command changes in relation to MPLS HA, see the following documents:

- Cisco Express Forwarding: Command Changes

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbcefcd.htm

- MPLS High Availability: Command Changes

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbcmdha.htm

MPLS VPN Features

Cisco IOS Release 12.2(27)SBB supports the following Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) features.

MPLS VPN—Carrier Supporting Carrier

For detailed information about this Label Distribution Protocol (LDP)-related feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb2scsc.htm

MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution

For detailed information about this Border Gateway Protocol (BGP)-related feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbcsc13.htm

MPLS VPN—eBGP Multipath Support for CSC and InterAS MPLS VPNs

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

- MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbcsc13.htm

- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_smlp.htm

MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_xnlb.htm

MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_smlp.htm

MPLS VPN - Show Running VRF

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_svrf.htm

Multicast-VPN: Multicast Support for MPLS VPN

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/ios122s/122snwft/release/122sb/122sbb27/sbb_mvpn.htm

MSDP Compliance with IETF RFC 3618

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_msdp.htm

Multicast Subsecond Convergence

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/fs_subcv.htm

Multirouter Automatic Protection Switching (APS)

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/software/ios122s/122snwft/release/122sb/122sbb27/10000_c//bba_sbb.pdf

Nonstop Forwarding and Stateful Switchover Features

Nonstop Forwarding

Cisco IOS Release 12.2(27)SBB 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/122sb/122sbb27/sbb_nsf.htm

Stateful Switchover

Cisco IOS Release 12.2(27)SBB supports the following Stateful Switchover (SSO) features:

- APS Stateful Switchover (SSO)
- 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, see the *Stateful Switchover* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_sso.htm

OSPF Features

Cisco IOS Release 12.2(27)SBB supports the following Open Shortest Path First (OSPF) features.

OSPF ABR Type 3 LSA Filtering

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/ft11at3f.htm

OSPF Area Transit Capability

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/ospfatc.htm

OSPF Forwarding Address Suppression in Translated Type-5 LSAs

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/ftoadsup.htm

OSPF Inbound Filtering using Route Maps with a Distribute List

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/120s24/routmap.htm

OSPF Incremental Shortest Path First (i-SPF) Support

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/120s24/ospfispf.htm

OSPF Support for a Redistribution Limit of Maximum-Prefixes Imported

For detailed information about this feature (which is also known as the OSPF Limit on Number of Redistributed Routes feature), see the following Cisco document:

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

OSPF Link State Database Overload Protection

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/ospfopro.htm

OSPF Per-Interface Link-Local Signaling (LLS)

For detailed information about this feature (which is also known as the OSPF Link-local Signaling (LLS) Per Interface Basis feature), see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/ospflls.htm

OSPF Sham-Link Support for MPLS VPN

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/shamlink.htm

OSPF Shortest Paths First Throttling

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/fsspftrl.htm

OSPF Stub Router Advertisement

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/fsospfau.htm

OSPF Support for Fast Hellos

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/fasthelo.htm

OSPF Support for Forwarding Adjacencies over MPLS Traffic Engineered Tunnels

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/120s24/ospffa.htm

OSPF Support for Link State Advertisement (LSA) Throttling

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/120s25/fsolsath.htm

OSPF Support for Multi-VRF on CE Routers

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/ospfvrfl.htm

OSPF Support for Unlimited Software VRFs per Provider Edge (PE) Router

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/gtospfvf.htm

OSPF Update Packet-Pacing Configurable Timers

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/fsospfct.htm

Per-Packet Load Balancing (PPLB)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/pplb.htm

PIM MIB Extension for IP Multicast

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/fs_pmmib.htm

PIM Multicast Scalability

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.

Post-Switchover Core Dump

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/coredump.htm

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_pwef.htm

QoS Features

Cisco IOS Release 12.2(27)SBB supports the following quality of service (QoS) features that are documented in the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

- 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)
- Configurable per ATM-VC Hold Queue Size
- Diffserv Compliant WRED
- Enhanced Random Early Detection (RED) Statistics
- Hierarchical Input Policing
- MLPPP with Link Fragmentation Interleave (LFI)
- Link Fragmentation Interleave over Frame Relay (FRF.12)
- Low Latency Queueing (LLQ)
- Low Latency Queueing (LLQ) for Frame Relay
- Modular QoS CLI (MQC)
- Policy Map Scaling
- Priority Queueing (PQ)
- QoS for Virtual Private Networks
- QoS Packet Marking
- QoS Policy Propagation via Border Gateway Protocol (QPPB)
- Random Early Detection (RED)
- Random Early Detection (RED) with Queue-Limit
- Three Color Policer
- Three-Level Policy Maps
- Two-Rate Policer (this feature may also be known as Dual Rate Three Color Policer)
- VC Oversubscription
- Weighted RED (WRED)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/10000_c/10kqos.pdf

In addition, Cisco IOS Release 12.2(27)SBB supports the following QoS features.

Modular QoS CLI (MQC)-Based Frame Relay Traffic Shaping

The Modular QoS CLI (MQC)-based Frame Relay Traffic Shaping feature provides users the ability to configure Frame Relay Traffic Shaping (FRTS) by using MQC commands.

QoS: Enhanced Show Commands for Active Policies

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_acpm.htm

Route Processor Redundancy Plus (RPR+)

For detailed information about this feature, see the *Stateful Switchover* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_sso.htm

TCP Window Scaling

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbbtcpwn.htm

UDP Forwarding Support of IP Redundancy Virtual Router Group (VRG)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_udpv.htm

Using 31-Bit Prefixes on IPv4 Point-to-Point Links

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sb/122sbb27/sbb_u31a.htm

VPN Routing/Forwarding (VRF) ARP Entry Support

The VPN routing/forwarding (VRF) option in the Address Resolution Protocol (ARP) command enables you to configure static ARP entries per VRF.

[**no**] **arp** [*vrf name*] *ipaddr hardware-addr* {**arpa** | **sap** | **smds** | **snap**} [{*alias* | *interfaces*}]

Following is output from a configuration example:

```
Router(config)# arp?
A.B.C.D IP address of ARP entry
vrf Configure static ARP for a VPN Routing/Forwarding instance
Router(config)# arp vrf V4 ?
```

```
A.B.C.D IP address of ARP entry
Router(config)# arp vrf V4 20.1.1.1 0000.0000.0001 arpa
```

VPN Routing/Forwarding (VRF) CLI Command

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 is output 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
```

New Hardware Features in Cisco IOS Release 12.2(27)SBA1

Cisco IOS Release 12.2(27)SBA1 does not introduce new hardware features. For information about supported platforms, see the "Supported Hardware" section on page 5.

New Software Features in Cisco IOS Release 12.2(27)SBA1

This section describes new and changed features in Cisco IOS Release 12.2(27)SBA1. 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(27)SBA1. 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 Cisco IOS Release 12.2(27)SBA1 for the Cisco 7500 series routers supports all features that were introduced in Cisco IOS Release 12.2(27)SBA. For information about these features, see the "New Software Features in Cisco IOS Release 12.2(27)SBA" section on page 36.

Any Transport over MPLS (AToM): Sequencing Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaatom.htm

Distributed LFI/dQoS over Leased Lines

For detailed information about this feature, see the *Distributed Link Fragmentation and Interleaving over Leased Lines* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbadlfi2.htm

L2VPN FR FECN/BECN Marking

For detailed information about this feature, see the *BECN and FECN Marking for Frame Relay over MPLS* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbafecn.htm

L2VPN Pseudowire Switching

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbpseudo.htm

Layer 2 Local Switching: SSO/NSF Support for Ethernet to Ethernet VLAN Interworking

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbalocal.htm

Multi-VRF Support (VRF Lite)

For detailed information about this feature (which is also known as the MPLS Multi-VRF (VRF-lite) feature), see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/vrflite.htm

New Hardware Features in Cisco IOS Release 12.2(27)SBA

Cisco IOS Release 12.2(27)SBA does not introduce new hardware features. For information about supported platforms, see the "Supported Hardware" section on page 5.

New Software Features in Cisco IOS Release 12.2(27)SBA

This section describes new and changed features in Cisco IOS Release 12.2(27)SBA. 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(27)SBA. 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.

AAA Features

Cisco IOS Release 12.2(27)SBA introduces the following AAA features.

AAA Double Authentication Secured by Absolute Timeout

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_dasat.htm

AAA Per-User Scalability

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbarfaaa.htm

AAA-PPP-VPDN Non-Blocking

Previously, Cisco IOS software created a statically configurable number of processes to authenticate calls. Each of these processes 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 will not limit the rate of call handling.

Accounting of VPDN Disconnect Cause

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. These eight disconnect-cause codes 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/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fappendx/scgrdat3.htm

ATM Multilink PPP Support on Multiple VCs

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaatmml.htm

ATM OAM Features

Cisco IOS Release 12.2(27)SBA introduces the following ATM OAM features:

ATM OAM Ping

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbatmpng.htm

ATM OAM Support for F5 Continuity Check

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbamcc.htm

ATM OAM Traffic Reduction

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbmoam.htm

Attribute Filtering Per-Domain and VRF Aware Framed-Routes

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbarfaaa.htm

Attribute Screening for Access Requests

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_asfar.htm

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbauto2.htm

Bridged 1483 Encapsulated Traffic over ATM SVCs

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbridge.htm

Byte-Based Weighted Random Early Detection

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbasbyte.htm

DHCP Features

Cisco IOS Release 12.2(27)SBA introduces the following DHCP features.

DHCP Accounting

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbadhpca.htm

DHCP Address Allocation Using Option 82

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbcpopt.htm

DHCP Client Dynamic Subnet Allocation API

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 Client on WAN Interfaces

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaandhp.htm

DHCP—Configurable DHCP Client

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbhcpcf.htm

DHCP Enhancements for Edge-Session Management

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaiedge.htm

DHCP Lease Limit per ATM RBE Unnumbered Interface

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbahcpls.htm

DHCP Lease Query Command

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_leas.htm

DHCP ODAP Server Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaodaps.htm

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

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/ios122s/122snwft/release/122sba27/sbandhcp.htm

DHCP Option 82 Support for Routed Bridge Encapsulation

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbarbeo.htm

DHCP Relay—MPLS VPN Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbahmpls.htm

DHCP Relay Subscriber Identifier Suboption

For detailed information about this feature, see the *DHCP—Subscriber Identifier Suboption of Option82* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_opt82.htm

DHCP Release and Renew CLI in EXEC Mode

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbahcprr.htm

DHCP Secured IP Address Assignment

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbasiaa.htm

DHCP Server—Import All Enhancement

When you enter the **import all** DHCP pool configuration command, the DHCP Server—Import All Enhancement feature allows options that are imported by one subsystem to coexist with options that are imported from another subsystem. When the session is terminated or the lease is released, the imported options are cleared from the DHCP server database.

DHCP Server—On-Demand Address Pool Manager

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbandhcp.htm

DHCP Server—Option to Ignore All BOOTP Requests

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbootp.htm

DHCP—Static Mapping

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbhcpsm.htm

DHCP—Statically Configured Routes Using a DHCP Gateway

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/ddgtwy.htm

DHCPv6 Prefix Delegation via AAA

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

A client locates a DHCP server 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 IPv6 Addressing and Basic Connectivity* document:

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

Dialer CEF

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbadlrce.htm

Distributed Management Event MIB Conformance to RFC 2981

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbbpr2.htm

Dynamic DNS Support for Cisco IOS Software

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_ddns.htm

Dynamic Per VRF AAA

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbarfaaa.htm

Enable Multilink PPP via RADIUS for Preauthentication User

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbapprad.htm

Enabling OSPFv2 on an Interface Using the ip ospf area Command

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/ospfarea.htm

Encrypted Vendor-Specific Attributes

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbancvsa.htm

Enhanced Test Command

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaaacmd.htm

Framed-Route in RADIUS Accounting

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_fra22.htm

Improved show commands for MLP-ATM LFI

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/ios122s/122snwft/release/122sba27/sbrmlp.htm

Intelligent Service Architecture (ISA) Features

Cisco IOS Release 12.2(27)SBA introduces the following Intelligent Service Architecture (ISA) features for the Intelligent Service Gateway (ISG):

- ISA: Accounting: Per Session, Service & Flow
- ISA: Accounting: Postpaid
- ISA: Accounting: Prepaid
- ISA: Accounting: Tariff Switching

- ISA: Flow Control: Flow Redirect (L4, Captive Portal)
- ISA: Flow Control: QoS Control: Dynamic Rate Limiting
- ISA: Instrumentation: Advanced Conditional Debugging
- ISA: Instrumentation: Session & Flow Monitoring (local and external)
- ISA: Network Interface: IP Routed, VRF Aware MPLS
- ISA: Network Interface: Tunneled (L2TP)
- ISA: Policy Control: Cisco Policy Language
- ISA: Policy Control: DHCP Proxy
- ISA: Policy Control: Multidimensional Identity per Session
- ISA: Policy Control: Policy: Domain Based (Auto-domain)
- ISA: Policy Control: Policy Server: CoA (QoS, L4 Redirect, User ACL, TimeOut)
- ISA: Policy Control: Policy Server: SSG-SESM Protocol
- ISA: Policy Control: Policy: Triggers: Duration
- ISA: Policy Control: Service Profiles
- ISA: Policy Control: User Profiles
- ISA: Session: Auth: PBHK
- ISA: Session: Auth: Single Sign On
- ISA: Session: Authentication (MAC, IP, EAP)
- ISA: Session: Creation: Interface IP Session: L2
- ISA: Session: Creation: Interface IP Session: L3
- ISA: Session: Creation: IP Session: Protocol Event (DHCP)
- ISA: Session: Creation: IP Session: Subnet & Source IP: L2
- ISA: Session: Creation: IP Session: Subnet & Source IP: L3
- ISA: Session: LifeCycle: Idle Timeout
- ISA: Session: LifeCycle: POD
- ISA: Session: Multi-Service Creation and Flow Control
- ISA: Session: VRF Transfer

For detailed information about these features, see the *Intelligent Service Architecture Configuration Guide* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/isa/index.htm

IPv6 Access Services: DHCPv6 Prefix Delegation

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 any dynamic state for individual clients, such as DNS server addresses and domain search list options.

For more information, see the *Implementing IPv6 Addressing and Basic Connectivity* document:

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

ISDN Backup in MPLS Core

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbasdnbk.htm

L2TP and L2TPv3 Features

Cisco IOS Release 12.2(27)SBA introduces the following L2TP and L2TPv3 features.

L2TP Dial-Out Load Balancing and Redundancy

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbl2tlbr.htm

L2TP Extended Failover

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba2tpef.htm

L2TP Redirect

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba2tpmr.htm

L2TP Security

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba2tsec.htm

L2TP Tunnel Connection Speed Labeling

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbalabel.htm

L2TPv3 Control Message Hashing

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/ios122s/122snwft/release/122sba27/sba_l2v3.htm

L2TPv3 Control Message Rate Limiting

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/ios122s/122snwft/release/122sba27/sba_l2v3.htm

Protocol Demultiplexing for L2TPv3

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/ios122s/122snwft/release/122sba27/sba_l2v3.htm

L2VPN Pseudowire Redundancy

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbpseudo.htm

Layer 2 Local Switching: SSO/NSF Support for Frame Relay to Frame Relay

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbalocal.htm

Layer 2 VPN: Syslog, SNMP Trap and Show Command Enhancements for AToM and L2TPv3

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/ios122s/122snwft/release/122sba27/sba_l2v3.htm

Low Latency Queueing with Priority Percentage Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sballqpc.htm

MLP LFI over ATM Configuration Scaling

For detailed information about this feature, see the *Link Fragmentation and Interleaving for Frame Relay and ATM Virtual Circuits* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbamlatm.htm

MPLS Features

Cisco IOS Release 12.2(27)SBA introduces the following MLPS features.

MPLS—LDP AutoConfiguration

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbadpaut.htm

MPLS—LDP MD5 Global Configuration

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_md5.htm

MPLS—LDP Session Protection

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaespro.htm

MPLS QoS—DiffServ Tunnel Mode Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbadftnl.htm

MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_xnlb.htm

MS-CHAP Version 2

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaschap.htm

Multilink PPP Minimum Links Mandatory

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbamlppp.htm

Offload Server Accounting Enhancement

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaffact.htm

Packet Classification Using the Frame Relay DLCI Number

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbalc26i.htm

peer pool backup Command

For detailed information about this feature, see the *Peer Pool Backup* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaeerpl.htm

Per VRF AAA

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbarfaaa.htm

Policer Enhancement: Multiple Actions

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbamu26s.htm

PPP MLP MRRU Negotiation Configuration

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbapmrru.htm

PPPoE Features

Cisco IOS Release 12.2(27)SBA introduces the following PPPoE features.

PPPoA/PPPoE Autosense for ATM PVCs

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_auto.htm

PPPoE Client DDR Idle Timer

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbpecls.htm

PPPoE Connection Throttling

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbppthr.htm

PPPoE Relay

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbppoer.htm

PPPoE Server Restructuring and PPPoE Profiles

For detailed information about this feature, see the *PPPoE Profiles* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbpprfls.htm

PPPoE Service Selection

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbpoess.htm

PPPoE Session Limit

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_ppesl.htm

PPPoE Session Limit per NAS Port

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/12sb_nas.htm

PPPoE Session Recovery After Reload

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbpprec.htm

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_pwef.htm

QoS Features

Cisco IOS Release 12.2(27)SBA introduces the following QoS features.

QoS: ATM Cell-Based Policer

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbafscbp.htm

QoS: ATM-CLP and Layer 2 CoS-Based WRED

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaswred.htm

QoS: Broadband Aggregation Enhancements, Phase 1

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/qos/index.htm

QoS: CBQoSMIB Parity Across Cisco IOS Release 12.0S, 12.2SB, and 12.3T

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/ios122s/122snwft/release/122sba27/sbafscbp.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/ios122s/122snwft/release/122sba27/sbaswred.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. The packet color classification 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/ios122s/122snwft/release/122sba27/sba_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 URLs:

  - http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftllqpct.htm
  - 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/ios122s/122snwft/release/122sba27/sbapctpg.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/ios122s/122snwft/release/122sba27/sbapctsg.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/ios122s/122snwft/release/122sba27/sbawrdql.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 CBQoSMIB and the MIB objects and tables listed above, 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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_cap.htm

QoS: Frame Relay QoS Hierarchical Queueing Framework Support on the Cisco 7200 Series Router

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_fhqf.htm

QoS: Match on ATM CLP

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbamcatm.htm

QoS: Percentage-Based Policing

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbapctpg.htm

QoS: Percentage-Based Shaping

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbapctsg.htm

QoS: Percentage-Based and Time-Based Policing Parameters

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbapbtbp.htm

QoS: Per-Session Shaping and Queuing on LNS

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/fsbpssq.htm

QoS: Time-Based Thresholds for WRED and Queue Limit

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbawrdql.htm

QoS: Tunnel Marking for L2TPv3 Tunnels

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbatnlmk.htm

RADIUS Features

Cisco IOS Release 12.2(27)SBA introduces the following RADIUS features.

RADIUS Centralized Filter Management

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbftrmn.htm

RADIUS EAP Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/eaprad.htm

RADIUS Logical Line ID

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbineid.htm

RADIUS NAS-IP-Address Configurability

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbsiara.htm

RADIUS Progress Codes

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbatr196.htm

RADIUS Route Download

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbadrou.htm

RADIUS Server Load Balancing

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/rd_ldbal.htm

RADIUS Server Reorder on Fail

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbrsrof.htm

RADIUS Timeout Set During Pre-Authentication

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbattr27.htm

RADIUS Tunnel Preference for Load Balancing and Fail-Over

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbradtun.htm

RADIUS VC Logging

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/rad_log.htm

RADIUS Attributes

Cisco IOS Release 12.2(27)SBA introduces the following RADIUS attributes.

Connect-Info RADIUS Attribute 77

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 each customer gets from his or her session.

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_ra5f.htm

RADIUS Attribute 52 and 53 Gigaword Support

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

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbrada82.htm

RADIUS Attribute 91 Encrypted and Tagged VSA Support

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/6400/64_24b6.htm#115840

RADIUS Attribute 104

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_ra104.htm

RADIUS Attribute Value Screening

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_ras.htm

RFC-2867 Tunnel Accounting

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_tnact.htm

Session Limit Per VRF

For detailed information about this feature (which is also known as the Session Limit per VPDN Template feature), see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_vrf.htm

Subscriber Service Switch

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_sss.htm

TCP MSS Adjustment

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sb_admss.htm

Timer and Retry Enhancements for L2TP and L2F

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbetreh.htm

Tunnel Authentication via Radius on LNS

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/ios122s/122snwft/release/122sba27/sbanauth.htm

Two-Rate Policer

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaplc26.htm

Virtual Sub-Interface

For detailed information about this feature, see the *Configuration Enhancements for Broadband Scalability* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbabbenh.htm

Virtual Template Interfaces Limit Expansion

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sba_vtle.htm

VLAN ID Rewrite

For detailed information about this feature, see the *Any Transport over MPLS* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaatom1.htm

VPDN Features

Cisco IOS Release 12.2(27)SBA introduces the following VPDN features.

Shell-Based Authentication of VPDN Users

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbxvpnt.htm

VPDN Default Group Template

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbaevpdn.htm

VPDN Group Session Limiting

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbapdngs.htm

VPDN Multihop by DNIS

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbamhopd.htm

VPN MIB Enhancements for per-VRF Session Counting

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). The 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 the 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 using GET requests or consecutively using repeated GET-NEXT requests.

VRF-Aware VPDN Tunnels

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbapdnmh.htm

VPN Tunnel Management

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/sbapnmng.htm

VRF-Autoclassify

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/vrfauto.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 restriction in Cisco IOS Release 12.2SB that can apply to the Cisco 7200 series routers, Cisco 7301 router, Cisco 7500 series routers, and Cisco 10000 series routers.

Limitations and Restrictions in Cisco IOS Release 12.2(27)SBB

This section describes limitations and restrictions in Cisco IOS Release 12.2(27)SBB and later releases.

System Limits for Policy Maps on Cisco 10000 Series Routers

The maximum number of classes supported per policy map on a Cisco 10000 series router in Cisco IOS Release 12.2(27)SBB is 64. The maximum number of policy maps supported per system is 4096.

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 exceeds 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.

Limitations and Restrictions in Cisco IOS Release 12.2(27)SBA

This section describes limitations and restrictions in Cisco IOS Release 12.2(27)SBA and later releases.

SNMP Version 1 BGP4-MIB Limitations

You may notice incorrect BGP trap OID output when you use the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). The problem is not due to any error with Cisco IOS software. This problem occurs because the BGP4-MIB does not follow RFC 1908 rules regarding version 1 and version 2 trap compliance. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2SB that can apply to the Cisco 7200 series routers, Cisco 7301 router, Cisco 7500 series routers, an 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.
- *What's New for IOS—What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in to Cisco.com and selecting **Support**: **Software Downloads**: **Cisco IOS Software**: **What's New for IOS**.

Important Notes for Cisco IOS Release 12.2(27)SBB5

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(27)SBB5 and later releases.

Logging of an Informational Message when a Terminal State is Reached [CSCsd64437]

As of Cisco IOS Release 12.2(37)SBB5, a router will log an informational message when it has reached a terminal state for Route Processor Redundancy (RPR), RPR Plus (RPR+), or Stateful Switchover (SSO). A terminal state is reached when the router has finished progressions for all its clients for one operational mode (that is, for RPR, RPR+, or SSO) and remains in this state. The logging of an informational message means that you no longer have to enter the **show redundancy states** command to determine if the router has reached a terminal state.

Important Notes for Cisco IOS Release 12.2(27)SBB

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(27)SBB and later releases.

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/partner/products/hw/routers/ps133/products_tech_note09186a00800a7b80.shtml

If you need assistance with the buffer tuning process, call your support team.

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:

Release 12.2(27)SBB and its rebuilds:

Release 12.2(27)SBA and its rebuilds:

Resolved Caveats—Cisco IOS Release 12.2(27)SBB9

Cisco IOS Release 12.2(27)SBB9 is a rebuild release for Cisco IOS Release 12.2(27)SBB. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBB but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsb14026

  Symptoms: A standby RSP reloads continuously.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for SSO and that has the **snmp mib notification-log default** command enabled.

  Workaround: Disable the **snmp mib notification-log default** command.

- CSCsg39295

  Symptoms: Password information may be displayed in a Syslog message as follows:

  ```
  %SYS-5-CONFIG_I: Configured from scp://userid:password@10.1.1.1/config.txt by
  console
  ```

  Conditions: When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, selection of ConfigCopyProtocol of SCP or FTP may result in the password being exposed in a syslog message.

  Workaround: When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, use the ConfigCopyProtocol of RCP to avoid exposure of the password.

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

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml.

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

- 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.

Miscellaneous

- CSCdz55178

  Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

  Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                         00000000011111111111222222222333^
                         12345678901234567890123456789012|
                                                          |
                                                      PROBLEM
                                                    (Variable Overflowed).
```

  Workaround: Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- CSCeb21064

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCeb69473

  Symptoms:Device crashes with a segmentation violation (SegV) exception.

  Conditions: Issuing the **connect** *target_ip* **[login|513] /terminal-type** *value* command with a large input parameter to the "/terminal-type" argument such as the following:

```
router>connect 192.168.0.1 login /terminal-type aaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Trying 192.168.0.1...Open
login:

*** System received a SegV exception ***
signal= 0xb, code= 0x1100, context= 0x82f9e688
PC = 0x61616160, Vector = 0x1100, SP = 0x833ae5a8
```

  Workarounds:

  AAA Authorization—AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it.

  For a complete description of authorization commands, refer to the following links:

  Configuring Authorization

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part05/schathor.htm

  ACS 4.1 Command Authorization Sets

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/SPC.html#wpxref9538

  ACS 4.1 Configuring a Shell Command Authorization Set for a User Group

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/GrpMgt.html#wp480029

Role-Based CLI Access—The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views

restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices. The following link provides more information about the Role-Based CLI Access feature:

Role-Based CLI Access

http://www.cisco.com/en/US/netsol/ns696/networking_solutions_white_paper09186a00801ee18d.shtml

Device Access Control—Due to the nature of this vulnerability, networking best practices such as access control lists (ACLs) and Control Plane Policing (CoPP) that restrict vulnerable device access to certain IP addresses or Subnetworks may not be effective. Device access best practices provide some mitigation for these issues by allowing systemic control of authenticated and unauthenticated users. Device access best practices are documented in:

Infrastructure Protection on Cisco IOS Software-Based Platforms Appendix B-Controlling Device Access

http://www.cisco.com/application/pdf/en/us/guest/products/ps1838/c1244/cdccont_0900aecd804ac831.pdf

Improving Security on Cisco Routers

http://www.cisco.com/warp/public/707/21.html

- CSCej69560

  Symptoms: Packet loss may occur on an MLP interface.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 24-port channelized E1/T1 line card when one of the interfaces in the bundle flaps very quickly or after a PRE switchover has occurred.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MLP interface.

- CSCek65070

  Symptoms: CRC, Frame, Abort errors and link flaps are seen on E1 and T1 interfaces.

  Conditions: This issue is seen on the Cisco 10000 series router that has a 4- port Channelized OC-3 or 1-port Channelized OC-12 line card. The configuration on the line card includes SDH or SONET E1 or T1 interfaces, some of which are not in use and not connected to anything on the far end.

  Workaround: The issue is triggered by having unterminated interfaces configured on the card. To prevent the issue from happening, any unused E1 or T1 interfaces should either be removed from the router configuration or at least set to clock source internal. This will reduce the chances that the interfaces that are in use will flap.

- 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.

- CSCin86298

  Symptoms: Use of Mini ACLs that are based on TCP flags sometimes produces different behavior to normal ACLs on some platforms.

  Conditions: For example, the In acesslist "access-list 101 permit tcp host 11.0.0.1 host 12.0.0.2 established is blocking the telnet from 12.0.0.2 (Refelector) to 11.0.0.1(Generator)," when these syn-ack packets should be permitted as established ones.

  Workaround: There is no workaround.

- CSCsb11124

  The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  Cisco has published a Security Advisory on this issue; it is available at http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml

- CSCsb12598

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

  Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd81407

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

  Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml.

- 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

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

Cisco is providing fixed software to address this issue. 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-20080326-IPv4IPv6.shtml.

- 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.

- 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.

- CSCsg15342

  Cisco 10000, uBR10012 and uBR7200 series devices use a User Datagram Protocol (UDP) based Inter-Process Communication (IPC) channel that is externally reachable. An attacker could exploit this vulnerability to cause a denial of service (DoS) condition on affected devices. No other platforms are affected.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-ipc.shtml.

- CSCsg17957

  Symptoms: A router may crash when forwarding an IP fragment.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(28)SB3 and that is configured for L2TP and QoS. Note that the symptom is not release-specific.

  Workaround: Remove the QoS configuration. If this is not an option, there is no workaround.

- CSCsg40567

  Symptoms: Malformed SSL packets may cause a router to leak multiple memory blocks.

  Conditions: This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

  Workaround: Disable the **ip http secure server** command.

- CSCsg70474

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsg96319

  Symptoms: When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the **ssh -l** *userid* **:***number ip-address* command.

  Conditions: This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:

  http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804831b6.html

  Workaround: Configure reverse SSH by entering the **ip ssh port** *portnum* **rotary** *group* command. This configuration is explained at the following URL:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

- 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.

- 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.

- 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.

- CSCsh47740

  Symptoms: In an ATM pseudowire configuration, when you reset a line card by entering the **hw-module slot** *slot-number* **reset** command, the pseudowire comes back up but the traffic does not resume, and an end-to-end ping fails.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the line card that was reset.

- CSCsh69969

  Symptoms: The rate in the output of the **show ip mroute active** command shows twice the number of packets per second.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsh83575

  Symptoms: After you have performed an In Service Software Upgrade (ISSU) from Cisco IOS Release 12.2(27)SBB8 and then enter the **issu** runversion command, all line cards may go down and can no longer be accessed.

  Conditions: The symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB8 when you attempt to upgrade to a Cisco IOS software image that contains the fix for CSCek67713.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCek67713. 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.

- CSCsh91746

  Symptoms: After creating T1 links on a channelized STM-1 interface, you cannot access the associated interfaces in global configuration mode or Exec mode.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Creating a new interface may clear the condition. If it does not, reload the router.

- CSCsi60004

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)

- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

TCP/IP Host-Mode Services

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

  Conditions: This symptom is seen under the following conditions:

  - The router must have RCP enabled.
  - The packet must come from the source address of the designated system configured to send RCP packets to the router.
  - The packet must have a specific data content.

  Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

- CSCsh04686

  Symptoms: With X25 over TCP (XOT) enabled on a router or catalyst switch, malformed traffic sent to TCP port 1998 will cause the device to reload. This was first observed in IOS 12.2(31)SB2.

  Conditions: Must have “x25 routing” enabled on the device.

  Workarounds: Use IPSEC or other tunneling mechanisms to protect XOT traffic. Also, apply ACLs on affected devices so that traffic is only accepted from trusted tunnel endpoints.

- CSCsh75069

  Symptoms: A router interface stops forwarding traffic when it receives traffic to the UDP echo port (port 7) addressed to the interface itself.

  Conditions: An input queue wedge condition exists in handling UDP traffic that is destined for the echo service.

  Workaround: Disable the UDP echo service with the **no udp-small- servers** configuration command.

Resolved Caveats—Cisco IOS Release 12.2(27)SBB8

Cisco IOS Release 12.2(27)SBB8 is a rebuild release for Cisco IOS Release 12.2(27)SBB. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBB8 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCin93236

  Symptoms: The CPU usage of the TACACS+ process may be high.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCeh31423. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh31423. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- 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.

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

IP Routing Protocols

- CSCse86806

  Symptoms: A Cisco router that has BGP neighbors that have the **neighbor default-originate** command enabled may not re-advertise the default route to these neighbors.

Conditions: This symptom is observed after a soft clear is applied to the outbound sessions or after a route refresh request has been received.

Workaround: Disable and re-enable the **neighbor default-originate** command on the affected BGP neighbors to force a default route to be sent to the affected BGP neighbors.

- 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.

Miscellaneous

- CSCeh87115

  Symptoms: The PXF engine may stall when PIM multicast traffic passes over MLP links.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCei05676

  Symptoms: When CDP is enabled or disabled on an interface of a 1-port Gigabit Ethernet half-height line card (ESR-HH-1GE), the interface goes down and back up again, causing traffic to be interrupted for up to 5 seconds.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCei47316

  Symptoms: A spurious memory access is generated when you configure WRED for a user-defined traffic class without a queue (that is, a traffic class without bandwidth, priority, and a shape action).

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Do not configure WRED in a traffic class without a queue.

- CSCsa87316

  Symptoms: A router may unexpectedly reload when you enter the **interface atm** *slot* **/ ima** *group-number* interface configuration command for a previously removed IMA group.

  Conditions: This symptom is observed on a Cisco router that is configured for QoS.

  Workaround: Do not enter the **interface atm** *slot* **/ ima** *group-number* interface configuration command for a previously removed IMA group.

- CSCsb44306

  Symptoms: The PXF engine may crash when you configure Link fragmentation and interleaving (LFI) on an interface with Frame Relay Fragmentation (FRF12). After the PXF engine has automatically recovered, some interfaces do not come up. You must perform a PRE switchover to enable all interfaces to come up.

Conditions: This symptom is observed on a Cisco 10000 series when traffic passes through the LFI interface and when the following events occur:

1. You enable Frame Relay traffic shaping on the main interface.
2. You disable Frame Relay traffic shaping on the main interface.
3. You remove the Frame Relay class from the subinterface.

Workaround: There is no workaround.

- CSCsb57868

  Symptoms: The following error message and a traceback may be generated after an SSO switchover or an In-Service Software Upgrade (ISSU) operation:

  ```
  %IPC-4-NOPORT: Port Not Found
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs that function in SSO mode and that runs Cisco IOS Release 12.2(27)SBB or a rebuild of Release 12.2(27)SBB. The symptom is more likely to occur with a heavily-configured router with a large number of interfaces and subinterfaces.

  Workaround: There is no workaround.

  Further Problem Description: The caveat is closed because the issue is purely cosmetic and does not impact performance in any way. There is no impact on the switchover or upgrade operation. Traffic through the router is unaffected.

  The message occurs because of a race condition between the RP and a line card during an HA switchover.

  The symptom does not occur in Cisco IOS Release 12.2(28)SB or later releases.

- CSCsb81721

  Symptoms: When you initiate an SSO switchover via the CLI, the standby PRE reloads continuously.

  Conditions: This symptom is observed on a Cisco 10000 series after a couple of manual switchovers.

  Workaround: There is no workaround.

- CSCsc42260

  Symptoms: When you delete a Frame-Relay PVC and redefine it, the available bandwidth that is left in the class-default queue may be miscalculated.

  Conditions: This symptom is observed on a Cisco 10000 series when you delete and redefine the same Frame-Relay PVC that has a nested output policy.

  Workaround: There is no workaround.

- CSCsd09382

  Symptoms: On an interface with an output policy, traffic is forwarded via FIFO queueing instead of class-based queueing.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsd11646

  Symptoms: On a router that runs Multiprotocol Label Switching (MPLS), the "%SYS-3-OVERRUN:" and "%SYS-6-BLKINFO" error messages may be generated and a software-forced crash may occur on the router.

Conditions: This symptom is observed when you enter the **show mpls ldp discovery** command under the following condition:

- There are multiple LDP adjacencies configured through one interface.
- The adjacencies between peers through this interface have not been fully established for some peers.
- The unestablished LDP adjacencies are coming while you enter the **show mpls ldp discovery** command.

Workaround: Do not enter the **show mpls ldp discovery** command while multiple LDP adjacencies are coming up. Rather, enter the **show mpls ldp neighbor** [**detail**] command while multiple LDP adjacencies are coming up.

- CSCsd33706

  Symptoms: When you enter the **no card** command for a 1-port Gigabit Ethernet half-height line card (ESR-HH-1GE), the configuration is not properly removed. When you enter the **card** command for the ESR-HH-1GE, all the subinterfaces that were supposed to be removed come back up.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsd36608

  Symptoms: A memory leak may occur in the interprocess communications (IPC) when a line card is reset.

  Conditions: This symptom is observed on a Cisco router that is configured for In Service Software Upgrade (ISSU).

  Workaround: There is no workaround.

- CSCsd57350

  Symptoms: When you change the shape value of a parent policy, traffic shaping may not function properly.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: After you have changed the shape value of the parent policy, remove and reapply the policy to the interface.

  Alternate Workaround: Remove the policy from the interface, change the shape value of the parent policy, and then re-attach the policy to the interface.

- CSCsd87526

  Symptoms: Traffic loss may occur during an APS cutover on a 4-port channelized STM-1/OC-3 line card.

  Conditions: This symptom is observed on a Cisco 10000 series after you have entered the **hw-module slot** *slot-number* **reset** command for the slot in which the 4-port channelized STM-1/OC-3 line card is installed.

  Workaround: There is no workaround.

- CSCse45180

  Symptoms: On Cisco 10000 that functions in a QoS environment, the computed default queue limit may be smaller than what you would expect.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 and that is configured with high-speed interfaces (that is, interfaces with a speed that is greater than 500 Mb).

Workaround: Explicitly configure the desired value via the **queue-limit** *number-of-packets* command.

- CSCse49188

  Symptoms: When you reconfigure an ATM PVP, inconsistencies may occur between the primary PRE and secondary PRE, causing the secondary PRE to reload and resynchronize with the primary PRE.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround. However, the reload of the secondary PRE has a minimal impact on the functionality of the router.

- CSCse68138

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsf29482

  Symptoms: A router may crash when you configure an output service policy for multilink interfaces that are in the down state.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Ensure that the multilink interfaces are in the up state before you configure an output service policy for the multilink interfaces.

- 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.

- CSCsg28133

  Symptoms: An LDP adjacency is not formed on a dot1q Gigabit Ethernet interface.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PREs when you enter the **issu runversion** to upgrade from Cisco IOS Release 12.2(27)SBB5 to Release 12.2(27)SBB7 or when you enter the **issu abortversion** command to downgrade from Release 12.2(27)SBB7 to Release 12.2(27)SBB5. Other releases could be affected too.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

Wide-Area Networking

- 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.

- 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.

- 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(27)SBB7

Cisco IOS Release 12.2(27)SBB7 is a rebuild release for Cisco IOS Release 12.2(27)SBB. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBB7 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsb11698

  Symptoms: Certain UDP packets that are directed at a TACACS port may become stuck in the interface queue.

  Conditions: This symptom is observed on a Cisco platform that is configured for AAA.

  Workarounds: When the symptom has occurred, you can increase the interface input hold queue to allow additional traffic to pass temporarily, but this is not a complete workaround. To prevent the symptom from occurring, create and apply an interface ACL, infrastructure ACL, or receive ACL to deny the UDP packets that have as destination the TACACS port (49) from entering the interface queue.

- CSCsc50986

  Symptoms: Network Time Protocol (NTP) unsynchronizes when NTP reply packets arrive out of order during synchronization of the system clock with an NTP server.

  Conditions: This symptom is observed when two NTP servers are used for time synchronization and when there is a difference of more than one minute between the clocks of the NTP servers. Initially the NTP client synchronizes with an NTP server. However, when the NTP client attempts to synchronize the system clock and the packets arrive out-of-order from corresponding NTP servers, NTP enters into the loop and no longer resynchronizes.

  Workaround: Configure a single NTP server.

Interfaces and Bridging

- CSCeb76005

  Symptoms: A Cisco router may reload unexpectedly when you enter the **no encapsulation frame-relay** interface configuration command for an interface.

  Conditions: This symptom is observed when the interface is configured for interface fragmentation and payload compression.

  Workaround: Configure the interface for map-class fragmentation.

- CSCsb82231

  Symptoms: A router may crash in response to a dot1q packet on an ATM subinterface or in response to a dot1q packet on VLAN 0 on a Gigabit Ethernet interface that is configured with dot1q subinterfaces.

  Conditions: This symptom is observed irrespective of whether or not the router is configured for dot1q encapsulation.

  Workaround: There is no workaround.

Miscellaneous

- CSCee13430

  Symptoms: A router may reload when you reconfigure a channel group.

  Conditions: This symptom is observed only when you enable a service policy on a serial interface before you reconfigure the channel group.

  Workaround: Remove the service policy before you reconfigure the channel group.

- CSCsc99111

  Symptoms: The following QoS configuration commands fail to complete, causing the platforms that they are running on to hang:

  – the **policy-map** command, including any commands in submodes under the **policy-map** command.

  – the **class-map** command, including any commands in submodes under the **class-map** command.

  – the **service-policy** command.

Conditions: This symptom is observed when the **show policy-map interface** command is run before the QoS configuration command is entered and when either one of the following conditions is present:

- The **show policy-map interface** command includes the *input* argument and only an output service policy is present on the interface.
- The **show policy-map interface** command includes the *output* argument and only an input service policy is present on the interface.

Workaround: There is no workaround. To prevent the symptom from occurring, enter the **show policy-map interface** command without the *input* or *output* argument. Doing so displays all service policies that are attached to the interface. Input and output policies are labeled as such in the command output.

Further Problem Description: Locks are used to control access to the QoS configuration database. This ensures that QoS **show** and configuration commands function against consistent views of the configuration data.

In the case of the **show policy-map interface** command, it is possible for the lock to be acquired but not released under the special case that is described in the Conditions section above. This situation occurs because of omissions in two error handling code paths that are triggered when a service policy is present only in the opposite direction from the direction that the **show policy-map interface** command requests.

Once the lock has been "orphaned" in this fashion, subsequent QoS configurations wait indefinitely for the lock to be released.

Other QoS **show** commands are not affected and continue to run normally.

- CSCsd76528

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: None of the policy classes after the first child policy of a hierarchical QoS policy take effect when you reload the router.

     Condition 1: This symptom is observed on a Cisco 7304 that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

     Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **service-policy output** interface configuration command to enable the child policies to take effect. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

  2. Symptom 2: On a Cisco 10000 series that is configured with hierarchical queueing policies, when you remove the **match vlan** command for a VLAN that matches a dot1q subinterface, the queues that are allocated to the subinterface are not cleared, allowing traffic to continue to flow through these queues.

     Condition 2: This symptom is observed on a Cisco 10000 series that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

     Workaround 2: There is no workaround. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

- 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.

- CSCse70934

  Symptoms: A Cisco 10000 series hat is configured for EoMPLS may not send packets over the EoMLPLS circuit.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB5 when the following sequence of events occurs:

  1. Create pseudowires on an ATM line card.
  2. Without removing the pseudowires, remove the ATM line card.
  3. Insert a half-height FE line card and a half-height GE line card.
  4. Enter the **no card** command.
  5. Create new pseudowires on the half-height FE line card and half-height GE line cards.

  This sequence of events causes the accurate number of AToM and local switching circuits on the controller to be miscounted, in turn, causing the promiscuous mode being disabled on the line cards, and preventing traffic from passing through.

  Workaround: Follow the correct sequence of events that includes unconfiguring the ATM line card:

  1. Create pseudowires on the ATM line card.
  2. Delete the PVCs and the pseudowires from the ATM line card.
  3. Remove the ATM line card.
  4. Enter the **no card** command to clear the remaining configuration on the ATM line card.
  5. Insert the half-height FE line card and half-height GE line card.
  6. Add the new pseudowire configuration.

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

Resolved Caveats—Cisco IOS Release 12.2(27)SBB6

Cisco IOS Release 12.2(27)SBB6 is a rebuild release for Cisco IOS Release 12.2(27)SBB. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBB6 but may be open in previous Cisco IOS releases.

Basic System Services

- 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.

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 12000 series when you delete a subinterface that processes traffic. The symptom may be platform-independent.

  Workaround: Shut down the subinterface before you delete it.

IP Routing Protocols

- CSCeh04837

  Symptoms: ARP entries may be purged unexpectedly.

  Conditions: This symptom is observed on a Cisco router when there is a large number of ARP entries and a Stateful Switchover (SSO) occurs.

  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.

- CSCsd92325

  Symptoms: The standby PRE may reload unexpectedly when you enter one of the following commands:

  - **no neighbor** *ip-address* **remote-as** *as-number*
  - **neighbor** *ip-address* **activate**

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB1 and that has PREs that are configured for RPR+.

  Workaround: There is no workaround.

Miscellaneous

- CSCea31603

  Symptoms: The entAliasMappingTable entries of the ENTITY-MIB are deleted for a preprovisioned line card that is inserted and then removed. Also, when the line card is re-inserted, the entAliasMappingTable entries do not return.

  Conditions: These symptoms are observed on a Cisco 10000 series and affects SNMP element managers that use the ENTITY-MIB to map the physical entity port to the Interface Index (ifIndex) via the entAliasMappingTable.

  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.

- CSCej32505

  Symptoms: Input and output rate counters that are displayed in the output of the **show interfaces** command may not be accurate or may be zero.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB and that is configured for CEF and SSO.

  Workaround: There is no workaround.

- CSCsa63173

  Symptoms: CEF may not be updated with a new path label that is received from a BGP peer.

  Conditions: This symptom is observed when a Cisco router that is configured for IPv4 BGP Label Distribution and multipath receives a BGP update that changes only the MPLS label to a non-bestpath multipath. In this situation, the router does not update the forwarding plane, causing dropping or misbranding of traffic because of label inconsistencies between the BGP table and the forwarding table.

  Workaround: There is no workaround.

- CSCsc40236

  Symptoms: Incorrect outgoing labels are installed for BGP-IPv4 Multipath prefixes.

  Conditions: This symptom has been observed anytime that a label changes from a BGP-IPv4 Multipath peer.

Workaround: Clearing the BGP neighbor should allow the correct labels to be installed.

- CSCsc60249

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

  Workaround: There is no workaround.

- CSCsc94359

  Symptoms: The BGP table and CEF forwarding table may have mismatched labels for prefixes that are learnt from a remote PE router.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when an eBGP session flap or route flap occurs on the remote PE router. A new label for the prefix is learnt from the remote PE router, but forwarding may not be updated properly.

  Workaround: There is no workaround. When the symptom has occurred, and to correct the situation, enter the **clear ip route vrf** *vrf-name network* command on the PE router that has mismatched labels.

- 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.

- CSCsd54157

  Symptoms: When you enter the **mpls ldp router-id loopback0 force** command, the router fails to use loopback0 as the local LDP router ID.

  Conditions: This symptom is observed on a Cisco router that has two loopback interfaces defined: loopback0 and loopback1. Loopback0 is reachable by other network nodes; loopback1 is not reachable by other network nodes. The symptom occurs under the following conditions:

  - The router has the **mpls ldp router-id loopback1 force** command enabled.
  - After you reload the router, the router uses loopback1 as the local LDP router ID, which can be verified in the output of the **show mpls ldp discovery** command.
  - When you enter the **mpls ldp router-id loopback0 force** command, the router fails to use loopback0 as the local LDP router ID.

  Workaround: Enter the **shutdown** command on the interface for loopback1.

  Alternate workaround: To avoid shutting down the interface for loopback1, after you have first entered the **mpls ldp router-id loopback1 force** command, enter the **mpls ldp router-id loopback0 force** command to enable the local LDP router ID to be changed to loopback0:0 and to enable the LDP session to come up.

- CSCsd62864

  Symptoms: You cannot remove a QoS class that has the **random-detect** command enabled and that is applied as an output service policy to an interface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB3.

  Workaround: Remove the queueing action from the class before you remove the class.

- 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.

- 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.

- CSCse11643

  Symptoms: Connectivity may go down and traffic may be lost on serial interfaces when the secondary card in an APS pair is reset.

  Conditions: This symptom is observed on a Cisco 10008 that is configured with a PRE2 and that runs Cisco IOS Release 12.2(27)SBB5.

  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.

TCP/IP Host-Mode Services

- 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.

- CSCsd92422

  Symptoms: The standby PR on a PE router may crash when you enter the **clear ip bgp *** command on the connected CE router.

  Conditions: The symptom is observed on a Cisco router that functions as a PE router when both the PE router and the CE router have the **bgp graceful-restart** command enabled.

  Workaround: Disable the **bgp graceful-restart** command on both routers.

Wide-Area Networking

- CSCsc05413

  Symptoms: IPCP is not established when you bring up an MLP bundle between a Cisco 12000 series and a Cisco 7500 series. On the Cisco 12000 series, the IPCP state remains in “REQsent” and on the Cisco 7500 series, the IPCP state is stopped.

  Conditions: This symptom is observed when you create an MLP bundle that consists of two member links and when you bring up the MLP interface. Note that LCP is properly established but IPCP is not, causing IP connectivity to be lost. The symptom may also occur in a configuration with a Cisco 10000 series.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(27)SBB5

Cisco IOS Release 12.2(27)SBB5 is a rebuild release for Cisco IOS Release 12.2(27)SBB. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBB5 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCsa69518

  Symptoms: In a multicast VPN, a BGP MDT update of the router's own address (that is used as the source for the default MDT and that is usually the loopback address) is sent as Route Distinguisher 0:0.

  Conditions: This symptom is observed on a Cisco router when the **mdt default** command is configured before the **rd** command in the VRF configuration.

  Workaround: Enter the **clear ip bgp *** EXEC command or remove the VRF by entering the **no ip vrf** command and then reconfigure the VRF by entering the **rd** command.

- CSCsc52732

  Symptoms: When PIM is enabled or disabled on a subinterface, multicast traffic that is received on another subinterface of the same main interface is dropped for a moment.

  Conditions: This symptom is observed on a Cisco router that is configured for IP Multicast. The higher the multicast traffic rate is, the more packets are dropped.

  Workaround: There is no workaround.

Miscellaneous

- 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.

- CSCsb28300

  Symptoms: When you enter the **issu loadversion** command, the standby RP may become stuck in the standby cold bulk state.

  Conditions: This symptom is observed on a Cisco router that has dual RPs and that is configured for Service Software Upgrade (ISSU).

  Workaround: There is no workaround.

- CSCsb47281

  Symptoms: When you enter the **issu loadversion** command, the standby RP may become stuck in the standby cold bulk state.

  Conditions: This symptom is observed on a Cisco router that has dual RPs and that is configured for Service Software Upgrade (ISSU). The output of the **show redundancy history** command shows that the "CEF RRP RF Client" function causes the standby RP to remain in the cold bulk state.

  Workaround: There is no workaround.

- CSCsd64437

  A router will log an informational message when it has reached a terminal state for Route Processor Redundancy (RPR), RPR Plus (RPR+), or Stateful Switchover (SSO). A terminal state is reached when the router has finished progressions for all its clients for one operational mode (that is, RPR, RPR+, or SSO) and remains in this state. The logging of an informational message means that you no longer have to enter the **show redundancy states** command to determine if the router has reached a terminal state.

TCP/IP Host-Mode Services

- CSCsb51019

  Symptoms: A TCP session does not time out but is stuck in the FINWAIT1 state and the following error message is generated:

  ```
  %TCP-6-BADAUTH: No MD5 digest from x.x.x.x to y.y.y.y(179) (RST)
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that is connected to a third-party vendor router after the BGP authentication password is changed on the Cisco router.

  Workaround: Identify the BGP connection that is stale by entering the **show tcp brief** command and then clear the TCP control block.

- CSCsc39357

  Symptoms: A Cisco router may drop a TCP connection to a remote router.

  Conditions: This symptom is observed when an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than what the remote router can handle, causing the remote router to advertise a zero window. Subsequently, when the remote router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be 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.

Resolved Caveats—Cisco IOS Release 12.2(27)SBB4

Cisco IOS Release 12.2(27)SBB4 is a rebuild release for Cisco IOS Release 12.2(27)SBB. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBB4 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsd11547

  Symptoms: The values are not populated for some of the object identifiers (OIDs) in the CISCO-PROCESS-MIB.

  Conditions: This symptom is observed on a Cisco platform that is configured for SNMP when you enter a getmany command for the cpmProcExtUtilTable object.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeg51291

  Symptoms: A VRF ping fails to reach an OSPF neighbor interface.

  Conditions: This symptom is observed when the platform on which the ping originates and the OSPF neighbor interface are connected via an OSPF sham link that is used for interconnecting traffic between two VPN sites.

  Workaround: There is no workaround.

- CSCeh92012

  Symptoms: Border Gateway Protocol (BGP) next-hop information is not redistributed as expected by Open Shortest Path First (OSPF).

  Conditions: This symptom is on a Cisco 7206VXR that is configured with an NPE-G1 (revision A) and that runs Cisco IOS interim Release 12.4(1.8)T. However, the symptom is platform-independent and occurs also in other releases.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb05456

  Symptoms: A Cisco platform may reset its RP when two simultaneous **write memory** commands from two different vty connections are executed, and messages similar to the following may appear in the crashinfo file:

  ```
  validblock_diagnose, code = 10
  current memory block, bp = 0x48FCC7D8, memory pool type is Processor data check, ptr = 0x48FCC808
  next memory block, bp = 0x491AC060, memory pool type is Processor data check, ptr = 0x491AC090
  previous memory block, bp = 0x48FCBBE8, memory pool type is Processor data check, ptr = 0x48FCBC18
  ```

  The symptom is intermittent and is related to the way NVRAM is accessed.

  Conditions: This symptom is observed on a Catalyst 6000 series Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXD but is platform- and release-independent.

  Workaround: Set the boot configuration to non-NVRAM media such as a disk or bootflash by entering the following commands:

  boot config disk0:

  filename

  nvbypass

- CSCei69803

  Symptoms: After the PXF engine on the PRE reloads, traffic that is being forwarded via default routes (both global and VRF) is dropped.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs.

  Workaround: Force a switchover to the standby PRE by entering the **switchover pxf restart** command. Note that this workaround is available only when the PREs function in SSO redundancy mode.

- CSCej77348

  Symptoms: Buddy queues are created when they should not be created.

  Conditions: This symptom is observed on a Cisco 10000 series when a nested policy map is attached to an interface with a link bandwidth that is more than 500 Mbps. In this situation, a buddy queue is created for each class queue that is created.

  Workaround: There is no workaround.

- CSCej81121

  Symptoms: Both the active and standby RPs may crash and the following error message is generated:

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

  Conditions: This symptom is observed when the active RP is under stress because traffic is being processed and you enter a command that is related to NVRAM while the standby RP boots and synchronizes with the active RP.

  Workaround: Do not enter a command that is related to NVRAM for the active RP while the standby RP boots and synchronizes with the active RP.

- CSCsc65787

  Symptoms: A router may modify the interface MTU of an interface during the initialization process. In turn, this situation may modify layer 3 protocol MTUs (such as IP MTUs), preventing OSPF, IS-IS, or other L3 protocols from coming up.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image of Release 12.2SB that includes the fix for caveat CSCsa73817 when the MPLS MTU is larger than the interface MTU.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa73817. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Configure the interface MTU to be equal to or larger than the MPLS MTU and configure the IP MTU to the desired value.

- CSCsd47642

  Symptoms: After a router is reloaded, a service policy is no longer attached to a dot1q trunk interface in the running configuration.

  Conditions: This symptom is observed on a Cisco 10000 series when the service policy is configured with a class-matching QoS group and a strict priority queue for this class. The service policy is applied to dot1q trunk interface. When the router is reloaded, the service policy is no longer associated with the trunk interface in the running configuration. Note that the startup configuration still appears correct.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **copy startup-config running-config** command to re-attach the service policy.

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

- CSCeg82698

  Symptoms: PPTP tunnels do not come up.

  Conditions: This symptom is observed when VPDN is configured.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(27)SBB3

Cisco IOS Release 12.2(27)SBB3 is a rebuild release for Cisco IOS Release 12.2(27)SBB. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBB3 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeg62206

  Symptoms: High CPU utilization may occur during the TPLUS process on a platform.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(6c) and that is configured for TACACS. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCei34102

  Symptoms: A router that has many sessions configured crashes when interfaces flap.

  Conditions: This symptom is observed on a Cisco router that functions in a stress situation when 8000 PPPoA sessions are brought up and the interfaces flap.

  Workaround: There is no workaround.

  Further Problem Description: The router crashes when it attempts to establish 8000 PPPoA sessions and 800 tunnels for scalability characterization. When the interfaces flap for a first time, all 8000 sessions come up. The crash occurs when the interfaces flap for a second time.

IP Routing Protocols

- 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.

- CSCsb60277

  Symptoms: When you remove an ATM subinterface, a spurious memory access may be generated.

  Conditions: This symptom is observed on a Cisco 10000 series but may be platform-independent.

  Workaround: There is no workaround.

- CSCsc00378

  Symptoms: Changes in an export map are not picked up by the BGP Scanner.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when you apply an export map to a VRF and when the interface that connects the PE router to a CE router is configured for OSPF.

  Workaround: Enter the **clear ip ospf process** command to enable the BGP Scanner to pick up the changes in the export map.

- CSCsc59089

  Symptoms: BGP does not advertise all routes to a peer that sends a route-refresh request.

  Conditions: This symptom is observed under the following conditions:

  – The router is in the process of converging all of its peers and has updates ready in the output queue for the peer.

  – The peer sends a route-refresh request to the router. This may occur when the **clear ip bgp * soft in** command is entered on the peer or when a VRF is added to the peer.

  – The router processes the route-refresh request from the peer while the router still has updates in the output queue for the peer.

  In this situation, all of prefixes that are advertised by the unsent updates in the output queue for the peer are lost.

  Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip bgp * soft out** command on the router to force the router to send all updates to its peers.

Miscellaneous

- CSCeg20335

  Symptoms: A Cisco 10000 series may lose the PVC configurations for several subinterfaces and high CPU usage may occur. When you attempt to reconfigure the PVCs, error messages similar to the following may be generated:

```
Router#pvc 35/134
Unable to create PVC 35/134 on ATM1/0/0.10350134. Possibly multiple users configuring
IOS simultaneously
Further info about other user:
Process id: 42, Process: Slot 1/0 CMD Process, TTY: 0, Location: Console
Router(config-subif)#
```

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(7)XI1 or Release 12.2(27)SBB.

Workaround: Reload the router.

- CSCeg28531

  Symptoms: A format operation for a disk fails and hangs.

  Conditions: This symptom is observed on a Cisco platform when you enter the **format** EXEC command for a second time.

  Workaround: There is no workaround.

- CSCeh39027

  Symptoms: The output of the **show pxf cpu subblock** command may show a negative number of interleaved packets or bytes when Link Fragmentation and Interleaving (LFI) is disabled and the interface is passing traffic.

  Conditions: This symptom is observed on a Cisco 10000 series that has an LFI over ATM (LFIoATM) or LFI over Frame Relay (LFIoFR) interface.

  Workaround: There is no workaround. However, the symptom relates to counters only and does not affect the operational behavior of the router.

- CSCeh47169

  Symptoms: A Cisco router may reload because of I/O memory corruption when you use Telnet, reverse Telnet, rsh, or other vty-based applications, for example, a vty-based application to access a service module.

  Conditions: This symptom is observed on a Cisco router that contain the fix for caveat CSCef84400. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef84400. 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.

- CSCeh90231

  Symptoms: When the cbQosPolicyMapCfgTable object of the CISCO-CLASS-BASED-QOS-MIB MIB is polled via SNMP, the child policy maps that are configured via the **service-policy** command as an action for a class under a parent policy map are not retrieved.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB.

  Workaround: There is no workaround.

- CSCeh98154

  Symptoms: When you enter the **show processes cpu monitor** command through a Secure Shell (SSH) login session, the SSH session immediately freezes and the CPU usage increases.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBA or Release 12.2(27)SBB.

  Workaround: There is no workaround.

- CSCei39771

  Symptoms: After the router has reloaded, super ACLs cause a high CPU usage, and all traffic that uses the policy map is evaluated as if the traffic matches the first class in the policy.

Conditions: This symptom is observed on a Cisco 10000 series only when there are hundreds of policy maps configured.

Workaround: There is no workaround.

- CSCei79969

  Symptoms: When a forced reload occurs on a standby RP, the active RP generates the following error message and a traceback:

  ```
  %ISSU-3-NOT_FIND_MSG_SES
  ```

  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 and that functions as an ASBR-PE router when you remove the **ip vrf** *vrf-name* command and immediately cause a forced reload of the standby RP.

  Workaround: There is no workaround.

- CSCei93170

  Symptoms: The standby PRE may become stuck in the DISABLE mode while the router boots or reloads.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB2, that functions in HA redundancy mode, and that has a very large configuration.

  Workaround: There is no workaround.

- CSCek02672

  Symptoms: A Cisco 10000 series may use the physical egress interface as the syslog source interface instead of the configured loopback interface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB1 and that is equipped with redundant PREs after a PRE switchover has occurred.

  Workaround: If this is an option, unconfigure the syslog source interface before the PRE switchover occurs and reconfigure it after the switchover has occurred. If this is not an option, there is no workaround.

- CSCek24426

  Symptoms: When an RPR+ switchover from the primary RP to the standby RP occurs, a Cisco 10000 series may crash just after generating the following error messages:

  ```
  %C10KATM-1-REPROGRAM: Force reprogram command failure for 2/0
  %C10K-3-LC_ERR: Slot[4/0] 1gigethernet-1 eth_cmd_reprogram_cmd_parser:Card does not
  support cmd!
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB.

  Workaround: There is no workaround.

- CSCsa96444

  Symptoms: When you reload a non-active primary line card by entering the **hw-module slot** *slot-number* **reload** command, all circuits may bounce.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with line cards that function in SR-APS mode when the port of the active secondary line card processes traffic.

  Workaround: There is no workaround.

- CSCsb04236

  Symptoms: On a Cisco 10000 series, if an interface is configured for Link Fragmentation and Interleaving (LFI), traffic sharing between configured queues in QoS profiles may not be proportional to the configured values.

  Conditions: This symptom is observed only for links that have LFI enabled and for which the bandwidth ratio between the queues is not within 5 percent of the configured value. The symptom may affect LFIoFR, LFIoATM, LFIoMLP, and FRF.12.

  Workaround: There is no workaround.

  Further Problem Description: Links that do not have LFI configured are almost always within 5 percent of the configured bandwidth.

- CSCsb88925

  Symptoms: A router may crash when you change the configuration by removing a service policy from a subinterface and move the service policy to an ATM PVC.

  Conditions: This symptom is observed on a Cisco 10000 series

  Workaround: There is no workaround.

- CSCsb94413

  Symptoms: When you enter the **show startup-config | begin** command to search for text in a very large startup configuration, it may take a long period of time to find the text.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Do not enter the **show startup-config | begin** command. Rather, enter the **more nvram:startup-config | begin** command. Also, if you accidently enter the **show startup-config | begin** command, use the CRTL and ^ keys to stop the search and return to the prompt.

- CSCsc11636

  Symptoms: A router requires a very long time to boot (more than 5 minutes, potentially hours). Also, changes to the QoS configuration may require long times.

  Conditions: This symptom is observed when the QoS configuration has a complex arrangement of many policies that reference many access control entries (ACEs) through a number of class maps. The time required is, roughly, proportional to the number of combinations of interfaces, policies, classes, and ACEs. For example, if each of 200 interfaces has a QoS policy, each policy uses five class maps, each class map references two ACLs, and each ACL has 30 entries, there are 60,000 combinations.

  Workaround: Either reduce the number of combinations of interfaces, policies, class maps, and ACEs, or load the configuration in two stages. The first stage (from NVRAM) should contain the interface and ACL definitions, and the second stage (from another file) should contain the classes and policies.

- CSCsc33825

  Symptoms: A CPUHOG condition may occur when you modify ACLs that are used with a policy map to perform classification that is based on the ACLs. This situation may cause incorrect packet classification during the processing of the ACL changes.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB1.

  Workaround: There is no workaround.

Further Problem Description: The fix for this caveat includes the following changes:

- Unnecessary notifications about ACL and class-map configuration changes are eliminated.
- During the processing of policy-map changes, the old classifier is kept active until the new one is fully configured (see caveat CSCsc37918).
- During the compilation of ACL changes, the SuperACL process now classifies to the class default instead of to the first class in the policy map (see caveat CSCei39771).

- CSCsc34944

  Symptoms: The output of the **show running vrf** *vrf-name* command shows a difference between the T1 controller information and the T3 controller T3 information. (The T3 controller is not displayed although the T1 controller is displayed.)

  Conditions: This symptom is observed on a Cisco 10008 that runs the c10k2-p11-mz image of Cisco IOS Release 12.2(27)SBB1 and that is configured with a PRE2 and a 6-port channelized T3 line card.

  Workaround: To some degree, you can confirm the information of T3 controller through the output of the **show running-config** command.

- CSCsc37253

  Symptoms: When you replace an OC-12 POS or OC-12 ATM line card with an OC-3 POS line card and you configure the port with any type of encapsulation (HDLC, PPP, or Frame Relay), the line protocol does not come up.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround. When the symptom occurs, reload microcode onto the PXF engine to enable the line protocol to come up.

- CSCsc37434

  Symptoms: For an interface that is configured for FRF.12, the channelized T3 interface statistics (that is, for the input packets) are incorrect and do not match with the policy map statistics. The policy map does have the correct packet statistics. This situation may affect NMS polling: collecting the interface statistics may result in wrong data collection.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB2 and that is configured with a 6-port channelized T3 line card that has an interface that is configured for FRF.12. Note that the symptom does not occur when FRF.12 is not configured.

  Workaround: There is no workaround.

- CSCsc44237

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: A switch or router that is configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

     The output of the **show processes memory** command shows that the "ATM PA Helper" process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

     Condition 1: This symptom is observed on a Cisco switch or router that runs a Cisco IOS software image that contains the fixes for caveats CSCeh04646 and CSCeb30831. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh04646 and http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb30831.

Cisco IOS software releases that are not listed in the "First Fixed-in Version" fields at these locations are not affected.

Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

2. Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory.

   The output of the **show processes memory** command shows that the "PIM process" does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

   Condition 2: This symptom observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCef50104.

   A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef50104. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

   Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf** *vrf-name* command is configured, enter the **ip vrf forwarding** *vrf-name* command on at least one interface that has PIM enabled.

- CSCsc45678

  Symptoms: When you modify ATM PVC shaping parameters (either by changing from VBR-nrt to UBR or by modifying the parameters such as SCR or PCR), the modification does not take effect although it the changes do appear in the configuration and in the output of the **show atm pvc** command.

  Conditions: This symptom is observed in some cases when ATM PVC shaping is modified on an existing PVC. The following table details all the various cases and explains whether or not the symptom occurs:

Case	Interface	Subinterface	Symptom Occurs
1	Up/Up	Up/Up	No
2	Up/Up	Down/Down	No
3	Up/Up	Admin Down	Yes
4	Down/Down	Down/Down	Yes
5	Down/Down	Admin Down	Yes
6	Admin Down	Admin Down	Yes

  The symptom is not observed in any other circumstances and does not occur when a PVC is created or deleted.

  Workaround: When you modify ATM PVC shaping parameters, proceed as follows:

  1. Delete the ATM PVC from the subinterface.
  2. Quit the configuration mode.
  3. Recreate the ATM PVC with the new shaping parameters.

- CSCsc52795

  Symptoms: Fiber issues or remote shutdowns take a long time (more than two seconds) to result in link-down processing, causing forwarded traffic be lost even when other load-balanced links are available.

Conditions: This symptom is observed on a Cisco 10000 series when you configure interface carrier-delay to a low millisecond to minimize the forwarding interruption.

Workaround: There is no workaround.

- CSCsc54539

  Symptoms: Security ACLs with more than eight lines stop functioning and either permit all traffic or drop all traffic.

  Conditions: This symptom is observed on a Cisco 10000 series when a named or numbered ACL is used in a class map. The ACL continues to function properly until it is changed or removed from all interfaces and then re-applied. The symptom occurs because the ACL is no longer turbo-compiled.

  Workaround: Do not use an ACL in a class map that is also used for security.

  Further Problem Description: Note that the symptom occurs only for ACLs that need to be turbo-compiled. ACLs with eight or fewer lines do not need to be turbo-compiled and the symptom does not occur for these ACLs.

- CSCsc93021

  Symptoms: Static analysis warnings are generated when uninitialized variables are present.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCsa74819

  Symptoms: When you enter the **no vpdn ip udp ignore checksum** command in order not to ignore the checksum, this configuration change is not retained after the router is reloaded.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS image that integrates the fix for CSCef90365, that is, a Cisco IOS image in which the **vpdn ip udp ignore checksum** command is enabled by default.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef90365. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: After the router had reloaded, re-enter the **no vpdn ip udp ignore checksum** command.

- CSCsc38968

  Symptoms: A subinterface comes back up after an End-to-End Keepalive (EEK) failure even though EEK is still down.

  Conditions: This symptom is observed when the Frame Relay End-to-End Keepalive feature is enabled in bidirectional mode in a configuration with a Frame Relay hub and spoke and when an EEK failure occurs. In this situation, the subinterface of the hub goes down and the output of the **show frame-relay end-to-end keepalive** command shows the EEK status as down on the PVC. However, when the hub receives an full status LMI update from the Frame Relay spoke, the subinterface on the hub comes back up even though EEK is still down. This is improper behavior.

  To see the message log that reports that the subinterface goes up or down, ensure that the **logging event subif-link-status** command is enabled on the subinterface.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(27)SBB2

Cisco IOS Release 12.2(27)SBB2 is a rebuild release for Cisco IOS Release 12.2(27)SBB. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBB2 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCei13040

  Symptoms: When an OSPF neighbor comes back up after a very fast (sub-second) interface flap, OSPF routes that are learned via the interface that flapped may not be re-installed in the RIB.

  Conditions: This symptom is observed when the following two events occur:

  – The interface flaps very quickly.

  – The neighbor comes back up before the LSA generation timer expires.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that flapped.

  Alternate Workaround: Enter the **clear ip route *** EXEC command.

- CSCsc07467

  Symptoms: An OSPF route is lost after an interface flaps.

  Conditions: This symptom is observed rarely when all of the following conditions are present:

  – There is a very brief (shorter than 500 ms) interface flap on a point-to-point interface such as a POS interface.

  – The flap is not noticed by the neighbor, so the neighbors interface remains up.

  – The OSPF adjacency goes down and comes back up very quickly (the total time is shorter than 500 ms).

  – OSPF runs an SPF during this period and, based on the transient adjacency information, removes routes via this adjacency.

  – The OSPF LSA generation is delayed because of LSA throttling. When the LSA throttle timer expires and the LSA is built, the LSA appears unchanged.

  Workaround: Increase the carrier-delay time for the interface to about 1 second or longer.

  Alternate Workaround: Use an LSA build time shorter than the time that it takes for an adjacency to come up completely.

Miscellaneous

- CSCei84450

  Symptoms: A Cisco 10000 series unexpectedly ceases to forward traffic over an AToM VC even though the AToM circuit is in the UP state.

  Conditions: This symptom is observed when the AToM VC is configured on an ATM interface, when the AToM VC is routed over an MPLS traffic engineering tunnel, and when the AToM VC has just changed its state.

Workaround: There is no workaround.

- CSCej28291

  Symptoms: Low link utilization at a throughput of about 70 percent may occur in certain configurations and traffic patterns.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB when the following conditions are present:

  - Traffic is sent over 1500 PPP over Serial and 1500 PPP over ATM links.
  - The interfaces are configured with three queues that have 1 percent, 9 percent, and 89 percent of the bandwidth.
  - The interfaces are overdriven by generated traffic, the largest part of which is sent to the smallest queue with some load to the other queues as well.

  Workaround: There is no workaround.

- CSCej43295

  Symptoms: A traffic interruption of over 20 seconds occurs when fiber is pulled from a port in an SR-APS configuration.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with four 4-port channelized OC-3 line cards that are configured for SR-APS.

  Workaround: There is no workaround. Traffic recovers on its own after 20 seconds.

- CSCsb03042

  Symptoms: A Cisco 10000 series may be unable to add PVPs to physical ATM interfaces because bandwidth oversubscription is incorrectly reported.

  Conditions: This symptom is observed on a Cisco 10008 that runs Cisco IOS Release 12.3(7)XI4 and that is configured with a PRE-2 and a 4-port OC-3/STM-1 ATM, single mode line card. The symptom could also occur in Release 12.2(27)SBB. The router functions in an environment that includes PPPoX DSL aggregation, a create on-demand configuration, VBR-NRT oversubscription, and an ATM PVC Range.

  Workaround: There is no workaround.

- CSCsb52835

  Symptoms: In the output of the **show policy-map interface** command, the output queue appears on both the input policy and the output policy, both of which record “interface drops.” This situation is also shown as WRED drops in the output policy.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB.

  Workaround: There is no workaround.

- CSCsc14076

  Symptoms: When you change an ATM PVC from VBR-NRT to UBR or the other way around, the subscribed bandwidth is incorrect, which is shown in the output of the **show controllers atm** command.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsc30782

  Symptoms: The access list-based classification on a source IP address does not function correctly in an output service policy.

Conditions: This symptom is observed on a Cisco 10000 series that functions in a QoS configuration with three hierarchical service policies.

Workaround: Remove the grand child service policy from the child policy map and re-apply the grand child service policy to the child policy map. If this is not an option, there is no workaround.

Open Caveats—Cisco IOS Release 12.2(27)SBB1

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(27)SBB1. All the caveats listed in this section are open in Cisco IOS Release 12.2(27)SBB1. This section describes only severity 1, severity 2, and select severity 3 caveats.

Interfaces and Bridging

- CSCeh64309

  Symptoms: A standby RP reloads unexpectedly.

  Conditions: This symptom is observed on a Cisco router when the IP address of a VLAN is deleted via the **default ip address** *ip-address mask* command during a TFTP copy operation in the wrong order in relation to the **default encapsulation dot1q** command.

  Workaround: Place the commands in the correct order as in the following example:

```
interface GigabitEthernet7/0/0.1
       default ip address 192.1.1.1 255.255.255.0
       default encapsulation dot1q
       ....
```

  Alternate Workaround: Remove the **default ip address** *ip-address mask* command entirely, as in the following example:

```
interface GigabitEthernet7/0/0.1
       default encapsulation dot1q
       ....
```

  Note that in this example, the **default encapsulation dot1q** command actually deconfigures the **default ip address** *ip-address mask* command automatically.

IP Routing Protocols

- CSCsa79739

  Symptoms: A memory allocation failure traceback is logged on a router that is configured for BGP.

  Conditions: This symptom is observed when you enter the **clear ip bgp *** command and when there is a large number of routes.

  Workaround: Enter the **clear ip bgp soft [in|out]** command to generate a BGP update.

Miscellaneous

- CSCef81909

  Symptoms: An MPLS interface may not drop some packets that are larger than the size of the configured MTU.

Conditions: This symptom is observed on a Cisco 10000 series when the packet size is as follows:

- For a POS interface, the packet size is between the size of the MTU and the size of the MTU plus 114 bytes.
- For a GE interface, the packet size is between the size of the MTU and the size of the MTU plus 24 bytes.

Workaround: There is no workaround.

- CSCeg16419

  Symptoms: A Frame Relay PVC remains active when the peer interface is shut down.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Frame Relay over MPLS when the AToM tunnel between the Frame Relay PVC and the peer interface is configured for LMI.

  Workaround: There is no workaround.

- CSCeg25335

  Symptoms: The accounting counters in the output of the **show interface** *type slot/port* **accounting** command are not updated on a PE router.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that is configured for AToM AAL5 local switching.

  Workaround: There is no workaround.

- CSCeg54016

  Symptoms: Priority Queuing (PQ) traffic may be dropped from an ATM VC.

  Conditions: This symptom is observed on a Cisco 10000 series when LFIoATM is configured together with traffic shaping on a per-VC/VP basis, when the VPs are overdriven, and when interleaving is not enabled on the ATM VC.

  Workaround: Enable interleaving on the ATM VC.

  Further Problem Description: We recommend that you do not use the configuration that is described in the Conditions above. If you do, ensure that interleaving is enabled on the ATM VC. When interleaving is disabled, the priority queue becomes a multilink packet queue and does not receive preferential treatment on the bundle.

- CSCeg56206

  Symptoms: Multilink statistics are not propagated to a Frame Relay DLCI when LFIoFR is enabled on the MLP interface.

  Conditions: This symptom is observed on a Cisco 10000 series. The symptom occurs only for DLCI statistics; multilink statistics are correct.

  Workaround: There is no workaround.

- CSCeg58121

  Symptoms: The output of the **show pxf cpu queue** *interface* command does not show any dequeued packets for Priority Queueing (PQ).

  Conditions: This symptom is observed on a Cisco 10000 series that is configured LFIoFR and occurs after you have entered the **microcode reload pxf** command.

  Workaround: There is no workaround.

  Further Problem Description: We do not recommend that you use the **microcode reload pxf** command in a production network.

- CSCeg78563

  Symptoms: The link use may be as low as 94 percent of the expected rate on low-speed links that have FRF.12 enabled.

  Conditions: This symptom is observed under extremely rare conditions on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCeg90091

  Symptoms: Targeted LDP sessions flap.

  Conditions: This symptom is observed on a Cisco 10000 series when Virtual Circuit Connection Verification (VCCV) ping traffic exceeds 2500 pps.

  Workaround: Lower the VCCV ping traffic rate.

- CSCeh09708

  Symptoms: You cannot attach a Frame Relay map class to a VRF interface after you have removed an existing Frame Relay map class.

  Conditions: This symptom is observed on a Cisco 10000 series that has an input policy on a PVC via a Frame Relay map class and an output policy on a subinterface of the PVC.

  Workaround: Either attach both the input and output policies to the subinterface or place both the input and output policies in the Frame Relay map class.

- CSCeh27726

  Symptoms: The creation of an E1 controller is not blocked when T1 controllers are already configured on the same port, causing all T1 controllers to be changed to E1.

  Conditions: This symptom is observed on a Cisco 10000 series when you create an E1 controller on a port of a channelized OC-12 line card.

  Workaround: Only controllers of the same type are supported on the same port: do not change the type of a controller to E1 when other controllers on the same port are configured for T1.

- CSCeh34253

  Symptoms: The AToM statistics byte count in the output of **show mpls forwarding-table** command is incorrect.

  Conditions: This symptom is observed on a Cisco 10000 series when traffic is sent over an AToM VC.

  Workaround: There is no workaround.

- CSCeh38970

  Symptoms: The Count of APS (COAPS) switchovers register on an interface of an OC-48 POS line card does not increment after an APS switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that has OC-48 POS interfaces that are configured for APS configuration when you enter the **aps force** command to initiate a switchover from a working interface to a protect interface.

  Workaround: There is no workaround.

- CSCeh39027

  Symptoms: The output of the **show pxf cpu subblock** command may show a negative number of interleaved packets or bytes when Link Fragmentation and Interleaving (LFI) is disabled and the interface is passing traffic.

Conditions: This symptom is observed on a Cisco 10000 series that has an LFI over ATM (LFIoATM) or LFI over Frame Relay (LFIoFR) interface.

Workaround: There is no workaround. However, the symptom relates to counters only and does not affect the operational behavior of the router.

- CSCeh39660

  Symptoms: A standby PRE continues to reset when the auto boot image is not properly configured or when the PRE1 does not find the auto boot image.

  Conditions: This symptom is observed on a Cisco 10000 series during a major upgrade from a PRE1 to a PRE2 in a redundant system.

  Workaround: Ensure that the auto boot image is properly configured.

- CSCeh40097

  Symptoms: The link use may be between 90 and 95 percent of the expected rate on links that are configured for LFIoFR.

  Conditions: This symptom is observed under very rare conditions on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCeh48397

  Symptoms: When you enter the **show aps** command for an active PRE and a standby PRE that function in SSO mode while the standby PRE is in the HOT-STANDBY state, the automatic protection switching (APS) state may show as mismatched for the PREs.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with SONET line cards and that runs in SR-APS mode.

  Workaround: There is no workaround.

- CSCeh49788

  Symptoms: Large ICMP packets fail to pass over an MLP over ATM link or MLP over Frame Relay link. This situation also causes pings of large packets to fail.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in an MLP over ATM or MLP over Frame Relay configuration when the ICMP packets have a size of at least 3000 bytes and consist of at least three IP fragments.

  Workaround: There is no workaround.

- CSCeh51775

  Symptoms: Multilink VCs that are configured for MLPoATM, bundles, VCs, and VAI interfaces may flap continuously.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **microcode reload pxf** command.

  Workaround: There is no workaround.

  Further Problem Description: We do not recommend that you use the **microcode reload pxf** command in a production network.

- CSCeh54019

  Symptoms: During an upgrade from a PRE1 to a PRE2, the following error messages are generated on the PRE2 console:

```
Failed to assert Cutover alarm for RP A
%IPCGRP-3-ERROR: outgoing IPC bypass failed:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: There is no workaround. However, the error messages do not affect the upgrade.

- CSCeh64464

  Symptoms: An MLP over ATM member link of a multilink bundle may remain down.

  Conditions: This symptom is observed on a Cisco 10000 series when you remove and return an MLP over ATM member link to an active multilink bundle or place the MLP over ATM member link in another multilink bundle.

  Workaround: First shut down the multilink bundle before you add or remove the member link.

- CSCeh70291

  Symptoms: When you enter the **redundancy force-failover main-cpu** privileged EXEC command on a Cisco 10000 series that is configured with two Performance Routing Engines (PREs), an automatic protection system (APS) switchover occurs on SONET line cards, which is incorrect behavior.

  Conditions: This symptom is observed on a Cisco 10000 series with redundant PREs when APS is configured on SONET line cards and when the following sequence of events occurs:

  1. You enter the **aps force pos** *slot*/*subslot*/*port* **from working** interface configuration command on the Cisco 10000 series and its peer.
  2. You enter the **show aps** EXEC command. The output displays the active channels for both routers.
  3. You enter the **redundancy force-failover main-cpu** privileged EXEC on one of the routers, causing an APS switchover to occur on this router.

  Workaround: There is no workaround. However, when the symptoms occurs, there is no loss of data.

- CSCeh79117

  Symptoms: A memory allocation (malloc) error occurs and tracebacks are generated on a Cisco 10000 series.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router and that is configured with 750 VRFs and 250,000 VPNs when a remote peer is reloaded.

  Workaround: There is no workaround.

- CSCeh79964

  Symptoms: A PE router loses L3VPN connectivity with a CE router.

  Conditions: This symptom is observed on a Cisco 10000 series when a VLAN is configured with an AToM VC, the VLAN subinterface is deleted, and then the same VLAN ID is used for a L3VPN connection.

  Workaround: Do not use the same VLAN ID for the L3VPN connection between the PE router and the CE router but configure a different VLAN ID.

- CSCeh85664

  Symptoms: The SSO performance is slow (longer than 4 seconds) with an OC-48 POS line card.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs when the mode of the OC-48 POS line card is not set.

  Workaround: Configure the OC-48 POS line card to function in POS mode.

- CSCeh93149

  Symptoms: All packets may be dropped from an MVPN when traffic is switched to a data MDT.

Conditions: This symptom is observed very rarely on a Cisco 100000 series that functions as a PE router only after the direction of the traffic flow between the Cisco 10000 series and another PE router is reversed or with bidirectional traffic when both unicast and multicast VRFs are configured on the Cisco 10000 series and bidirectional traffic is sent on the MVPN.

Workaround: There is no workaround.

- CSCei09643

  Symptoms: The configuration of the secondary PRE differs from the configuration of the primary PRE.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with AToM VCs over ATM AAL5 PVCs.

  Workaround: Initiate a switchover to synchronize the primary and secondary PREs.

- CSCei13877

  Symptoms: When a protection line card is removed and replaced, traffic is interrupted for a period between one and ten seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has an active POS APS configuration with OC-3 POS or OC-12 POS line cards.

  Workaround: There is no workaround.

- CSCei23628

  Symptoms: You cannot copy a startup configuration file with a large size to the NVRAM of a standby PRE2 during an upgrade from a PRE1 to a PRE2.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs that function in RPR mode when the size of the startup configuration file is larger than the size of the NVRAM of the PRE1

  Workaround: Perform a second copy operation.

- CSCsa59560

  Symptoms: A provider (P) router may drop a packet that is larger than 1472 bytes.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a P router and that is connected to a provider edge (PE) router in the following configuration:

  - A source transmits a packet that is larger than 1472 bytes via an IP connection to the PE router.
  - The PE router forwards the packets through an MVPN tunnel over a Gigabit Ethernet connection to the P router, which is the next hop for the PE router.
  - The size of the packet exceeds the default MTU of the MVPN tunnel.

  Workaround: There is no workaround.

- CSCsa65102

  Symptoms: When you change the encapsulation on a Gigabit Ethernet subinterface, the service policy that is attached to this subinterface may be removed.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB and that is configured with a PRE2.

  Workaround: There is no workaround.

- CSCsa72673

  Symptoms: If you apply a service policy to Fast Ethernet interface 0/0/0 on a Cisco 10000 series, the ciscoCBQosMIB cbQosPoliceStatsTable and csQosTSStatsTable may be empty.

Conditions: This symptom is observed when you use SNMP to poll the CISCO-CLASS-BASED-QOS-MIB and when there is a service policy attached to Fast Ethernet interface 0/0/0.

Workaround: Remove the service policy from Fast Ethernet interface 0/0/0.

- CSCsa74551

  Symptoms: A Cisco 10000 series may display CPUHOG messages when you modify the configuration of a policy map.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB only when the policy map is applied to thousands of interfaces.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is harmless and does not affect the proper functionality of the router.

- CSCsa82775

  Symptoms: An AIS-DS3 alarm is not detected at the T3 controller level.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card.

  Workaround: There is no workaround.

- CSCsa86548

  Symptoms: The parent of a hierarchical policing policy that is attached as an output policy to an interface of 24-Port T1/E1 line card may not increment its packet, conform, exceed and violate counters.

  Conditions: This symptom is observed on a Cisco 10000 series only when Frame Relay encapsulation is configured.

  Workaround: There is no workaround.

  Further Problem Description: This symptom is related to counters only; the policer behavior and functionality are not affected.

- CSCsa96774

  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.

- CSCsb00534

  Symptoms: When FRF.12 is applied to thousands of DLCIs, a Cisco 10000 series may generate CPUHOG error messages and tracebacks.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **microcode reload pxf** command.

Workaround: There is no workaround.

Further Problem Description: We do not recommend that you use the **microcode reload pxf** command in a production network.

- CSCsb03230

  Symptoms: A Cisco 10000 series may crash when you reload the router.

  Conditions: This symptom is observed very rarely when PXF debugging is enabled.

  Workaround: Do not enable PXF debugging.

- CSCsb03458

  Symptoms: The performance of a Cisco 10000 series may be briefly affected when an ATM PVC configuration is modified or when an ATM PVC is deleted and recreated.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE2 only when the router has both ATM interfaces and multicast enabled. The symptom occurs when you enter the **no pvc** interface configuration command followed by the **pvc** interface configuration command to change the configuration of an ATM PVC or to delete and recreate and ATM PVC.

  Workaround: When you change the ATM PVC or when you delete and recreate an ATM PVC, enter only the **pvc** interface configuration command, that is, without first entering the **no pvc** interface configuration command.

- CSCsb04236

  Symptoms: On a Cisco 10000 series, if an interface is configured for Link Fragmentation and Interleaving (LFI), traffic sharing between configured queues in QoS profiles may not be proportional to the configured values.

  Conditions: This symptom is observed only for links that have LFI enabled and for which the bandwidth ratio between the queues is not within 5 percent of the configured value. The symptom may affect LFIoFR, LFIoATM, LFIoMLP, and FRF.12.

  Workaround: There is no workaround.

  Further Problem Description: Links that do not have LFI configured are almost always within 5 percent of the configured bandwidth.

- CSCsb04655

  Symptoms: Serial and POS interfaces that are configured for Frame Relay may flap during the ISSU process.

  Conditions This symptom is observed on a Cisco 10000 series that is configured with redundant PREs.

  Workaround: There is no workaround.

- CSCsb08466

  Symptoms: On a Cisco 10000 series that is configured with full-rate Gigabit Ethernet (GE) interfaces, traffic sharing between configured queues in QoS profiles may not be proportional to the configured values.

  Conditions: This symptom is observed only with very high speed interfaces such as GE and OC-48 interfaces for which the bandwidth ratio between queues may not be within 5 percent of the configured value.

  Workaround: There is no workaround.

  Further Problem Description: Lower speed interfaces are almost always within 5 percent of the configured bandwidth.

- CSCsb08527

  Symptoms: When multiple traps are generated in a short period of time, the default *length* argument of 10 of the **snmp-server queue-length** *length* command may cause some traps to be dropped.

  Conditions: This symptom is observed on a Cisco 10000 series when you use an SNMP host to monitor traps.

  Workaround: Enter another value for the *length* argument of the **snmp-server queue-length** *length* command: enter a number that is greater than 10, in the order of 50 to 100.

- CSCsb08587

  Symptoms: Drops may occur on the priority queue when low latency queueing (LLQ) is configured and extreme traffic conditions occur.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB. The priority queue starts to drop a small portion of the packets at 900,000 pps or a higher rate.

  As an example, the symptom would occur on a Gigabit Ethernet interface with a priority queue configured with a 75-percent policer when small packets are sent at 900,000 pps or a higher rate.

  Workaround: There is no workaround.

- CSCsb10143

  Symptoms: A small number of packets may be dropped from a Gigabit Ethernet (GE) interface.

  Conditions: This symptom is observed on a Cisco 10000 series when you send packets with sizes from 64 to 87 bytes at line rate and when QoS is enabled on the GE interface.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs only when user queues are applied to the GE interface. The observed drop rate is very low (6 pps).

- CSCsb10145

  Symptoms: When you enter the **issu runversion** command and the command execution is followed by a switchover, the following error message and traceback are generated:

  ```
  %IPCGRP-3-CMDOP: IPC command 402 (slot2/0): line card ipc is disabled - dropping
  non-blocking ipc command
  Traceback= 60509B80 60696FBC 60697AD8
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 6-port channelized T3 line card.

  Workaround: There is no workaround. However, the ISSU operation and switchover succeed.

- 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.

- CSCsb10789

  Symptoms: A Cisco 10000 series that is configured for Multilink PPP (MLP), LFI, and WRED may generate the following error messages and traceback:

  ```
  %C10K_MULTILINK_STATE-3-EREVENT: cannot deactivate member at this time
  %C10K_MULTILINK_USER_WARNING-2-CRITEVENT: member incapable of clean removal at this
  time
  ```

```
%GENERAL-3-EREVENT: clear bundle data failed
-Traceback= 60505148 6102CF2C 6102CF5C 6102A88C 6102A930 609F15C0 609EC164 605B3E5C
605B3FB8
```

Conditions: This symptom is observed only when you enter the **microcode reload pxf** command.

Workaround: There is no workaround. However, the functionality of the router is not affected.

- CSCsb12456

  Symptoms: When you copy a large configuration via TFTP to a channelized OC-12 line card (with 768 interfaces), the interprocess communication (IPC) channel to the channelized OC-12 line card is dropped, and the log shows messages similar to the following:

  ```
  %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot 2/0.
  %IPCOIR-2-CARD_UP_DOWN: Card in slot 2/0 is down.
  Notifying 1choc12-1 driver.
  %IPCGRP-3-CMDOP: IPC command 405 (slot2/0): line card ipc is disabled - dropping
  non-blocking ipc command
  -Traceback= 60504368 6069013C 60690C58
  %C10K_ALARM-6-INFO: ASSERT CRITICAL slot 2 Card Stopped
  Responding OIR Alarm - subslot 0
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs that function in SSO mode and with one or more channelized OC-12 line cards.

  Workaround: There is no workaround. However, the line card recovers and reloads on its own a few seconds after the symptom has occurred.

- CSCsb13223

  Symptoms: Traffic may be unstable and the overall link use may be poor when you configure quality of service (QoS) user queues by entering the **bandwidth remaining percent** *value* command.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB when the following conditions are present:

  - The links are between 100 Mbps and 900 Mbps (for example, STM1/OC3 or STM4/OC12 links).
  - There are more than three user queues provisioned via the **bandwidth remaining percent** *value* command.
  - Traffic is sent to all the queues.

  Workaround: Enter the **maximize-utilization** command on the queues that are provisioned via the **bandwidth remaining percent** *value* command.

  Alternate Workaround: Do not enter the **bandwidth remaining percent** *value* command. Rather, enter the **bandwidth percent** *value* command.

  Further Problem Description: The symptom does not occur on other interfaces such as E3/T3 and STM4/OC12. The symptom is specific to interfaces that are configured between 100 Mbps and 900 Mbps.

- CSCsb15086

  Symptoms: When you enter the **issu runversion** command and the command execution is followed by a switchover, the following error message and traceback are generated on the new active PRE:

  ```
  %IPC-4-NOPORT: Port Not Found. 130000 --> 10010, Index:8, Seq: 41113, flags: 0, size:
  36
  -Traceback= 605071F4 606E569C 606E60A4 611B06C4 611B0828 605E1FB4 605E1FA0
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs.

  Workaround: There is no workaround. However, the ISSU operation and switchover succeed.

- CSCsb18877

  Symptoms: The values of the cRFcRFStatusFailoverTime.0 and cRFStatusPeerStandByEntryTime.0 objects of the CISCO-RF-MIB are always zero.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SNMP when you use the CISCO-RF-MIB to monitor the cRFStatusFailoverTime and cRFStatusPeerStandByEntryTime objects.

  Workaround: There is no workaround.

- CSCsb19052

  Symptoms: Multilink interfaces remain down in an LFI over ATM configuration, there is high CPU use, and a "Queue ID exhausted" error message is generated.

  Conditions: These symptoms are observed on a Cisco 10000 series when the total number of queues on the router is close to 128,000, which is the maximum number of supported queues. LFI over ATM does not scale to this number.

  Workaround: There is no workaround. Note that up to 88,000 queues function successfully in an LFI over ATM configuration.

- CSCsb19602

  Symptoms: When you enter the **hw-module secondary reset** command, an ALIGN-3-TRACE error message is generated.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PRE2s.

  Workaround: There is no workaround.

  Further Problem Description: The traceback does not appear to impact the functionality of the router.

- CSCsb19856

  Symptoms: FRF.12 may not function on an interface. Even though a policy map is configured, it is missing from the interface.

  Conditions: This symptom is observed on Cisco 10000 series that is configured with redundant PREs and about 4095 DLCIs, that is, the maximum number supported. Even though the interface has all the required commands in the running configuration, the output of the **show policy-map interface** *interface* command does not show a policy map attached to the interface.

  Workaround: Load the initial configuration with only one PRE in the active state and then bring up the secondary PRE.

- CSCsb20224

  Symptoms: When you boot a Cisco 10000 series the following error message may be generated:

  ```
  %IP-4-DUPADDR: Duplicate address 23.4.2.254 on FastEthernet0/0/0, sourced by
  0009.b688.df00
  ```

  Conditions: This symptom is observed on a Cisco 100000 series that is configured with redundant PRE2s.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not appear to impact the functionality of Fast Ethernet interface 0/0/0.

Resolved Caveats—Cisco IOS Release 12.2(27)SBB1

Cisco IOS Release 12.2(27)SBB1 is a rebuild release for Cisco IOS Release 12.2(27)SBB. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBB1 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

- CSCsb31412

  Symptoms: A standby PRE-2 may crash continuously when you enter the **tacacs-server host** *host-ip-address* **key** *string* command and when the **aaa new-model** command is not enabled.

  Conditions: This symptom is observed on a Cisco 10000 series when you insert a standby PRE-2 in the chassis.

  Workaround: Disable the **tacacs-server host** *host-ip-address* **key** *string* command if the **aaa new-model** command is not enabled.

IP Routing Protocols

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

- CSCeh66610

  Symptoms: The BGP timer (minimum hold time from neighbor) is configurable but is not seen in the configuration.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(27)SBB.

  Workaround: There is no workaround.

- CSCei26899

  Symptoms: When you reset a BGP peer, some prefixes are missing.

  Conditions: This symptom is observed on a Cisco MGX8850 RPM-XF that runs Cisco IOS Release 12.3(11)T. However, the symptom is platform-independent and may also occur in other releases.

  Workaround: There is no workaround.

- CSCsb25194

  Symptoms: After an HA switchover, BGP sessions fail because the hold time expires, causing traffic to fail until the session comes back up.

  Conditions: This symptom is observed on a Cisco router that has BGP Graceful Restart configured with timers that are configured with values that are less than the default values. For example, 10-second keepalives and a 30-second holdtime causes the symptom to occur.

  Workaround: There is no workaround. Using default timers with 60-second keepalives and a 180-second holdtime prevents the symptom from occurring, but this may not be a practical workaround if you have to make too many changes in a network.

- CSCsb25237

  Symptoms: BGP Nonstop Routing sessions do not re-establish quickly enough after an NSF switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with low keepalive and holdtime values.

  Workaround: There is no workaround.

- CSCsb51101

  Symptoms: When you perform an SSO switchover, packets may be lost because of a “no route” condition. The loss of these packets is an indication of a prolonged SSO convergence time. The routes for these packets are restored automatically within a few seconds.

  Conditions: This symptom is observed on a Cisco router with dual RPs that function in SSO mode.

  Workaround: There is no workaround.

- CSCsb51968

  Symptoms: An EIGRP neighbor adjacency may reset during an ISSU upgrade procedure.

  Conditions: This symptom is observed on a Cisco 10000 series but may be platform-independent.

  Workaround: There is no workaround.

Miscellaneous

- CSCea17268

  Symptoms: If the **show users** command is used on standby, the following may be seen:

```
Router show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
   1 vty 0                 idle                    never
```

  See the line with “never”.

  This may also be present in some cases when a switchover is done, and standby becomes newly active. When it is active, “clear line 1” will not deallocate it.

  Conditions: Go to the submode of “config t”, then check “show users” on standby. You should see the “never” row. Now make the switchover without exiting the “config t”. The newly active standby should have the “never” row.

  Workaround: Try to exit “config t” before the switchover. If you are in that mode, there is no way to remove it unless you do another switchover.

- CSCee56112

  Symptoms: When issuing the **show policy-map interface** *interface name* **[input|output]** command, the output should only show the input or the output policies, but not both. There is no issue with functionality.

  Conditions: This symptom occurs when requesting either the input or the output policies.

  Workaround: There is no workaround.

- CSCef15141

  Symptoms: The Priority Queueing (PQ) latency values (in milliseconds) are higher than twice the MTU plus 6 ms on 4-Mbps and 8-Mbps subrates of an 8-port clear channel E3/DS3 line card.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.3(7)XI or Release 12.2(27)SBB.

  Workaround: A workaround is to provision Cisco or Digital Link subrates as multiples of 358 kbps time slots:

  For a 4-Mbps subrate, provision the Cisco or Digital Link interface as 3938 or 4296 kbps.

  For an 8-Mbps subrate, provision the Cisco or Digital Link interface as 7876 or 8234 kbps.

  Further Problem Description: The Cisco DSU mode or Digital Link DSU mode breaks the available bandwidth into 358 kbps chunks (time slots). The line card uses a bandwidth multiple of 358 kbps that is larger than the user-configured 4-Mbps and8-Mbps subrates. This situation creates a bandwidth mismatch between the line card and PXF, causing backpressure.

- CSCeh08263

  Symptoms: Toggling to/from E1 to T1 mode on the 24-port ChE1/T1 line card causes the card to reset and generate an OIR event. This results in extra line card reset messages in the console log. This will also be observed when the line card is initialized as a result of router reload or insertion of the line card when the card is configured for T1 mode.

  Conditions: This symptom occurs on a Cisco 10000 router with a 24-port Channelized E1/T1 line card.

  Workaround: There is no workaround. The line card will successfully initialize and function properly after the extra reset/OIR.

  Additional information: When performing an In-Service Software Upgrade (ISSU) from an image WITHOUT this fix to one WITH this fix, an incompatibility will be flagged. This is because the line card will be reloaded and reset in order to apply the fix.

  The reload and reset will result in a traffic interruption of 20-25 seconds for all interfaces on the ChE1/T1 line card. This will happen when upgrading from Cisco IOS Release 12.2(27)SBB to 12.2(27)SBB1, for example.

- CSCeh22837

  Symptoms: The following error message is generated repeatedly on a standby PRE:

  ```
  Cannot insert into AVL tree
  ```

  This message is generated when an attempt is made to add policy map information to the CISCO-CLASS-BASED-QOS-MIB and when a collision of cbQosPolicyIndex values occurs. (The cbQosPolicyIndex is the internal QID of the service policy.) This situation prevents the service policy from being added to the MIB but does not prevent the service policy from being applied to the interface.

In addition, missing entries occur only when you use the CISCO-CLASS-BASED-QOS-MIB after a switchover from the active PRE to the standby PRE (on which the error is generated). The error message is generated once for each missing combination (that is, service policy, interface, and direction).

Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs that function in SSO or RPR+ mode. The occurrence of the symptom depends on the number of interfaces to which service policies are attached.

Workaround: There is no workaround.

- CSCeh48541

  Symptoms: The PXF engine of a PRE2 crashes and a "PXF DMA TBB Length Error" may be generated.

  Conditions: This symptom is observed on a Cisco 10000 series only when an output service policy is applied with both absolute priority and police actions as in the following example:

```
Policy Map adsl1000-ar600
    Class P1
      police 600000 12000 12000 conform-action transmit exceed-action drop
violate-action drop
      priority
    Class class-default
      police 104000 12000 12000 conform-action transmit exceed-action drop
violate-action drop
```

  Workaround: There is no workaround.

- CSCeh61467

  This caveat consists of the two symptoms, two conditions, and two workarounds:

  1. Symptom 1: After you have disabled MVPN on a VRF interface, the CPU use for the PIM process increases to 99 or 100 percent and remains at that level.

     Condition 1: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases.

     Workaround 1: Before you disable MVPN on the VRF interface, enable and then disable multicast routing by entering the **ip multicast-routing vrf** *vrf-name* global configuration command followed by the **no ip multicast-routing vrf** *vrf-name* global configuration command.

  2. Symptom 2: A router that functions under stress and that is configured with a VRF interface may crash when an MDT group is removed from a remote PE router.

     Condition 2: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases, and occurs only when there are frequent link flaps or other multicast topology changes that affect the VRF interface.

     Workaround 2: There is no workaround.

- CSCeh70353

  Symptoms: VCCI values go in and out of synchronization when an ATM line card is configured for MDR.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCeh76090

  Symptoms: A Cisco 10000 series may crash when you swap flash cards.

  Conditions: This symptom is observed very rarely and only after repeated (more than 80) instances of removing and reinserting a flash card.

  Workaround: Remove the flash card quickly, wait for a few seconds, and then reinsert the flash card quickly.

- CSCeh85674

  Symptoms: The SSO switchover for a 1-port OC-48/STM-16 POS line card takes more than 3 seconds.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCeh93928

  Symptoms: A ping over a 4-port channelized STM-1/OC-3 line card that is configured for Frame Relay, HDLC, or PPP fails when an RPR switchover occurs.

  Conditions: This symptom is observed on a Cisco 10000 series when the active PRE runs a different Cisco IOS software image than the standby PRE. The symptom may also occur with a 1-port channelized OC-12/STM-4 line card.

  Workaround: There is no workaround.

- CSCei01846

  Symptoms: ATM sessions may flap when the virtual path (VP) or the ATM port is overdriven.

  Conditions: This symptom is observed on a Cisco 10000 series only when keepalives or OAM is configured for the session and when the VP or the ATM port is overdriven.

  Workaround: Disable keepalives or OAM.

- CSCei04496

  Symptoms: The expected traffic convergence time after a second switchover is 90 seconds but the actual traffic convergence time is more than 150 seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PREs and that is configured with 4000 interfaces. The PREs function in RPR+ mode.

  Workaround: There is no workaround.

- CSCei07809

  Symptoms: After an SSO switchover occurs, the newly active PRE may generate error messages similar to the following ones for a full-height Gigabit Ethernet line card:

  ```
  Ironbus retry count is 40
  %PXF_DMA-3-IRONBUS_NOTRUNNING: Data path to slot 5/0 failed to synchronize (State Not Running)
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SSO or ISSU.

  Workaround: There is no workaround.

- CSCei07913

  Symptoms: Traffic that passes through a Cisco 10000 series may not recover after an SSO switchover when MVPNs are configured.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs and that functions as a PE router when the customer Rendezvous Point is located away from the traffic source.

Workaround: Configure the customer Rendezvous Point close to the traffic source. Also, enter the **ip pim register-rate-limit 1** command to facilitate traffic recovery for low MVPN traffic levels.

Further Problem Description: After performing an SSO switchover, all multicast packets are punted, causing the use of the CPU to increase, and in turn, causing BGP sessions to flap and traffic to drop.

- CSCei09385

  Symptoms: A 4-port channelized STM-1/OC-3 line card resets during an SSO switchover.

  Conditions: This symptom is observed on a Cisco 10000 series when the 4-port channelized STM-1/OC-3 line card operates fully configured with the maximum number of configurable interfaces (768 T1 or E1 interfaces) at 90 percent of the maximum traffic rate.

  Workaround: There is no workaround.

  Further Problem Description: After an SSO switchover, some line card tasks take too long to run to completion, causing an "SW_WATCHDOG" timeout to occur and the line card to reset. The fix for this caveat shortens the scheduled duration of such line card tasks.

- CSCei16493

  Symptoms: When a Single router-APS (SR-APS) configuration is removed and re-applied, continuous tracebacks are generated on the standby PRE2.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PRE2s that function in SSO mode and 4-port channelized STM-1 (ESR-4CHSTM1) line cards that function in linear 1+1 APS mode. APS is configured by entering the **associate slot** *slot_one slot_two* command.

  Workaround: To clear the symptom, initiate a PRE switchover by entering the **redundancy force-switchover main-cpu** command. Note, however, that the tracebacks do not impact the functionality of the router nor interrupt traffic.

- CSCei22506

  Symptoms: When you change the configuration from, for example, HDLC to PPP, the **no framing**, **no path**, or **no aug mapping** command is typically used to clear the controller setting. When the controller is reconfigured after having been cleared, an ifindex traceback is generated on both the active and standby PRE. When the ifindex is not synchronized properly to the standby PRE, an SSO switchover causes prolonged traffic outage of between 10 and 20 seconds.

  Conditions These symptoms are observed on a Cisco 10000 series that is configured with redundant PREs.

  Workaround: Do not clear the controller. If you must clear the controller, reset the standby PRE after you have reconfigured the controller to prevent prolonged traffic outages during SSO switchovers.

- CSCei23197

  Symptoms: Traffic may be lost and misdirected on interfaces of a 6-port channelized T3 line card.

  Conditions: This symptom is observed on a Cisco 10000 series when an RPR+ switchover occurs.

  Workaround: Do not use RPR+. Rather, use SSO. If this is not an option, there is no workaround.

- CSCei31102

  Symptoms: When you copy a file to the startup configuration of the active RP of a redundant pair of RPs that is configured for SSO, the running configuration instead of the startup configuration is synchronized to the standby RP.

Conditions: This symptom is observed on a Cisco router when you copy a file, for example via TFTP, to the startup configuration of the active RP.

Workaround: Copy the startup configuration to the standby RP by entering the **copy startup stby-nvram:startup** command.

- CSCei45893

  Symptoms: Multiple labels appear in label table for a prefix after cutover.

  Conditions: This symptom only occurs when BGP does not have graceful-restart enabled, and a cutover occurs.

  Workaround: Enable the **bgp graceful-restart** command or the **clear ip route vrf** *vpn* ***** command.

  Further Problem Description: Old labels are not removed on cutover. Any change to the route after the cutover period will clean up the labels.

- CSCei52198

  Symptoms: The **show startup-config** command takes too long and runs the CPU up to 100%.

  Conditions: This problem is specific to the **show startup- config** command and its alternate command **show config** command.

  Workaround: There is no workaround.

  Resolution: The **show startup** command has been rewritten to greatly improve performance.

- CSCei63369

  Symptoms: When a single router-APS (SR-APS) is configured CHSTM1 cards on Cisco 10000 series routers, resetting or OIRing one card will stop the traffic, and it will never restart.

  Conditions: This symptom is observed on a Cisco 10000 series router that has 4- port channelized STM-1 (ESR-4CHSTM1) line cards that function in linear 1+1 APS mode. APS is configured by entering the **associate lot** *slot_one slot_two* command.

  Workaround: To clear the symptom, remove APS configuration by entering the **no associate slot** *slot_one slot_two* command and then, re-configuring APS by entering the **associate slot** *slot_one slot_two* command.

- CSCei64659

  Symptoms: When using the **show led** command, the output from the alternate PRE2 may have extra characters appear.

  Conditions: This symptom may occur any time the **show led** command is used.

  Workaround: There is no workaround.

- CSCei83838

  Symptoms: It takes too long for traffic to resume after an HA switchover on a 4-port channelized OC-3 line card on a Cisco 10000 series.

  Conditions: This symptom is observed on a 4-port channelized OC-3 line card that is configured for SONET framing, channelized T3s with 768 T1 interfaces, and PPP encapsulation when an automated script performs an HA switchover.

  Workaround: There is no workaround. Note that the symptom does not occur after a manual HA switchover.

- CSCei84416

  Symptoms: A 4-port channelized OC-3 line card resets unexpectedly.

Conditions: This symptom is observed on a Cisco 10000 series when the line card is unconfigured, causing the default line clocking to be set on both sides of the connection.

Workaround: Ensure that the correct clocking is configured.

- CSCei91640

  Symptoms: A Cisco 10000 series that is configured for LFIoATM crashes. The crash log shows that the crash occurs because of a bus error on a TLB store exception. Immediately before the crash, there are also two error messages generates that describe an "Illegal access to a low address" error to address 0x84.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB.

  Workaround: There is no workaround.

- CSCej03663

  Symptoms: The active PRE and standby PRE lose their synchronization.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **no card** command immediately after you have shut down a line card.

  Workaround: Reset the standby PRE. You can prevent the symptom from occurring by waiting about 20 seconds after entering the **shutdown** command before you enter the **no card** command.

- CSCej11101

  Symptoms: A Cisco router gives an error message when variable bit rate (VBR) or unspecified bit rate (UBR) permanent virtual circuit (PVC) is removed.

  Conditions: This symptom is observed on a Cisco 10000 series router.

  Workaround: There is no workaround.

- CSCej12350

  Symptoms: A Cisco 10000 series reloads when you perform an OIR of a 24-port channelized E1/T1 line card.

  Conditions: This symptom is observed when you remove the 24-port channelized E1/T1 line card, enter the **no card** command, and reinsert the line card.

  Workaround: Perform an OIR of the line card without entering the **no card** command.

- CSCej17003

  Symptoms: The standby PRE of a Cisco 10000 series may crash because of a TLB exception error.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with dual PREs and that has a large configuration (for example, about 1.6 MB) when you enter the **no card** command for a slot that is configured with a GE line card before the router has completed the bootup process.

  Workaround: Wait until the router has completed the bootup process before you enter the **no card** command.

- CSCin96857

  Symptoms: The active RP (or PRE) crashes when the standby RP (or PRE) comes up.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 10000 series when an RPR switchover occurs or when the redundancy mode is changed from SSO to RPR.

  Workaround: There is no workaround.

- CSCsa52472

  Symptoms: Drops occur on a strict priority queue that is configured at a high rate.

  Conditions: This symptom is observed on a Cisco 10000 series on interfaces of the following line cards:

  - 1-Port OC-12/STM-4 POS
  - 1-port Gigabit Ethernet
  - 1-port OC-48/STM-16 POS

  Workaround: There is no workaround.

- CSCsa65096

  Symptoms: A router may crash during the boot process when the startup configuration includes the **hw-module shutdown** command.

  Conditions: This symptom is observed on a Cisco 10000 series but is platform-independent. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa51602. Cisco IOS software releases not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCsa67594

  Symptoms: Low link usage may occur on a Cisco 10000 series that is configured with a PRE2.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB on low-speed links (typically 128 Kbps or lower) that are configured with a priority queue and several other user queues. The symptom occurs only with certain QoS configurations and traffic profiles.

  Workaround: There is no workaround.

- CSCsa71096

  Symptoms: When a high number of QoS policy maps is configured, it may take a long time for a router to activate all of them.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB when a very large amount (thousands) of QoS policy maps and class maps are configured and applied to interfaces.

  Workaround: There is no workaround.

  Further Problem Description: QoS policy maps are compiled on the Cisco 10000 series, therefore compilation time is a factor in policy map activation. Each policy map is compiled individually, so the more policy maps are configured and applied, the longer it will take for all of them to be activated on the router. When a policy map is compiled, it is activated immediately, so some policy maps are activated very quickly while others may take several minutes to become active. It takes about 0.3 seconds to compile a policy map on a Cisco 10000 series.

- CSCsa72510

  Symptoms: When you reset a module or line card, an error message and traceback that includes a reference to "%COMMON_FIB-SP-4-CHAIN_REMOVE_INCONS3" may be generated. Typically, there are no further adverse effects and the router continues to behave normally, however, in extremely rare situations, the router may crash immediately after the error occurs.

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 and that is configured for IP loadbalancing when a change occurs that causes a recalculation of the loadbalancing, for example, when an interface is shut down, a route flaps, a line card resets, and so on.

Workaround: Reconfigure the router or network to prevent equal-cost loadbalancing on routes. If this is not an option, there is no workaround.

- CSCsa82031

  Symptoms: When you perform a microcode reload for the PXF engine while traffic passes through interfaces and subinterfaces that have FRF.12 enabled (that is, map classes are attached to the main interfaces), the following symptoms may occur:

  - Tracebacks are generated.
  - The interfaces remain in the up/down state and the subinterfaces remain in down/down state while the traffic is running, preventing the traffic from passing through. When the traffic stops, the interfaces and subinterfaces come up, but a ping still fails on all interfaces and subinterfaces.
  - The PXF engine may crash.

  Conditions: These symptoms are observed on a Cisco 10000 series only when a large number (more than 1000) of DLCIs configured.

  Workaround: There is no workaround.

- CSCsa82771

  Symptoms: T1 and T3 clocks do not switch to the internal source when LOF-DS3, AIS-DS3, LOF-DS1, or AIS-DS1 alarms occur.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card.

  Workaround: There is no workaround.

- CSCsa89073

  Symptoms: When an LP-RDI alarm occurs, the TU controller goes down and the E1 controller remains up and does not report any errors. The TU controller should remain up under this alarm condition.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card when the E1 controller is configured under an AU-4 via SDH framing.

  Workaround: There is no workaround. However, the transmission of data is not affected.

- CSCsa89477

  Symptoms: When a T3 controller goes down, a link down trap of the channelized interface will be sent with Generic Trap Type 3(LinkUP).

  Conditions: This symptom is seen on a 6-port channelized T3 line card.

  Workaround: There is no workaround.

- CSCsa90041

  Symptoms: When you enter the **set ip dscp** policy-map class configuration command, the ToS value for packets are not marked properly. The other three bits for DSCP are marked properly.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsa91462

  Symptoms: The PXF engine may crash when multicast traffic passes through the router. The PXF engine recovers after the crash but a connected PE router may be unable to reach the RR by using the router as the transit path.

  Conditions: This symptom is observed on a Cisco 10000 series that has neighbors that are configured for OSPF and BGP.

  Workaround: Reload the router. If this not an option, there is no workaround.

- CSCsa92310

  Symptoms: After an ISSU "runversion" has occurred with a major Minimal Disruptive Restart (MDR) for interfaces of a 1-port Gigabit Ethernet half-height line card, the line card stops forwarding 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.

- CSCsb03849

  Symptoms: A Cisco 10000 series fails to boot after you have reloaded the router.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB when the **microcode pxf** *ucode filename* command is part of the startup configuration.

  Workaround: Remove the **microcode pxf** *ucode filename* command from the startup configuration.

- CSCsb04956

  Symptoms: On a Cisco router that has redundant RPs functioning in SSO mode, a series of XDR error messages and tracebacks similar to the following may be generated:

  ```
  %XDR-6-ISSUBADRCVTFM: Failed to rcv_transform message - slot 0, reason:
  ISSU_RC_MSG_SESSION_NOT_REGISTERED
  -Traceback= 60508224 6040B77C 603DA868 603FA360 606A31DC 606A3390

  %ISSU-3-DEBUG_ERROR: Passing an invalid session ID (0) to ISSU debug macro
  -Traceback= 6121072C 6040B648 603DA8A8 603FA360 606A31DC 606A3390

  %XDR-3-CLIENTISSUBADNEGOMSG: Unexpected nego msg - slot 0, client IPv6 table broker,
  ctxt 0
  -Traceback= 60508224 603DAA58 603FA360 606A31DC 606A3390
  ```

  The output of the **show xdr linecard** command shows "PEER BEING REMOVED" for the standby RP, and the standby RP does not recover from this state. When an SSO switchover occurs, traffic forwarding stops and NSF does no longer function.

  Conditions: This symptom is observed when the standby RP crashes or is removed during an XDR ISSU negotiation. The symptom occurs only in SSO mode.

  Workaround: There is no workaround.

- CSCsb09807

  Symptoms: The SSO switchover time on a channelized OC-3 or OC-12 line card that is configured for PPP, Frame Relay, and HDLC encapsulation is too long. The traffic interruption may last between 3 and 40 seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PREs functioning in SSO mode and that is configured with one or more 1-port channelized OC-12/STM-4 or 4-port channelized OC-3/STM-1 line cards that are configured with any type of encapsulation.

  Workaround: There is no workaround.

- CSCsb13268

  Symptoms: Some counters may not be cleared when you enter the **clear counters** command.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for FRF.12.

  Workaround: There is no workaround.

- CSCsb17203

  Symptoms: A Cisco 12000 series that is configured with dual PRPs, that has more than one 10G Engine 5 SPA Interface Processor (12000-SIP-600), and that has a 10-port Gigabit Ethernet (SPA-10X1GE) installed in each 12000-SIP-600 may not load one of the SPA modules after a cold boot.

  Conditions: The symptom is observed only when the Cisco 12000 series is powered off and powered back on. The symptom does not occur on a Cisco 12000 series that is configured with a single PRP.

  Workaround: Reload the router via a warm reload.

  Further Problem Description: The symptom is related to a race condition that is only observed on the Cisco 12000 series. The symptom is more likely to occur when timing becomes an issue, for example, in a configuration with a large number of interfaces as described in the Symptoms above. However, the root cause of this race condition is platform-independent and relates to the interface IfIndex synchronization. This is the reason why the fix for this caveat is integrated in releases that do not support the Cisco 12000 series.

- CSCsb19101

  Symptoms: Seven to eight seconds of traffic loss occurs during an initial switchover after you have booted the router. During subsequent switchovers, the traffic loss lasts less than three seconds. The traffic loss occurs only on ATM interfaces.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB, that is configured for SSO, and that has ATM interfaces.

  Workaround: There is no workaround.

- CSCsb19966

  Symptoms: After a VBR-NRT VC is changed to a UBR circuit, the SCR bandwidth is not released.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Delete the VBR-NRT VC and then recreate the VC as a UBR circuit.

- CSCsb21715

  Symptoms: On a Cisco 10000 series that is configured with redundant PREs that function in RPR+ mode, when the controller mode of a 24-port channelized E1/T1 line card is changed from E1 to T1 or from T1 to E1, an error occurs during further configuration of the controller, as described in the example below:

  ```
  controller t1 5/0/0 %ERROR: Standby doesn't support this command ^ % Invalid input
  detected at '^' marker.
  ```

  When you configure the controller mode, the standby PRE receives the synchronization message but does not execute it, causing the active PRE to function in T1 mode and the standby PRE to function in E1 mode (or the other way around).

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB. The symptom does not occur when there is no change in the controller mode, nor does it occur when the router functions in SSO mode.

Workaround: If this an option, configure the router to function in SSO mode. If you must run the router in RPR+ mode, ensure that you save the configuration to NVRAM and reload the router after you have changed the controller mode from E1 to T1 or from T1 to E1.

- CSCsb28409

  Symptoms: The RP of a Cisco 10000 series may crash because of memory corruption when a class is added to a policy map that is already attached to an interface. The memory corruption can be a red zone violation, a corrupted block of pointers, or another type of memory corruption.

  Conditions: This symptom is observed when the following conditions are present:

  - A new class is being added to a policy map. Note that a class addition also occurs when an action is added to an empty class. Similarly, when the last action is removed from a class, the class is deleted from the policy map.
  - The policy map is non-hierarchical and is already attached to an interface.
  - The number of classes (including the class default but excluding the new class that is being added) that are already present in the policy map is a power of two number, that is, 2, 4, 8, and so on.

  Workaround: Remove the policy from the interface before you add the class. Re-attach the policy after you have added the class.

  Further Problem Description: The addition of the class causes a memory corruption. The effect of the memory corruption depends on the memory consumption of the router. If the middle of a free block is corrupted, then the router will continue operating. However if a block boundary is corrupted or if the middle of an allocated block is corrupted, then router may crash.

- CSCsb30553

  Symptoms: A router may crash when you modify the queue limit in a class of a policy map that is being used.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE-2 and that runs Cisco IOS Release 12.2(27)SB.

  Workaround: There is no workaround.

- CSCsb32727

  Symptoms: PXF buffers may not be replenished when a child policy map of a hierarchical policy map that is configured for LFI is removed by entering the **no policy-map pmap** command while a high rate of traffic is still being processed on the interface to which the policy map is attached.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB.

  Workaround: Shut down the interface before you removing the policy map.

  First Alternate Workaround: Unconfigure the parent policy map before you remove the child policy map.

  Second Alternate Workaround: Remove LFI from the map class through by entering the **no frame-relay fragment** command.

  Third Alternate Workaround: Remove the class map from the interface before you remove the policy map.

- CSCsb33599

  Symptoms: A RPR switchover from a PRE-1 that runs one Cisco IOS software image to a PRE-2 that runs another Cisco IOS software image may take longer than you would expect. It takes up to 30 minutes for traffic to be fully restored.

Conditions: This symptom is observed on a Cisco 10000 series when software upgrade from a PRE-1 to a PRE-2 is performed via a Fast Software Upgrade (FSU). However, the symptom occurs only when the PRE-1 runs as a standby mode for more than 35 minutes.

Workaround: Ensure that an RPR switchover occurs before the standby PRE-1 runs in standby mode for 35 minutes. Alternately, reset the standby PRE-1 and wait until it comes back up before you initiate an RPR switchover.

- CSCsb33959

  Symptoms: When you attempt to attach another output policy to a subinterface that has already a Frame Relay class map with LFI and an output service policy attached, no error message is generated to prevent you from doing so. The interface accepts both of these output policies (one on the subinterface and one is in the Frame Relay class-map).

  Each time you modify the configuration of subinterface (for example, you remove the service policy from the interface, you remove the Frame Relay class map, or you add the Frame relay class map after you have removed it), the following error messages are generated:

  ```
  Internal variables out of sync in c10k_toggle_xcm_policies.
  Internal variables out of sync in c10k_toggle_xcm_policies.
  Internal variables out of sync in c10k_policy_write_first_police_data_index.
  Internal variables out of sync in c10k_toggle_xcm_policies.
  ```

  To remove these error messages, initiate a PRE switchover (in a configuration with redundant PREs) or reset the PRE (in a configuration with a single PRE).

  When you have two policies configured on the subinterface, you cannot know which output policy has taken affect. When you remove one of the statements (that is, the Frame Relay map class or the service policy output), QoS does not seem to function properly.

  Conditions: These symptoms are observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsb34750

  Symptoms: When configuring a Cisco 10000 series router with QoS on the native dot1q subinterface, packets leaving that subinterface may not get classified.

  Conditions: This symptom is observed on a Cisco C10008 router that is running Cisco IOS Release 12.2(27)SBB and is configured with a PRE2-RP processor when a service policy is applied to the native dot1q subinterface.

  Workaround:
  1. Remove the “native” dot1q encapsulation on the subinterface (normal dot1q subinterface).
  2. Apply QoS policy on the main interface (“native” dot1q encapsulation is still on the subinterface).

- CSCsb35091

  Symptoms: A short while after you have configured a policy map, the router displays the following error message and traceback:

  ```
  %GENERAL-3-EREVENT: Error in Final table
  -Traceback= 60506178 60F8CD04 60FAD9C4 60FAF1D0 60FAF314 60FAFF5C 60FCAEE8 60F8C9D4
  60F89088 60F8BF94 60F8C184 60F8C338
  ```

  Conditions: This symptom is observed on a Cisco 10000 series when a class in the policy map matches on an access control group (ACL) that contains an IP address mask, as in the following example:

  ```
  ip access-list extended TEST
  permit ip any 10.6.0.0 0.0.0.255
  ```

  Workaround: There is no workaround.

- CSCsb35499

  Symptoms: The following commands are not available on virtual-access sub- interfaces and will cause the creation of full virtual-access interfaces:

  ```
  ip bgp
  ip cgmp
  ip dvmrp
  ip igmp
  ip mroute-cache
  ip ospf
  ip policy
  ip rgmp
  ip route-cache
  ip sap
  ip split-horizon
  ip summary-address
  ip tcp
  ip traffic-export
  ip urd
  ```

  Conditions: This symptom occurs in Cisco IOS Release 12.2(27)SBA and later 12.2SB releases.

  Workaround: There is no workaround.

- CSCsb40981

  Symptoms: Service policy is applied on an interface with policer under each class. The policer appears to be working fine initially. If the policer values are changed, the show policy commands display the new values, but the policing still seems to be working as per the old values. For example, packets conformed or exceeded as per the old values.

  Conditions: This symptom occurs when policer is tested on GigE interface of a Cisco 10000 series PRE-2 that is running Cisco IOS Release 12.2(27)SBB.

  Workaround: Remove the class and added it back to the policy-map.

- CSCsb43060

  Symptoms: A router crashes when you apply a grandchild policy to a child class.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB.

  Workaround: Remove the policy map from the interface, edit the policy, and then re-apply the policy map to the interface.

- CSCsb44002

  Symptoms: When running multiple instances of the **show pxf cpu queue ATM x/y/z** command, the Cisco 10000 ESR may crash with a bus error.

  Conditions: This symptom occurs on a Cisco 10000 ESR.

  Workaround: There is no workaround.

- CSCsb44311

  Symptoms: When FRF.12 (Frame Relay LFI) is configured for a nested QoS policy, the shape value of the parent policy does not take effect.

  Conditions: This symptom is observed on a Cisco 10000 series only when both Frame Relay LFI and nested policies are configured.

  Workaround: There is no workaround.

- CSCsb46114

  Symptoms: The alarm in the **show facility-alarm status** command does not get clear after the standby PRE is reset and comes back up.

  Conditions: This symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(27)SBB.

  Workaround: Reload the standby PRE.

- CSCsb46474

  Symptoms: After shutting down the ATM interface, the critical LOCD alarm does not clear in the "show facility-alarm status" display.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(27)SBB.

  Workaround: Reload the router to clear the LOCD alarm.

- CSCsb46587

  Symptoms: A Cisco 10000 series reloads when you swap line cards of a different type.

  Conditions: This symptom is observed when an ATM line that is configured with PVCs is replaced with a channelized line card and when you configure a channel on the channelized line card.

  Workaround: Remove the PVCs from the ATM line card before you replace the ATM line card with a line card of another type.

- CSCsb46737

  Symptoms: After issuing the **shut** command followed by the **no shut** command on the POS interface, the alarm of Critical on the standby PRE remains to be on (yellow). When seeing show logging, %C10K_ALARM-6-INFO: CLEAR CRITICAL POS <port> is seen. The interface appears up under "show interfaces pos", and traffic still flows.

  Conditions: This symptom is observed on a standby PRE.

  Workaround: Issuing the **shut** command followed by the **no shut** command on the interface on the now active PRE will clear the alarms.

- CSCsb48269

  Symptoms: A 24che1t1 interface line protocol does not come up.

  Conditions: This problem occurs when issuing the **shutdown** command followed by the **no shutdown** command on the corresponding controller with the interval of more than one minute.

  Workaround: This problem is restored by issuing the **shutdown** command followed by the **no shutdown** command on the interface.

- CSCsb49313

  Symptoms: The Cisco 10000 series ESR 24-port E1/T1 line card supports increments of 110 feet. However, increments of 110 feet can not be configured in Cisco IOS Release 12.2(27)SBB.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(27)SBB.

  Workaround: There is no workaround.

- CSCsb51621

  Symptoms: Not able to modify the UBR shaping rate.

  Conditions: This symptom occurs when the rate of the shaped UBR is modified.

  Workaround: Removing the VC where the UBR is applied and creating the new VC and applying the required UBR rate.

- CSCsb52900

  Symptoms: An inconsistency may occur in the outlabel information that is used by BGP and MPLS forwarding.

  Conditions: This symptom is observed when there are two route reflectors (RRs) that advertise the same route and when one of the routes is the best path. The symptom occurs when the following conditions are present:

  - The PE router that is the source restarts, causing the prefix to be readvertised with a new label.
  - The RR that forms the non-best path delays the withdrawal and readvertisement of the prefix, for example, because the RR has a heavy load.

  This situation causes BGP to function with the new label but MPLS forwarding to function with the old label.

  Workaround: Enter the **clear ip route** *network* command for the affected prefix.

- CSCsb54070

  Symptoms: According to the URL http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/lnc d-sw/tobleros.htm, AU-3 and AU-4-TUG-3s are based on the higher order path and do not operate independently, but operate in groups of three. If you shutdown any AU-3 or AU-4-TUG-3 controller, the other two controllers on the same SONET port are also shut down.

  Conditions: In Cisco IOS Release 12.0(25)SX, the au-4-tug-3 controller does not have to configure anything. It would go admin down if you shut one of three controllers down.

  In Cisco IOS Release 12.2(27)SBB, the au-4-tug-3 controller has to have “mode” configured before it would go admin down.

  Workaround: There is no workaround.

- CSCsb55208

  Symptoms: A Cisco 10000 series crashes in the c10k_collect_if_qos_stats_dma function.

  Conditions: This symptom is observed when there are create-on demand VCs. (The periodic statistics collector is always on.)

  Workaround: There is no workaround.

- CSCsb58192

  Symptoms: The following error message is displayed after Power OFF/ON, reload or switchover:

  ```
  %ISSU-3-DEBUG_ERROR: Passing an invalid session ID (0) to ISSU debug macro
  -Traceback= 61213D18 613F31B8 613F171C 613F2240
  ```

  Conditions: This symptom occurs with PRE2-RP with SSO mode. An error message is outputted with one of the following three patterns:
  1.PowerOFF/ON
  2.redundancy force-switchover Main-PRE
  3.reload

  Workaround: There is no workaround.

- CSCsb58719

  Symptoms: With hard loops, the line protocol on random T1s on DSEs 7-12 stays down to an externally provided loop.

  Conditions: This symptom occurs when you have an external loopback facing the routers.

  Workaround: There is no workaround.

- CSCsb60886

  Symptoms: A Cisco 10000 series line card reloads continuously.

  Conditions: This symptom is observed on a Cisco 10000 series when the PRE is booted.

  Workaround: There is no workaround.

- CSCsb65610

  Symptoms: After a PRE switchover has occurred, a PE router stops switching packets to a remote PE router.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB and that functions as a PE router when the remote PE router also runs Release 12.2(27)SBB. The symptom does not occur when the remote PE router runs Release 12.0(25)SX6.

  Workaround: Reload the router or disable the PXF engine on the router.

- CSCsb69761

  Symptoms: A 1-port OC-12 ATM line card that is inserted into the chassis may reload continuously.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: To stop the line card from reloading, reload the router with the line card in the chassis. To prevent the symptom from occurring, enter the **card** *slot/subslot* **1oc12atm-1** command to the configuration before you insert the line card.

- CSCsb71982

  Symptoms: The PXF engine may crash because of the following DMA Toaster Fault error:

  ```
  Toaster IWRA Exception
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB or Release 12.3(7)XI when a packet enters via an interface that is configured for ingress NetFlow and when the packet requires IP fragmentation when it enters the outbound interface.

  Workaround: Disable ingress NetFlow.

- CSCsb80316

  Symptoms: When you attempt to create an E1 link with more than 24 timeslots, the E1 link is not created and an error message is generated.

  Conditions: This symptom is observed on a Cisco 10000 series when you attempt to create an E1 link with more than 24 timeslots on a 1-port channelized OC-12 line card that is configured for SDH or SONET or on a 4-port channelized OC-3 line card that is configured for SONET.

  Workaround: There is no workaround.

- CSCsb82250

  Symptoms: After you reload a PXF engine or after a PXF engine crashes and reloads, traffic forwarding may stop in an environment with label POP and disposition operations.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a P router in an environment with label POP and disposition operations. The symptom generally does not affect a router that functions as a PE router, except if the PE router is configured with the MPLS VPN--Carrier Supporting Carrier feature.

  Workaround: Initiate a switchover to the standby PRE.

First Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interfaces that are configured for MPLS, that is, the interfaces that have the **mpls ip** command enabled.

Second Alternate Workaround: Reload the router.

- CSCsb88374

  Symptoms: The initial switchover of an image could result in longer than expected traffic outage.

  Conditions: This symptom occurs on a Cisco 10000 series router with 2 PREs that are running Cisco IOS Release 12.2(27)SBB1 with an ATM line card.

  Workaround: There is no workaround.

- CSCsb98303

  Symptoms: After an ISSU Runversion command is run on a router, the 6-port CT3 line card gets into a state where the Line Protocol will not come up.

  Conditions: This symptom is observed on a Cisco 10000 series router that is doing an ISSU upgrade from Cisco IOS Release 12.2(27)SBB to 12.2(27)SBB1. The router will only see this issue if a 6CT3 line card is in the router.

  Workaround: There is no workaround.

  Further Problem Description: If this problem happens, after the ISSU process is complete, the line card will have to be reset to get full functionality to return to the router. This can be done with the **hw-module slot X/Y reset** command.

- CSCsc01471

  Symptoms: ATM interface transitions may result in an error message such as the following:

  ```
  Sep 28 11:49:20.703 UTC: %C10KATM-3-INTERNAL: C10K ATM internal error,
  c10k_atm_check_slot_sync, no slotptr from hwidb ATM7/0/2 0
  -Traceback= 6050A81C 600BE1C4 600BE2A4 600C91FC 600B4B7C 601C6C4C 601C5D40 601EDAB4
  604B5BEC 60179BF4 604CF22C 605E551C 605E5508
  ```

  Conditions: This symptom occurs on the ATM only, if using or configuring an ATM port greater than 0.

  Workaround: There is no workaround.

  Further Problem Description: No effect in most circumstances but may lead to 10-12 second SSO switchover for the s/first switchover after a cold boot.

TCP/IP Host-Mode Services

- CSCei45898

  Symptoms: BGP Nonstop Routing sessions do not re-establish quickly enough after an NSF switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with low keepalive and holdtime values.

  Workaround: There is no workaround.

- CSCej00914

  Symptoms: It takes too long to execute the **show tcp ha connection** command.

  Conditions: This symptom is observed on a Cisco router only when the **ip domain lookup** command is enabled.

Workaround: Enter the **no ip domain lookup** command. If this is not an option, there is no workaround.

Wide-Area Networking

- CSCei31669

  Symptoms: When the last link from a multilink group interface bundle is removed, the bundle interface state is not set to the DOWN state on the standby RP, causing the bundle interface state to be inconsistent after a switchover.

  Conditions: This symptom is observed on a Cisco router that is configured for MLP and SSO when the last link in a bundle is shut down by entering the **shutdown** command.

  Workaround: There is no workaround.

- CSCsb31573

  Symptoms: IP traffic does not pass on a router even though the subinterface is up.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a DS3 subinterface that functions as a Frame Relay NNI trunk and you do the same at the other side of the trunk. The symptom may be platform-independent.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface instead of the subinterface.

Open Caveats—Cisco IOS Release 12.2(27)SBB

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(27)SBB. All the caveats listed in this section are open in Cisco IOS Release 12.2(27)SBB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Interfaces and Bridging

- CSCeh64309

  Symptoms: A standby RP reloads unexpectedly.

  Conditions: This symptom is observed on a Cisco router when the IP address of a VLAN is deleted via the **default ip address** *ip-address mask* command during a TFTP copy operation in the wrong order in relation to the **default encapsulation dot1q** command.

  Workaround: Place the commands in the correct order as in the following example:

```
interface GigabitEthernet7/0/0.1
       default ip address 192.1.1.1 255.255.255.0
       default encapsulation dot1q
       ....
```

  Alternate Workaround: Remove the **default ip address** *ip-address mask* command entirely, as in the following example:

```
interface GigabitEthernet7/0/0.1
       default encapsulation dot1q
       ....
```

Note that in this example, the **default encapsulation dot1q** command actually deconfigures the **default ip address** *ip-address mask* command automatically.

IP Routing Protocols

- CSCsa79739

  Symptoms: A memory allocation failure traceback is logged on a router that is configured for BGP.

  Conditions: This symptom is observed when you enter the **clear ip bgp *** command and when there is a large number of routes.

  Workaround: Enter the **clear ip bgp soft** [**in**|**out**] command to generate a BGP update.

Miscellaneous

- CSCef15141

  Symptoms: The Priority Queueing (PQ) latency values (in milliseconds) are higher than twice the MTU plus 6 ms on 4-Mbps and 8-Mbps subrates of an 8-port clear channel E3/DS3 line card.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.3(7)XI or Release 12.2(27)SBB.

  Workaround: A workaround is to provision Cisco or Digital Link subrates as multiples of 358 kbps time slots:

  - For a 4-Mbps subrate, provision the Cisco or Digital Link interface as 3938 or 4296 kbps.
  - For an 8-Mbps subrate, provision the Cisco or Digital Link interface as 7876 or 8234 kbps.

  Further Problem Description: The Cisco DSU mode or Digital Link DSU mode breaks the available bandwidth into 358 kbps chunks (time slots). The line card uses a bandwidth multiple of 358 kbps that is larger than the user-configured 4-Mbps and8-Mbps subrates. This situation creates a bandwidth mismatch between the line card and PXF, causing backpressure.

- CSCef81909

  Symptoms: An MPLS interface may not drop some packets that are larger than the size of the configured MTU.

  Conditions: This symptom is observed on a Cisco 10000 series when the packet size is as follows:

  - For a POS interface, the packet size is between the size of the MTU and the size of the MTU plus 114 bytes.
  - For a GE interface, the packet size is between the size of the MTU and the size of the MTU plus 24 bytes.

  Workaround: There is no workaround.

- CSCeg16419

  Symptoms: A Frame Relay PVC remains active when the peer interface is shut down.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Frame Relay over MPLS when the AToM tunnel between the Frame Relay PVC and the peer interface is configured for LMI.

  Workaround: There is no workaround.

- CSCeg25335

  Symptoms: The accounting counters in the output of the **show interface** *type slot/port* **accounting** command are not updated on a PE router.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that is configured for AToM AAL5 local switching.

  Workaround: There is no workaround.

- CSCeg54016

  Symptoms: Priority Queuing (PQ) traffic may be dropped from an ATM VC.

  Conditions: This symptom is observed on a Cisco 10000 series when LFIoATM is configured together with traffic shaping on a per-VC/VP basis, when the VPs are overdriven, and when interleaving is not enabled on the ATM VC.

  Workaround: Enable interleaving on the ATM VC.

  Further Problem Description: We recommend that you do not use the configuration that is described in the Conditions above. If you do, ensure that interleaving is enabled on the ATM VC. When interleaving is disabled, the priority queue becomes a multilink packet queue and does not receive preferential treatment on the bundle.

- CSCeg56206

  Symptoms: Multilink statistics are not propagated to a Frame Relay DLCI when LFIoFR is enabled on the MLP interface.

  Conditions: This symptom is observed on a Cisco 10000 series. The symptom occurs only for DLCI statistics; multilink statistics are correct.

  Workaround: There is no workaround.

- CSCeg58121

  Symptoms: The output of the **show pxf cpu queue** *interface* command does not show any dequeued packets for Priority Queueing (PQ).

  Conditions: This symptom is observed on a Cisco 10000 series that is configured LFIoFR and occurs after you have entered the **microcode reload pxf** command.

  Workaround: There is no workaround.

  Further Problem Description: We do not recommend that you use the **microcode reload pxf** command in a production network.

- CSCeg78563

  Symptoms: The link use may be as low as 94 percent of the expected rate on low-speed links that have FRF.12 enabled.

  Conditions: This symptom is observed under extremely rare conditions on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCeg90091

  Symptoms: Targeted LDP sessions flap.

  Conditions: This symptom is observed on a Cisco 10000 series when Virtual Circuit Connection Verification (VCCV) ping traffic exceeds 2500 pps.

  Workaround: Lower the VCCV ping traffic rate.

- CSCeh09708

  Symptoms: You cannot attach a Frame Relay map class to a VRF interface after you have removed an existing Frame Relay map class.

  Conditions: This symptom is observed on a Cisco 10000 series that has an input policy on a PVC via a Frame Relay map class and an output policy on a subinterface of the PVC.

  Workaround: Either attach both the input and output policies to the subinterface or place both the input and output policies in the Frame Relay map class.

- CSCeh22837

  Symptoms: The following error message is generated repeatedly on a standby PRE:

  ```
  Cannot insert into AVL tree
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs that function in SSO or RPR+ mode.

  Workaround: There is no workaround. However, the message is of a cosmetic nature only.

- CSCeh27726

  Symptoms: The creation of an E1 controller is not blocked when T1 controllers are already configured on the same port, causing all T1 controllers to be changed to E1.

  Conditions: This symptom is observed on a Cisco 10000 series when you create an E1 controller on a port of a channelized OC-12 line card.

  Workaround: Only controllers of the same type are supported on the same port: do not change the type of a controller to E1 when other controllers on the same port are configured for T1.

- CSCeh34253

  Symptoms: The AToM statistics byte count in the output of **show mpls forwarding-table** command is incorrect.

  Conditions: This symptom is observed on a Cisco 10000 series when traffic is sent over an AToM VC.

  Workaround: There is no workaround.

- CSCeh38970

  Symptoms: The Count of APS (COAPS) switchovers register on an interface of an OC-48 POS line card does not increment after an APS switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that has OC-48 POS interfaces that are configured for APS configuration when you enter the **aps force** command to initiate a switchover from a working interface to a protect interface.

  Workaround: There is no workaround.

- CSCeh39027

  Symptoms: The output of the **show pxf cpu subblock** command may show a negative number of interleaved packets or bytes when Link Fragmentation and Interleaving (LFI) is disabled and the interface is passing traffic.

  Conditions: This symptom is observed on a Cisco 10000 series that has an LFI over ATM (LFIoATM) or LFI over Frame Relay (LFIoFR) interface.

  Workaround: There is no workaround. However, the symptom relates to counters only and does not affect the operational behavior of the router.

- CSCeh39660

  Symptoms: A standby PRE continues to reset when the auto boot image is not properly configured or when the PRE1 does not find the auto boot image.

  Conditions: This symptom is observed on a Cisco 10000 series during a major upgrade from a PRE1 to a PRE2 in a redundant system.

  Workaround: Ensure that the auto boot image is properly configured.

- CSCeh40097

  Symptoms: The link use may be between 90 and 95 percent of the expected rate on links that are configured for LFIoFR.

  Conditions: This symptom is observed under very rare conditions on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCeh48397

  Symptoms: When you enter the **show aps** command for an active PRE and a standby PRE that function in SSO mode while the standby PRE is in the HOT-STANDBY state, the automatic protection switching (APS) state may show as mismatched for the PREs.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with SONET line cards and that runs in SR-APS mode.

  Workaround: There is no workaround.

- CSCeh49788

  Symptoms: Large ICMP packets fail to pass over an MLP over ATM link or MLP over Frame Relay link. This situation also causes pings of large packets to fail.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in an MLP over ATM or MLP over Frame Relay configuration when the ICMP packets have a size of at least 3000 bytes and consist of at least three IP fragments.

  Workaround: There is no workaround.

- CSCeh51775

  Symptoms: Multilink VCs that are configured for MLPoATM, bundles, VCs, and VAI interfaces may flap continuously.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **microcode reload pxf** command.

  Workaround: There is no workaround.

  Further Problem Description: We do not recommend that you use the **microcode reload pxf** command in a production network.

- CSCeh54019

  Symptoms: During an upgrade from a PRE1 to a PRE2, the following error messages are generated on the PRE2 console:

  ```
  Failed to assert Cutover alarm for RP A
  %IPCGRP-3-ERROR: outgoing IPC bypass failed:
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ```

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround. However, the error messages do not affect the upgrade.

- CSCeh64464

  Symptoms: An MLP over ATM member link of a multilink bundle may remain down.

  Conditions: This symptom is observed on a Cisco 10000 series when you remove and return an MLP over ATM member link to an active multilink bundle or place the MLP over ATM member link in another multilink bundle.

  Workaround: First shut down the multilink bundle before you add or remove the member link.

- CSCeh70291

  Symptoms: When you enter the **redundancy force-failover main-cpu** privileged EXEC command on a Cisco 10000 series that is configured with two Performance Routing Engines (PREs), an automatic protection system (APS) switchover occurs on SONET line cards, which is incorrect behavior.

  Conditions: This symptom is observed on a Cisco 10000 series with redundant PREs when APS is configured on SONET line cards and when the following sequence of events occurs:

  1. You enter the **aps force pos** *slot/subslot/port* **from working** interface configuration command on the Cisco 10000 series and its peer.
  2. You enter the **show aps** EXEC command. The output displays the active channels for both routers.
  3. You enter the **redundancy force-failover main-cpu** privileged EXEC on one of the routers, causing an APS switchover to occur on this router.

  Workaround: There is no workaround. However, when the symptoms occurs, there is no loss of data.

- CSCeh76090

  Symptoms: A Cisco 10000 series may crash when you swap flash cards.

  Conditions: This symptom is observed very rarely and only after repeated (more than 80) instances of removing and reinserting a flash card.

  Workaround: Remove the flash card quickly, wait for a few seconds, and then reinsert the flash card quickly.

- CSCeh79117

  Symptoms: A memory allocation (malloc) error occurs and tracebacks are generated on a Cisco 10000 series.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router and that is configured with 750 VRFs and 250,000 VPNs when a remote peer is reloaded.

  Workaround: There is no workaround.

- CSCeh79964

  Symptoms: A PE router loses L3VPN connectivity with a CE router.

  Conditions: This symptom is observed on a Cisco 10000 series when a VLAN is configured with an AToM VC, the VLAN subinterface is deleted, and then the same VLAN ID is used for a L3VPN connection.

  Workaround: Do not use the same VLAN ID for the L3VPN connection between the PE router and the CE router but configure a different VLAN ID.

- CSCeh85664

  Symptoms: The SSO performance is slow (longer than 4 seconds) with an OC-48 POS line card.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs when the mode of the OC-48 POS line card is not set.

Workaround: Configure the OC-48 POS line card to function in POS mode.

- CSCeh93149

  Symptoms: All packets may be dropped from an MVPN when traffic is switched to a data MDT.

  Conditions: This symptom is observed very rarely on a Cisco 100000 series that functions as a PE router only after the direction of the traffic flow between the Cisco 10000 series and another PE router is reversed or with bidirectional traffic when both unicast and multicast VRFs are configured on the Cisco 10000 series and bidirectional traffic is sent on the MVPN.

  Workaround: There is no workaround.

- CSCei04496

  Symptoms: The expected traffic convergence time after a second switchover is 90 seconds but the actual traffic convergence time is more than 150 seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PREs and that is configured with 4000 interfaces. The PREs function in RPR+ mode.

  Workaround: There is no workaround.

- CSCei07913

  Symptoms: Traffic that passes through a Cisco 10000 series may not recover after an SSO switchover when MVPNs are configured.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs and that functions as a PE router when the customer Rendezvous Point is located away from the traffic source.

  Workaround: Configure the customer Rendezvous Point close to the traffic source. Also, enter the **ip pim register-rate-limit 1** command to facilitate traffic recovery for low MVPN traffic levels.

  Further Problem Description: After performing an SSO switchover, all multicast packets are punted, causing the use of the CPU to increase, and in turn, causing BGP sessions to flap and traffic to drop.

- CSCei09643

  Symptoms: The configuration of the secondary PRE differs from the configuration of the primary PRE.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with AToM VCs over ATM AAL5 PVCs.

  Workaround: Initiate a switchover to synchronize the primary and secondary PREs.

- CSCei13877

  Symptoms: When a protection line card is removed and replaced, traffic is interrupted for a period between one and ten seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has an active POS APS configuration with OC-3 POS or OC-12 POS line cards.

  Workaround: There is no workaround.

- CSCei16493

  Symptoms: When a Single router-APS (SR-APS) configuration is removed and re-applied, continuous tracebacks are generated on the standby PRE2.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PRE2s that function in SSO mode and 4-port channelized STM-1 (ESR-4CHSTM1) line cards that function in linear 1+1 APS mode. APS is configured by entering the **associate slot** *slot_one slot_two* command.

Workaround: To clear the symptom, initiate a PRE switchover by entering the **redundancy force-switchover main-cpu** command. Note, however, that the tracebacks do not impact the functionality of the router nor interrupt traffic.

- CSCei22506

  Symptoms: When you change the configuration from, for example, HDLC to PPP, the **no framing**, **no path**, or **no aug mapping** command is typically used to clear the controller setting. When the controller is reconfigured after having been cleared, an ifindex traceback is generated on both the active and standby PRE. When the ifindex is not synchronized properly to the standby PRE, an SSO switchover causes prolonged traffic outage of between 10 and 20 seconds.

  Conditions These symptoms are observed on a Cisco 10000 series that is configured with redundant PREs.

  Workaround: Do not clear the controller. If you must clear the controller, reset the standby PRE after you have reconfigured the controller to prevent prolonged traffic outages during SSO switchovers.

- CSCei23628

  Symptoms: You cannot copy a startup configuration file with a large size to the NVRAM of a standby PRE2 during an upgrade from a PRE1 to a PRE2.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs that function in RPR mode when the size of the startup configuration file is larger than the size of the NVRAM of the PRE1

  Workaround: Perform a second copy operation.

- CSCsa59560

  Symptoms: A provider (P) router may drop a packet that is larger than 1472 bytes.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a P router and that is connected to a provider edge (PE) router in the following configuration:

  - A source transmits a packet that is larger than 1472 bytes via an IP connection to the PE router.
  - The PE router forwards the packets through an MVPN tunnel over a Gigabit Ethernet connection to the P router, which is the next hop for the PE router.
  - The size of the packet exceeds the default MTU of the MVPN tunnel.

  Workaround: There is no workaround.

- CSCsa65102

  Symptoms: When you change the encapsulation on a Gigabit Ethernet subinterface, the service policy that is attached to this subinterface may be removed.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB and that is configured with a PRE2.

  Workaround: There is no workaround.

- CSCsa67594

  Symptoms: Low link usage may occur on a Cisco 10000 series that is configured with a PRE2.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB on low-speed links (typically 128 Kbps or lower) that are configured with a priority queue and several other user queues. The symptom occurs only with certain QoS configurations and traffic profiles.

  Workaround: There is no workaround.

- CSCsa71096

  Symptoms: When a high number of QoS policy maps is configured, it may take a long time for a router to activate all of them.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB when a very large amount (thousands) of QoS policy maps and class maps are configured and applied to interfaces.

  Workaround: There is no workaround.

  Further Problem Description: QoS policy maps are compiled on the Cisco 10000 series, therefore compilation time is a factor in policy map activation. Each policy map is compiled individually, so the more policy maps are configured and applied, the longer it will take for all of them to be activated on the router. When a policy map is compiled, it is activated immediately, so some policy maps are activated very quickly while others may take several minutes to become active. It takes about 0.3 seconds to compile a policy map on a Cisco 10000 series.

- CSCsa72673

  Symptoms: If you apply a service policy to Fast Ethernet interface 0/0/0 on a Cisco 10000 series, the ciscoCBQosMIB cbQosPoliceStatsTable and csQosTSStatsTable may be empty.

  Conditions: This symptom is observed when you use SNMP to poll the CISCO-CLASS-BASED-QOS-MIB and when there is a service policy attached to Fast Ethernet interface 0/0/0.

  Workaround: Remove the service policy from Fast Ethernet interface 0/0/0.

- CSCsa74551

  Symptoms: A Cisco 10000 series may display CPUHOG messages when you modify the configuration of a policy map.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB only when the policy map is applied to thousands of interfaces.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is harmless and does not affect the proper functionality of the router.

- CSCsa82771

  Symptoms: T1 and T3 clocks do not switch to the internal source when LOF-DS3, AIS-DS3, LOF-DS1, or AIS-DS1 alarms occur.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card.

  Workaround: There is no workaround.

- CSCsa82775

  Symptoms: An AIS-DS3 alarm is not detected at the T3 controller level.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card.

  Workaround: There is no workaround.

- CSCsa86548

  Symptoms: The parent of a hierarchical policing policy that is attached as an output policy to an interface of 24-Port T1/E1 line card may not increment its packet, conform, exceed and violate counters.

Conditions: This symptom is observed on a Cisco 10000 series only when Frame Relay encapsulation is configured.

Workaround: There is no workaround.

Further Problem Description: This symptom is related to counters only; the policer behavior and functionality are not affected.

- CSCsa89073

  Symptoms: When an LP-RDI alarm occurs, the TU controller goes down and the E1 controller remains up and does not report any errors. The TU controller should remain up under this alarm condition.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card when the E1 controller is configured under an AU-4 via SDH framing.

  Workaround: There is no workaround. However, the transmission of data is not affected.

- CSCsa96774

  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.

- CSCsb00534

  Symptoms: When FRF.12 is applied to thousands of DLCIs, a Cisco 10000 series may generate CPUHOG error messages and tracebacks.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **microcode reload pxf** command.

  Workaround: There is no workaround.

  Further Problem Description: We do not recommend that you use the **microcode reload pxf** command in a production network.

- CSCsb03230

  Symptoms: A Cisco 10000 series may crash when you reload the router.

  Conditions: This symptom is observed very rarely when PXF debugging is enabled.

  Workaround: Do not enable PXF debugging.

- CSCsb03458

  Symptoms: The performance of a Cisco 10000 series may be briefly affected when an ATM PVC configuration is modified or when an ATM PVC is deleted and recreated.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE2 only when the router has both ATM interfaces and multicast enabled. The symptom occurs when you enter the **no pvc** interface configuration command followed by the **pvc** interface configuration command to change the configuration of an ATM PVC or to delete and recreate and ATM PVC.

Workaround: When you change the ATM PVC or when you delete and recreate an ATM PVC, enter only the **pvc** interface configuration command, that is, without first entering the **no pvc** interface configuration command.

- CSCsb03849

  Symptoms: A Cisco 10000 series fails to boot after you have reloaded the router.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB when the **microcode pxf** *ucode filename* command is part of the startup configuration.

  Workaround: Remove the **microcode pxf** *ucode filename* command from the startup configuration.

- CSCsb04236

  Symptoms: On a Cisco 10000 series, if an interface is configured for Link Fragmentation and Interleaving (LFI), traffic sharing between configured queues in QoS profiles may not be proportional to the configured values.

  Conditions: This symptom is observed only for links that have LFI enabled and for which the bandwidth ratio between the queues is not within 5 percent of the configured value. The symptom may affect LFIoFR, LFIoATM, LFIoMLP, and FRF.12.

  Workaround: There is no workaround.

  Further Problem Description: Links that do not have LFI configured are almost always within 5 percent of the configured bandwidth.

- CSCsb04655

  Symptoms: Serial and POS interfaces that are configured for Frame Relay may flap during the ISSU process.

  Conditions This symptom is observed on a Cisco 10000 series that is configured with redundant PREs.

  Workaround: There is no workaround.

- CSCsb08466

  Symptoms: On a Cisco 10000 series that is configured with full-rate Gigabit Ethernet (GE) interfaces, traffic sharing between configured queues in QoS profiles may not be proportional to the configured values.

  Conditions: This symptom is observed only with very high speed interfaces such as GE and OC-48 interfaces for which the bandwidth ratio between queues may not be within 5 percent of the configured value.

  Workaround: There is no workaround.

  Further Problem Description: Lower speed interfaces are almost always within 5 percent of the configured bandwidth.

- CSCsb08527

  Symptoms: When multiple traps are generated in a short period of time, the default *length* argument of 10 of the **snmp-server queue-length** *length* command may cause some traps to be dropped.

  Conditions: This symptom is observed on a Cisco 10000 series when you use an SNMP host to monitor traps.

Workaround: Enter another value for the *length* argument of the **snmp-server queue-length** *length* command: enter a number that is greater than 10, in the order of 50 to 100.

- CSCsb08587

  Symptoms: Drops may occur on the priority queue when low latency queueing (LLQ) is configured and extreme traffic conditions occur.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB. The priority queue starts to drop a small portion of the packets at 900,000 pps or a higher rate.

  As an example, the symptom would occur on a Gigabit Ethernet interface with a priority queue configured with a 75-percent policer when small packets are sent at 900,000 pps or a higher rate.

  Workaround: There is no workaround.

- CSCsb10143

  Symptoms: A small number of packets may be dropped from a Gigabit Ethernet (GE) interface.

  Conditions: This symptom is observed on a Cisco 10000 series when you send packets with sizes from 64 to 87 bytes at line rate and when QoS is enabled on the GE interface.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs only when user queues are applied to the GE interface. The observed drop rate is very low (6 pps).

- CSCsb10145

  Symptoms: When you enter the **issu runversion** command and the command execution is followed by a switchover, the following error message and traceback are generated:

  ```
  %IPCGRP-3-CMDOP: IPC command 402 (slot2/0): line card ipc is disabled - dropping
  non-blocking ipc command
  ```

  ```
  Traceback= 60509B80 60696FBC 60697AD8
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 6-port channelized T3 line card.

  Workaround: There is no workaround. However, the ISSU operation and switchover succeed.

- 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.

- CSCsb10789

  Symptoms: A Cisco 10000 series that is configured for Multilink PPP (MLP), LFI, and WRED may generate the following error messages and traceback:

  ```
  %C10K_MULTILINK_STATE-3-EREVENT: cannot deactivate member at this time
  ```

  ```
  %C10K_MULTILINK_USER_WARNING-2-CRITEVENT: member incapable of clean removal at this
  time
  ```

  ```
  %GENERAL-3-EREVENT: clear bundle data failed
  ```

  ```
  -Traceback= 60505148 6102CF2C 6102CF5C 6102A88C 6102A930 609F15C0 609EC164 605B3E5C
  605B3FB8
  ```

  Conditions: This symptom is observed only when you enter the **microcode reload pxf** command.

Workaround: There is no workaround. However, the functionality of the router is not affected.

- CSCsb12456

  Symptoms: When you copy a large configuration via TFTP to a channelized OC-12 line card (with 768 interfaces), the interprocess communication (IPC) channel to the channelized OC-12 line card is dropped, and the log shows messages similar to the following:

  ```
  %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot 2/0.
  %IPCOIR-2-CARD_UP_DOWN: Card in slot 2/0 is down.
  Notifying 1choc12-1 driver.
  %IPCGRP-3-CMDOP: IPC command 405 (slot2/0): line card ipc is disabled -
  dropping non-blocking ipc command
  -Traceback= 60504368 6069013C 60690C58
  %C10K_ALARM-6-INFO: ASSERT CRITICAL slot 2 Card Stopped
  Responding OIR Alarm - subslot 0
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs that function in SSO mode and with one or more channelized OC-12 line cards.

  Workaround: There is no workaround. However, the line card recovers and reloads on its own a few seconds after the symptom has occurred.

- CSCsb13223

  Symptoms: Traffic may be unstable and the overall link use may be poor when you configure quality of service (QoS) user queues by entering the **bandwidth remaining percent** *value* command.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB when the following conditions are present:

  - The links are between 100 Mbps and 900 Mbps (for example, STM1/OC3 or STM4/OC12 links).
  - There are more than three user queues provisioned via the **bandwidth remaining percent** *value* command.
  - Traffic is sent to all the queues.

  Workaround: Enter the **maximize-utilization** command on the queues that are provisioned via the **bandwidth remaining percent** *value* command.

  Alternate Workaround: Do not enter the **bandwidth remaining percent** *value* command. Rather, enter the **bandwidth percent** *value* command.

  Further Problem Description: The symptom does not occur on other interfaces such as E3/T3 and STM4/OC12. The symptom is specific to interfaces that are configured between 100 Mbps and 900 Mbps.

- CSCsb13268

  Symptoms: Some counters may not be cleared when you enter the **clear counters** command.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for FRF.12.

  Workaround: There is no workaround.

- CSCsb15086

  Symptoms: When you enter the **issu runversion** command and the command execution is followed by a switchover, the following error message and traceback are generated on the new active PRE:

  ```
  %IPC-4-NOPORT: Port Not Found. 130000 --> 10010, Index:8, Seq: 41113, flags: 0,
  size: 36
  -Traceback= 605071F4 606E569C 606E60A4 611B06C4 611B0828 605E1FB4 605E1FA0
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs.

  Workaround: There is no workaround. However, the ISSU operation and switchover succeed.

- CSCsb18877

  Symptoms: The values of the cRFcRFStatusFailoverTime.0 and cRFStatusPeerStandByEntryTime.0 objects of the CISCO-RF-MIB are always zero.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SNMP when you use the CISCO-RF-MIB to monitor the cRFStatusFailoverTime and cRFStatusPeerStandByEntryTime objects.

  Workaround: There is no workaround.

- CSCsb19052

  Symptoms: Multilink interfaces remain down in an LFI over ATM configuration, there is high CPU use, and a “Queue ID exhausted” error message is generated.

  Conditions: These symptoms are observed on a Cisco 10000 series when the total number of queues on the router is close to 128,000, which is the maximum number of supported queues. LFI over ATM does not scale to this number.

  Workaround: There is no workaround. Note that up to 88,000 queues function successfully in an LFI over ATM configuration.

- CSCsb19101

  Symptoms: Seven to eight seconds of traffic loss occurs during an initial switchover after you have booted the router. During subsequent switchovers, the traffic loss lasts less than three seconds. The traffic loss occurs only on ATM interfaces.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB, that is configured for SSO, and that has ATM interfaces.

  Workaround: There is no workaround.

- CSCsb19602

  Symptoms: When you enter the **hw-module secondary reset** command, an ALIGN-3-TRACE error message is generated.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PRE2s.

  Workaround: There is no workaround.

  Further Problem Description: The traceback does not appear to impact the functionality of the router.

- CSCsb19856

  Symptoms: FRF.12 may not function on an interface. Even though a policy map is configured, it is missing from the interface.

Conditions: This symptom is observed on Cisco 10000 series that is configured with redundant PREs and about 4095 DLCIs, that is, the maximum number supported. Even though the interface has all the required commands in the running configuration, the output of the **show policy-map interface** *interface* command does not show a policy map attached to the interface.

Workaround: Load the initial configuration with only one PRE in the active state and then bring up the secondary PRE.

- CSCsb19966

  Symptoms: After a VBR-NRT VC is changed to a UBR circuit, the SCR bandwidth is not released.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Delete the VBR-NRT VC and then recreate the VC as a UBR circuit.

- CSCsb20224

  Symptoms: When you boot a Cisco 10000 series, the following error message may be generated:

  ```
  %IP-4-DUPADDR: Duplicate address 23.4.2.254 on FastEthernet0/0/0, sourced by
  0009.b688.df00
  ```

  Conditions: This symptom is observed on a Cisco 100000 series that is configured with redundant PRE2s.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not appear to impact the functionality of Fast Ethernet interface 0/0/0.

- CSCsb21715

  Symptoms: When you place a 24-port T1/E1 line card in T1 mode and you configure the controller (in the example below, t1 5/0/0), the following error message is generated:

  ```
  controller t1 5/0/0
  %ERROR: Standby doesn't support this command                              ^
  % Invalid input detected at '^' marker.
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB and that has redundant PREs that function in RPR+ mode.

  The symptom does not occur when the 24-port T1/E1 line card functions in E1 mode, nor does it occur when the router functions in SSO mode.

  Workaround: If this is an option, configure the router to function in SSO mode. If this is not an option, there is no workaround.

  Further Problem Description: When you configure the card mode, the standby PRE receives the synchronization message but does not execute it, causing the active PRE to function in T1 mode and the standby PRE to function in E1 mode.

- CSCsb62847

  The following caveat is neither open nor resolved but closed:

  Symptoms: When you perform an ISSU downgrade from a Cisco IOS Release later than Release 12.2(27)SBB, for example, from Release 12.2(27)SBB1, to Release 12.2(27)SBB, traffic may fail for a period of 30 to 90 seconds.

  Conditions: This symptom is observed on a Cisco router with routing protocols that have keepalives and holddown timers configured. For example, the symptom occurs when OSPF has default timers configured and when BGP has 10-second keepalives and 30-second holddown timers configured.

The symptom occurs when the active PRE runs Release 12.2(27)SBB1, when the standby PRE runs Release 12.2(27)SBB, when the ISSU system state is “runversion”, and when you enter the **abortversion** command, initiating a switchover so that the standby PRE that runs Release 12.2(27)SBB becomes the active PRE.

Workaround: Increase the holddown timers for all routing protocols. If this is not an option, there is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(27)SBA6

Cisco IOS Release 12.2(27)SBA6 is a rebuild release for Cisco IOS Release 12.2(27)SBA. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBA6 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCei77083

  Symptoms: A spurious memory access may be generated on an RSP when a VIP that is in a disabled or wedged condition is recovered because of a Cbus Complex or microcode reload.

  Conditions: This symptom is observed on a Cisco 7500 series that has a VIP that is in a disabled or wedged condition after the router has booted.

  Workaround: There is no workaround.

- CSCsb67916

  Symptoms: SNMP traps are received that indicate that an “authorization failure” has occurred with an offending source IP address of 0.0.0.0.

  Conditions: This symptom is observed on a Cisco platform that runs cisco IOS Release 12.2SXD. However, the symptom may also occur on a Cisco platform that is configured for SNMP and that runs another Cisco IOS software release.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCeb66519

  Symptoms: A slow memory leak occurs when the parser is invoked.

  Conditions: This symptom is platform- and release-independent. For platforms that support HCCP N+1 Redundancy, a leak with a size of 10KB to 20KB occurs each time that a static configuration synchronization is performed.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeh33504

  Symptoms: A router terminates 102,000 VPNv4 routes but route reflectors (RRs) report only a a subset of the total.

Conditions: This symptom is observed on a Cisco MGX RPM-XF that runs Cisco IOS Release 12.3(11)T4 when 204 routes are configured per VRF over 496 VPNs (one VPN has about 1000 routes). However, Cisco MGX RPM-PRs that function as RRs show that only 76245 routes are terminated on the Cisco MGX RPM-XF. The symptom is platform-independent and may also occur in other releases.

Workaround: There is no workaround.

- CSCei26899

  Symptoms: When you reset a BGP peer, some prefixes are missing.

  Conditions: This symptom is observed on a Cisco MGX8850 RPM-XF that runs Cisco IOS Release 12.3(11)T. However, the symptom is platform-independent and may also occur in other releases.

  Workaround: There is no workaround.

- 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.

- CSCsa87473

  Symptoms: A BGP speaker may fail to send all of its prefixes to a neighbor if the neighbor sends a refresh request to the BGP speaker at the same time that the BGP speaker is generating updates to the neighbor. This situation causes the neighbor to miss some prefixes from its BGP table.

  Conditions: This symptom may occur between any pair of BGP speakers.

  A common scenario is that a VPNv4 PE router is reloaded and then fails to learn all prefixes from its route reflector (RR). In this configuration, the symptom occurs when the processing of a VRF configuration causes the PE router to automatically generate a route-refresh request to the RR, while the RR is still generating updates to the PE.

  Workaround: There is no workaround.

- CSCsc59089

  Symptoms: BGP does not advertise all routes to a peer that sends a route-refresh request.

  Conditions: This symptom is observed under the following conditions:

  – The router is in the process of converging all of its peers and has updates ready in the output queue for the peer.

  – The peer sends a route-refresh request to the router. This may occur when the **clear ip bgp * soft in** command is entered on the peer or when a VRF is added to the peer.

  – The router processes the route-refresh request from the peer while the router still has updates in the output queue for the peer.

  In this situation, all of prefixes that are advertised by the unsent updates in the output queue for the peer are lost.

Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip bgp * soft out** command on the router to force the router to send all updates to its peers.

Miscellaneous

- CSCee11426

  Symptoms: Local switching is supported only when IP CEF enabled.

  Conditions: This symptom is observed on a Cisco router when IP CEF is enabled, when a local switching connection is brought up through a tunnel, and when IP CEF is subsequently disabled. In this situation, the tunnel does not come down as expected.

  Workaround: There is no workaround. However, a workaround is not required because the symptom does not affect normal operation or functionality of the router.

- CSCin88997

  Symptoms: A performance loss of up to 20 percent may occur on a router that is configured for Any Transport over MPLS (AToM).

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that run Cisco IOS Release 12.2SB but may also occur in other releases.

  Workaround: There is no workaround.

- 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.

- CSCsb54904

  Symptoms: Junk characters are generated when you set up a connection by using SSH v1.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBA. The symptom could also affect Release 12.2(27)SBC.

  Workaround: Use SSH v2.

- CSCsc65787

  Symptoms: A router may modify the interface MTU of an interface during the initialization process. In turn, this situation may modify layer 3 protocol MTUs (such as IP MTUs), preventing OSPF, IS-IS, or other L3 protocols from coming up.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image of Release 12.2SB that includes the fix for caveat CSCsa73817 when the MPLS MTU is larger than the interface MTU.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa73817. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Configure the interface MTU to be equal to or larger than the MPLS MTU and configure the IP MTU to the desired value.

- 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.

Resolved Caveats—Cisco IOS Release 12.2(27)SBA5

Cisco IOS Release 12.2(27)SBA5 is a rebuild release for Cisco IOS Release 12.2(27)SBA. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBA5 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCej87446

  Symptoms: Duplicate subinterfaces may be created when you enter a range of subinterfaces in the **interface range** command.

  Conditions: The symptom is observed on a Cisco platform when you use the **interface range** command to create a range of subinterfaces.

  Workaround: Do not use the **interface range** command to create a range of subinterfaces.

- CSCsc44237

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: A switch or router that is configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

     The output of the **show processes memory** command shows that the "ATM PA Helper" process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

     Condition 1: This symptom is observed on a Cisco switch or router that runs a Cisco IOS software image that contains the fixes for caveats CSCeh04646 and CSCeb30831. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh04646 and http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb30831.

     Cisco IOS software releases that are not listed in the "First Fixed-in Version" fields at these locations are not affected.

     Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

  2. Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory.

The output of the **show processes memory** command shows that the "PIM process" does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

Condition 2: This symptom observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCef50104.

A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef50104. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf** *vrf-name* command is configured, enter the **ip vrf forwarding** *vrf-name* command on at least one interface that has PIM enabled.

Wide-Area Networking

- CSCej14572

  Symptoms: PPP connections are incorrectly terminated.

  Conditions: This symptom is observed on a Cisco router when you enter the **no aaa new-model** command.

  Workaround: To prevent the symptom from occurring, ensure that the **aaa new-model** command is configured together with network authorization, that is, ensure that the **aaa authorization network** command is configured.

- CSCsc66592

  Symptoms: When a user session is not subject to renegotiation, an LNS sends PPP keepalives with a magic number that is different from the one negotiated between the client and the LAC, preventing the client from answering the keepalive requests of the LNS.

  Conditions: This symptom is observed on a Cisco router that functions as an LNS when a user session is not subject to renegotiation. The symptom does not occur when renegotiation is triggered on the LNS.

  Workaround: Disable keepalives on the virtual-template interface that is used to clone the configuration for the user sessions.

  Alternate Workaround: Configure renegotiation.

Resolved Caveats—Cisco IOS Release 12.2(27)SBA4

Cisco IOS Release 12.2(27)SBA4 is a rebuild release for Cisco IOS Release 12.2(27)SBA. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBA4 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeh69705

  Symptoms: An RSP crashes.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(27)SBA when you enter the **microcode reload** *slot-number* command a few times. Note that when you enter the **microcode reload** *slot-number* command just once, the symptom may not occur.

Workaround: There is no workaround.

- CSCeh75016

  Symptoms: A router that is configured for SNMP may crash or generate error messages such as the following ones:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access
  %ALIGN-3-TRACE: -Traceback
  ```

  Conditions: This symptom is observed on a Cisco router when interfaces are deleted from a configuration or when an OIR is performed.

  Workaround: There is no workaround.

Miscellaneous

- CSCeh40559

  Symptoms: A router stops forwarding traffic after the MLP LLQ configuration is removed from an interface.

  Conditions: This symptom is observed on a Cisco 7500 series while traffic is being sent.

  Workaround: Stop the traffic, remove MLP LLQ configuration from the interface, and restart the traffic.

- CSCeh52674

  Symptoms: When you enter the **no snmp-server host** *host-address* command, the host is not removed from the configuration, which is shown in the output of the **show running-config** command.

  Conditions: This symptom is observed on a Cisco platform that is configured for SNMP.

  Workaround: To remove the host, explicitly specify default UDP port number 162 by entering the **no snmp-server host** *host-address* **udp-port 162 public** command.

- CSCeh55676

  Symptoms: After an online insertion and removal (OIR) of a VIP, some routes are purged in CEF.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for dCEF when an OIR is performed on any slot. However, the symptom may also occur on other Cisco routers that are configured for dCEF or that have a standby RP.

  Workaround: There is no workaround.

- CSCeh69682

  Symptoms: A Cisco router that is configured as an Intelligent Service Gateway (ISG) may reload.

  Conditions: This symptom is observed when the Per-Subscriber Firewalls feature is installed for an IPv4 ISR subscriber session (via a user or service profile) and when IPv6 or IPX is enabled on the ISG.

  Workaround: Disable IPv6 and IPX on the ISG.

- CSCeh75203

  Symptoms: When a service logoff event occurs for a session, the child policy context points to an invalid an session ID. When you enter the **show subscriber session all** command after the service is logged off, the router may reload.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when a traffic classifier service is logged off.

  Workaround: Do not enter the **show subscriber session all** command when the traffic classifier service is logged off.

- CSCeh78720

  Symptoms: When policing is configured for two directions and you change the profile for policing for one direction, policing is no longer applied to a session.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when you remove the policing parameters such as CIR values from a policy map for one direction.

  Workaround: Reconfigure the desired policing parameters in the policy map.

- 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 the following command sequence is configured:

  aaa new-model

  tacacs-server host *host-ip-address*

  tacacs-server key *key*

  ip tacacs source-interface *subinterface-name*

  There must also be at least one authentication or authorization method list configured to use one more TACACS+ servers in order for the symptom to occur.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCuk90944. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Remove the **ip tacacs source-interface** *subinterface-name* command.

  Further Problem Description: Protocols other than TACACS+ that use TCP and that are implemented using the sockets library may also use an incorrect source address if configured to use a nondefault source interface or address. This situation may cause problems, depending on the configuration on 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 using 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 configuration.

- CSCeh89573

  Symptoms: Auto VC creation and provisioning does not work.

  Conditions: This symptom is observed on a Cisco 7301 when you enter the **create on-demand** command.

  Workaround: There is no workaround.

- CSCsa88871

  Symptoms: A router may crash after a switchover.

  Conditions: This symptom is observed on a Cisco router with an MPLS Forwarding Infrastructure (MFI) when line cards send statistics to the new RP before the new RP is fully initialized.

  Workaround: There is no workaround.

- CSCsa91894

  Symptoms: A Point-to-Point Termination and Aggregation (PTA) L2TP Access Concentrator (LAC) crashes.

  Conditions: This symptom is observed on a Cisco router that functions under stress as a PTA LAC when the same services are torn down and brought up every 60 seconds. The router crashes after 12 or 13 cycles in which 5000 session flap every 6 to 7 minutes when the Subscriber Service Switch (SSS) passes a stale policy context pointer to the policy manager.

  Workaround: There is no workaround.

- CSCsa98164

  Symptoms: When the **boot config** *file-system-prefix filename* **nvbypass** command is enabled, no file is created on a secondary Route Processor (RP).

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with two PREs that function in RPR+ mode but may also occur on other platforms that are configured with redundant RPs.

  Workaround: There is no workaround.

- CSCsb22718

  Symptoms: A router crashes when you clear VPDN tunnels and subscribers by entering the **clear vpdn tunnel l2tp all** command.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) with more than 7,000 subscribers.

  Workaround: There is no workaround.

- CSCsb97913

  Symptoms: The following error messages may be displayed on the active RSP of a Cisco 7500 series:

  ```
  %IPC-3-ISSU_ERROR: ISSU register peer failed with error code 0 for seat 1010000
  %ISSU-3-NOT_FIND_UNDER_ENDPOINT: Can not find peer uid by transport ERP id(0x1010000)
  control block under endpoint.
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs a crypto image of Cisco IOS Release 12.2SB.

  Workaround: There is no workaround. Note that the symptom does not cause any side effects.

Wide-Area Networking

- CSCeh60541

  Symptoms: The **l2tp hidden** command does not properly hide or unhide Layer 2 Tunneling Protocol (L2TP) attribute-value (AV) pairs.

  Conditions: This symptom is observed on a Cisco router that is configured for Virtual Private Dial-up Network (VPDN).

  Workaround: There is no workaround.

- CSCsa52807

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Resolved Caveats—Cisco IOS Release 12.2(27)SBA2

Cisco IOS Release 12.2(27)SBA2 is a rebuild release for Cisco IOS Release 12.2(27)SBA1. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBA2 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeh28173

  Symptoms: After automatic recovery from an RSP-QAERROR, an IPC failure may occur between the master RSP and the slave RSP or between the master RSP, the slave RSP, and the port adapters.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with two RSPs that function in HSA, RPR, RPR+, or SSO mode.

Workaround: Reset the slave RSP.

Miscellaneous

- CSCeh52674

  Symptoms: When you enter the **no snmp-server host** *host-address* command, the host is not removed from the configuration, which is shown in the output of the **show running-config** command.

  Conditions: This symptom is observed on a Cisco platform that is configured for SNMP.

  Workaround: To remove the host, explicitly specify default UDP port number 162 by entering the **no snmp-server host** *host-address* **udp-port 162 public** command.

- 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 the following command sequence is configured:

  ```
  aaa new-model
  tacacs-server host host-ip-address
  tacacs-server key key
  ip tacacs source-interface subinterface-name
  ```

  There must also be at least one authentication or authorization method list configured to use one or more TACACS+ servers in order for the symptom to occur.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCuk90944. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: Remove the **ip tacacs source-interface** *subinterface-name* command.

  Further Problem Description: Protocols other than TACACS+ that use TCP and that are implemented using the sockets library may also use an incorrect source address if configured to use a nondefault source interface or address. This situation may cause problems, depending on the configuration on 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 using 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 configuration.

- CSCsa88871

  Symptoms: A router may crash after a switchover.

  Conditions: This symptom is observed on a Cisco router with an MPLS Forwarding Infrastructure (MFI) when line cards send statistics to the new RP before the new RP is fully initialized.

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(27)SBA1

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(27)SBA1. All the caveats listed in this section are open in Cisco IOS Release 12.2(27)SBA1. This section describes only severity 1, severity 2, and select severity 3 caveats.

Interfaces and Bridging

- CSCeh55421

  Symptoms: A VIP4-80 in which PA-MC-8TE1+ port adapters are installed generates the following error message and crashes:

  ```
  %DMA-3-DTQ_DISPATCH_DIRTY_PAK.
  ```

  Conditions: This symptom is observed on a Cisco 7500 series when the PA-MC-8TE1+ port adapters are configured for QoS.

  Workaround: There is no workaround.

Miscellaneous

- CSCef72161

  Symptoms: A ping through a serial interface fails, and you cannot route data through the serial interface.

  Conditions: This symptom is observed only when the serial interface has ATM DXI encapsulation enabled.

  Workaround: There is no workaround.

- CSCef90619

  Symptoms: Tracebacks occur when Distributed Traffic Shaping (DTS) is configured on interfaces of an IMA, OC-3, OC-12, channelized STM-1, or multichannel T1 port adapter.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP4 and that runs Cisco IOS Release 12.2(25)S1 or a later release, or a release that is based on Cisco IOS Release 12.2(25)S1 or a later release. The symptom may not be platform-specific.

  Workaround: Detach the service policy from the affected interface.

- 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 12.2(27)SBA and that is configured for mobile IP.

  Workaround: There is no workaround.

- CSCeh00440

  Symptoms: The output of the **show ip mroute** command does not show RPF neighbor information.

  Conditions: This symptom is observed on a first-hop router that runs Cisco IOS Release 12.2(20)S7, Release 12.2(25)S3, or a release that is based on Release 12.2S.

Workaround: There is no workaround.

Wide-Area Networking

- CSCef71011

  Symptoms: Pings fail when translational bridging and ATM DXI encapsulation are configured.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, Release 12.2S, or a release that is based on Release 12.2S.

  Workaround: Do not configure ATM DXI encapsulation. Rather, configure HDLC, PPP, or Frame Relay encapsulation.

Open Caveats—Cisco IOS Release 12.2(27)SBA

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(27)SBA. All the caveats listed in this section are open in Cisco IOS Release 12.2(27)SBA. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCef72161

  Symptoms: A ping through a serial interface fails, and you cannot route data through the serial interface.

  Conditions: This symptom is observed only when the serial interface has ATM DXI encapsulation enabled.

  Workaround: There is no workaround.

- CSCef90619

  Symptoms: Tracebacks occur when Distributed Traffic Shaping (DTS) is configured on interfaces of an IMA, OC-3, OC-12, channelized STM-1, or multichannel T1 port adapter.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP4 and that runs Cisco IOS Release 12.2(25)S1 or a later release, or a release that is based on Cisco IOS Release 12.2(25)S1 or a later release. The symptom may not be platform-specific.

  Workaround: Detach the service policy from the affected interface.

- 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 12.2(27)SBA and that is configured for mobile IP.

  Workaround: There is no workaround.

- CSCeh00440

  Symptoms: The output of the **show ip mroute** command does not show RPF neighbor information.

  Conditions: This symptom is observed on a first-hop router that runs Cisco IOS Release 12.2(20)S7, Release 12.2(25)S3, or a release that is based on Release 12.2S.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCef71011

  Symptoms: Pings fail when translational bridging and ATM DXI encapsulation are configured.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, Release 12.2S, or a release that is based on Release 12.2S.

  Workaround: Do not configure ATM DXI encapsulation. Rather, configure HDLC, PPP, or Frame Relay encapsulation.

Resolved Caveats—Cisco IOS Release 12.2(27)SBA

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(27)SBA. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCee45312

  Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

  Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

  Only the systems that are running certain versions of Cisco IOS are affected.

  Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

  Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

  Refer to the Security Advisory at the following URL for more details

  http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page*:

  http://www.cisco.com/warp/public/108/index.shtml

- *Troubleshooting Bus Error Exceptions*:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml
- *Why Does My Router Lose Its Configuration During Reboot?*:

  http://www.cisco.com/warp/public/63/lose_config_6201.html
- *Troubleshooting Router Hangs*:

  http://www.cisco.com/warp/public/63/why_hang.html
- *Troubleshooting Memory Problems*:

  http://www.cisco.com/warp/public/63/mallocfail.shtml
- *Troubleshooting High CPU Utilization on Cisco Routers*:

  http://www.cisco.com/warp/public/63/highcpu.html
- *Troubleshooting Router Crashes*:

  http://www.cisco.com/warp/public/122/crashes_router_troubleshooting.shtml
- *Using CAR During DOS Attacks*:

  http://www.cisco.com/warp/public/63/car_rate_limit_icmp.html

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2SB. 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

This section provides information about release-specific documents.

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 & Solutions: **Products: Routers and Routing Systems**: **7200 Series Routers**
  - Cisco 7200 series technical documentation on Cisco.com at

    Products & Solutions: **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 & Solutions: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 7300 Series Routers**
  - Cisco 7300 series technical documentation on Cisco.com at

    Products & Solutions: 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 7500 Series Routers
  - Cisco 7500 series home page on Cisco.com at

    Products & Solutions: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 7500 Series Routers**
  - Cisco 7500 series technical documentation on Cisco.com at

    Products & Solutions: Routers & Routing Systems: **All Routers & Routing Systems**: **Cisco 7500 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7500 Series Routers**
  - For Cisco 7500 series technical documentation on http://www.cisco.com/univercd/home/index.htm, select a Cisco 7500 series router from the **Routers** pull-down menu on the top left of the page.
- Cisco 10000 Series Routers
  - Cisco 10000 series home page on Cisco.com at

    Products & Solutions: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 10000 Series Routers**
  - Cisco 10000 series technical documentation on Cisco.com at

    Products & Solutions: **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(27)SBA

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/index.htm

- Release 12.2(27)SBB

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sbb27/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.

Note Cisco IOS Release 12.2(27)SBA, Release 12.2(27)SBB, and the rebuilds of these releases are not supported in Cisco Feature Navigator. Later releases of Release 12.2SB will be supported in Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or 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.

To access Cisco Feature Navigator, 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://www.cisco.com/register

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

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 7 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 7 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 7 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 7 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**.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

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

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

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

Original SSLeay License:

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

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

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

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

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

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

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

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

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

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

Obtaining Documentation, 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 161.