Cross-Platform Release Notes for Cisco IOS Release 12.2SB

August 8, 2007

Cisco IOS Release 12.2(31)SB1f

OL-10968-01 Rev. P0

These release notes support Cisco IOS Release 12.2SB up to and including Cisco IOS Release 12.2(31)SB1f. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and related documents.

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

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

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

For a list of the software caveats that apply to Cisco IOS Release 12.2SB, see the "Caveats" section on page 81, the *Caveats for Cisco IOS Release 12.2* document, and the "Caveats" section in the *Cross-Platform Release Notes for Cisco IOS Release 12.2S*. These documents are updated for every maintenance release and are located on Cisco.com.

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

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, page 2
- System Requirements, page 3
- New and Changed Information, page 15
- MIBs, page 76
- Limitations and Restrictions, page 77
- Important Notes, page 78
- Caveats, page 81
- Troubleshooting, page 152
- Related Documentation, page 153
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 160

Introduction

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

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

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

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

Many of the features and the hardware that are supported in this software have been previously released to customers on other software releases.

For information on new features and Cisco IOS commands that are supported by Release 12.2SB, see the "New and Changed Information" section on page 15 and the "Caveats" section on page 81.

Early Deployment Releases

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

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

Cisco IOS ED Release	Type of ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(31)SB1f	Rebuild	No new software features.	No new hardware features.	08/08/2007
12.2(31)SB1e[1]	Rebuild	No new software features.	No new hardware features.	04/20/2007

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

Cisco IOS ED Release	Type of ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(31)SB1d	Rebuild	No new software features.	No new hardware features.	03/28/2007
12.2(31)SB1c	Rebuild	No new software features.	No new hardware features.	02/12/2007
12.2(31)SB1b	Rebuild	No new software features.	No new hardware features.	01/08/2007
12.2(31)SB1a	Rebuild	No new software features.	No new hardware features.	10/30/2006
12.2(31)SB1	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(31)SB1" section on page 15.	No new hardware features.	09/25/2006
12.2(31)SB	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(31)SB" section on page 16.	See the "New Hardware Features in Cisco IOS Release 12.2(31)SB" section on page 16.	8/07/2006
12.2(28)SB4	Rebuild	No new software features.	No new hardware features.	08/31/2006
12.2(28)SB3	Rebuild	No new software features.	No new hardware features.	07/24/2006
12.2(28)SB2	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(28)SB2" section on page 22.	See the New Hardware Features in Cisco IOS Release 12.2(28)SB2, page 22.	06/15/2006
12.2(28)SB1	Rebuild	No new software features.	No new hardware features.	05/11/2006
12.2(28)SB	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(28)SB" section on page 28.	See the"New Hardware Features in Cisco IOS Release 12.2(28)SB" section on page 25.	03/20/2006

1. Cisco IOS Release 12.2(31)SB1e provides a debug option for the Sun and Sym files. No resolved caveats have been integrated in Cisco IOS Release 12.2(31)SB1e.

System Requirements

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

- Memory Recommendations, page 3
- Supported Hardware, page 4
- Determining the Software Version, page 9
- Upgrading to a New Software Release, page 9
- Feature Support, page 13

Memory Recommendations

Note Memory recommendations tables are not included in the Cisco IOS Release 12.2SB release notes to improve the usability of the release notes documentation. The memory recommendations will be available through Cisco Feature Navigator.

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

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

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

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

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

Determining Memory Recommendations for Software Images (Feature Sets)

To determine memory recommendations for software images (feature sets) in Cisco IOS Release 12.2SB, go to the Cisco Feature Navigator home page and perform the following steps.

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

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

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

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

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

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

Step 5 From the Major Release drop-down menu, choose **12.2SB**.

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

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

Supported Hardware

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

- Supported Platforms, page 5
- Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, and Cisco 7304, page 5
- Supported Line Cards for the Cisco 10000 Series Routers, page 8

Supported Platforms

Cisco IOS Release 12.2SB supports the following platforms:

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

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 15.

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

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

Table 2 Supported Platforms for Cisco IOS Release 12.2(28)SB

Cisco IOS Release	7200 Series	7301 Router	7304 Router	10000 Series
12.2(31)SB1f	No	No	No	Yes
12.2(31)SB1e	No	No	No	Yes
12.2(31)SB1c	No	No	No	Yes
12.2(31)SB1b	No	No	No	Yes
12.2(31)SB1a	No	No	No	Yes
12.2(31)SB1	No	No	No	Yes
12.2(31)SB	No	No	No	Yes
12.2(28)SB4	Yes	Yes	Yes	Yes
12.2(28)SB3	Yes	Yes	Yes	Yes
12.2(28)SB2	Yes	Yes	Yes	Yes
12.2(28)SB1	No	No	Yes	No
12.2(28)SB	Yes	Yes	Yes	Yes

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

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

- Yes—The port adapter is supported in the software image.
- No—The port adapter is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS 12.2SB release in which the port adapter was introduced. For example, (28) means that a port adapter is introduced in Cisco IOS Release 12.2(28)SB. If a cell in this column contains an em dash (—), support for the port adapter was inherited from Cisco IOS Release 12.2 or from another release and was included in the initial base release of Cisco IOS Release 12.2SB.

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

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

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

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

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

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

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

Supported Line Cards for the Cisco 10000 Series Routers

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

Table 4 Supported Line Cards for the Cisco 10000 Series Router

Common Abbreviation	Cisco Product Number[1]	Line Card Description	In
ATM Line Cards			
1-Port OC-12 ATM	ESR-1OC-12-ATM[2]	1-port OC-12 ATM	—
4-Port OC-3 ATM	ESR-4OC3-ATM-SM	4-port OC-3/STM-1 ATM, single mode	—
4-Port OC-3 ATM LR	ESR-4OC3-ATM-SM-LR	4-port OC-3/STM-1 ATM, long reach	(28)
8-Port E3/DS3 ATM	ESR-8E3/DS3-ATM	8-port E3/DS3 ATM	—
Channelized Line Cards			
1-Port Channelized OC-12/STM-4	ESR-1COC-12/STM-4-SMI[3]	1-port channelized OC-12/STM-4 (STS-12), single mode, intermediate reach	—
	ESR-1COC-12/STM-4-SML	1-port channelized OC-12/STM-4 (STS-12), single mode, long reach	—
4-Port Channelized STM-1/OC-3	ESR-4OC3-ChSTM-1/OC-3	4-port channelized OC-3/STM-1 SDH, single mode	—
4-Port Channelized T3 Half-Height	ESR-HH-4CT3	4-port channelized T3 half-height	(28)
6-Port Channelized T3	ESR-6CT3	6-port channelized T3	—
24-Port T1/E1	ESR-24CT1/E1	24-port channelized E1/T1	—
Electrical Interface Line Card			
8-Port Unchannelized E3/T3	ESR-8E3/DS3	8-port clear channel E3/DS3 line card	—
Ethernet Line Cards			
1-Port GE	ESR-1GE	1-port Gigabit Ethernet	—
1-Port GE Half-Height	ESR-HH-1GE	1-port Gigabit Ethernet half-height	—
8-Port FE Half-Height	ESR-HH-8FE-TX	8-port Fast Ethernet half-height	—
Half-Height Carrier	ESR-HH-CARRIER	Full-length base carrier for half-height line card	—
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. If a product number is listed as a spare product in the table, that is, with an equal sign (=), it means that the product is only available as a spare product. For End-of-Sale (EOS) and End-of-Life (EOL) information about line cards, refer to the Cisco product bulletins at the following location: http://www.cisco.com/en/US/products/hw/routers/ps133/prod_eol_notices_list.html
2. The old part number for this line card is ESR-1OC12ATM-SM.
3. The old part number for this line card is ESR-1COC12-SMI.

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

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

Determining the Software Version

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

```
Router#> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (rsp-jsv-mz), Version 12.2(28)SB, EARLY DEPLOYMENT RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

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

For information about upgrading the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 router and Cisco 10000 series routers, see the document at the following location:

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

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

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

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

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

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

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

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

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

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

Microcode Software

This section describes microcode software that is supported for the Cisco 7304 in Cisco IOS Release 12.2S and consists of the following subsections:

- Bundled FPGAs for the Cisco 7304, page 10
- Shared Port Adapter FPD Image Packages for the Cisco 7304, page 11

Bundled FPGAs for the Cisco 7304

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

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

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

Bundled FPGAs for Cisco IOS Release 12.2(28)SB4

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

Bundled FPGAs for Cisco IOS Release 12.2(28)SB3

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

Bundled FPGAs for Cisco IOS Release 12.2(28)SB2

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

Bundled FPGAs for Cisco IOS Release 12.2(28)SB1

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

Bundled FPGAs for Cisco IOS Release 12.2(28)SB

All Cisco IOS Release 12.2(28)SB software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 5.

Table 5 Bundled FPGA Versions for Cisco IOS Release 12.2(28)SB Sorted by Hardware Type

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

Shared Port Adapter FPD Image Packages for the Cisco 7304

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 6 Release 12.2(28)SB FPD Image Package Contents

Supported SPAs	FPD ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
7304-4FE-SPA	1	Data & I/O FPGA	4.18	0.0
7304-2GE-SPA	1	Data & I/O FPGA	4.18	0.0
SPA-2XOC3-POS	1	I/O FPGA	3.4	0.0
SPA-4XOC3-POS	1	I/O FPGA	3.4	0.0
SPA-1OC12-POS	1	I/O FPGA	3.4	0.0

Table 6 Release 12.2(28)SB FPD Image Package Contents (continued)

Supported SPAs	FPD ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
SPA-2XT3/E3	1	ROMMON	2.12	0.0
	2	I/O FPGA	0.24	0.0
	3	E3 FPGA	0.6	0.0
	4	T3 FPGA	0.14	0.0
SPA-4XT3/E3	1	ROMMON	2.12	0.0
	2	I/O FPGA	0.24	0.0
	3	E3 FPGA	0.6	0.0
	4	T3 FPGA	0.14	0.0

Feature Support

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

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Note Feature set tables are not included in the Cisco IOS Release 12.2SB release notes to improve the usability of the release notes documentation. The feature-to-image mapping will be available through Cisco Feature Navigator.

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 5 From the Major Release drop-down menu, choose **12.2SB**.

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

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

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

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

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

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

Step 3 Click **Continue**.

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

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

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

New and Changed Information

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

- New Hardware Features in Cisco IOS Release 12.2(31)SB1, page 15
- New Software Features in Cisco IOS Release 12.2(31)SB1, page 15
- New Hardware Features in Cisco IOS Release 12.2(31)SB, page 16
- New Software Features in Cisco IOS Release 12.2(31)SB, page 16
- New Hardware Features in Cisco IOS Release 12.2(28)SB2, page 22
- New Software Features in Cisco IOS Release 12.2(28)SB2, page 22
- New Hardware Features in Cisco IOS Release 12.2(28)SB, page 25
- New Software Features in Cisco IOS Release 12.2(28)SB, page 28

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

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

New Hardware Features in Cisco IOS Release 12.2(31)SB1

There are no new hardware features for Cisco IOS Release 12.2(31)SB1.

New Software Features in Cisco IOS Release 12.2(31)SB1

This section describes new and changed features in Cisco IOS Release 12.2(31)SB1. Some features may be new to Cisco IOS Release 12.2SB but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.2(31)SB1. 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.

SSO - Multilink Frame Relay

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb/122sb31/fssso20s.htm

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

This section describes new and changed features in Cisco IOS Release 12.2(31)SB. Some features may be new to Cisco IOS Release 12.2SB but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.2(31)SB. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

Performance Routing Engine 3 (PRE-3)

Platform: Cisco 10000 series

For detailed information about this product, see the data sheet:

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

Note Unless specified otherwise, the PRE-3 supports all features that are supported on the PRE-2 in Cisco IOS Release 12.2(28)SB and Release 12.2(28)SB2.

For information about how to install the PRE-3, see the *Cisco 10008 Router Performance Routing Engine 3 Installation* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb/122sb31/10rpre3.pdf

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

This section describes new and changed features in Cisco IOS Release 12.2(31)SB. Some features may be new to Cisco IOS Release 12.2SB but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.2(31)SB. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

Table 7 shows features that have never before been released in any public Cisco IOS software image for the Cisco 10000 series and that released for the first time for the Cisco 10000 series in Cisco IOS Release 12.2(31)SB. Other features may be new for the Cisco 10000 series in Cisco IOS Release 12.2(31)SB, but have been released before in other public Cisco IOS software images for the Cisco 10000 series, and are therefore not included in Table 8.

Table 7 New Features for the Cisco 10000 Series in Cisco IOS Release 12.2(31)SB

Feature Name
802.1p COS Bit Set for PPP & PPPoE Control Frames
BGP Support for Next-Hop Address Tracking
CBQOSMIB Index Persistency
Child Service Policy Allowed Under Priority Class
Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)
Control Plane Policing (CPP)
Extranet Support for Multicast VPN
Frame Relay - Multilink (MLFR-FRF.16)
IP SLAs - LSP Health Monitor with LSP Discovery
Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces
MPLS PE-to-PE Traffic Statistics for NetFlow
MQC - Distribution of Remaining Bandwidth via Ratio
MQC - Multi-Level Priority Queues
MQC - Traffic Shaping Overhead Accounting for ATM
NAS-Port ID Format C Enhancement
NetFlow Export of BGP Nexthop Information
OSPF RFC 3623 Graceful Restart
Policing Support for GRE Tunnels
PPP-Max-Payload and IWF PPPoE Tag Support
PPPoE Agent Remote ID & DSL Line Characteristics Enhancement
PPPoE Session Limiting on Inner QinQ VLAN
QoS: Classification, Policing, and Marking on LAC
QoS: Hierarchical Queuing for Ethernet DSLAMs
Three-Level Scheduler Using MQC Hierarchical Queueing Framework
VLAN Tag Based QoS

Note Unless specified otherwise, the PRE-3 supports all features that are supported on the PRE-2 in Cisco IOS Release 12.2(28)SB and Release 12.2(28)SB2.

802.1p COS Bit Set for PPP & PPPoE Control Frames

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb/122sb31/sb8021p.htm

BGP Support for Next-Hop Address Tracking

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

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

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

CBQOSMIB Index Persistency

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

For detailed information about this feature, see the *QoS: CBQoS MIB Index Enhancements* document:

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

Child Service Policy Allowed Under Priority Class

Platform: Cisco 10000 series (PRE-3)

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

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

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

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

For detailed information about this feature, see "Chapter 2, Classifying Traffic" and "Chapter 7, Marking Traffic" in the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

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

Control Plane Policing (CPP)

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

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

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

Extranet Support for Multicast VPN

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

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

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

Frame Relay - Multilink (MLFR-FRF.16)

Platform: Cisco 10000 series (PRE-3)

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

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

IP SLAs - LSP Health Monitor with LSP Discovery

Platform: Cisco 10000 series (PRE-2)

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

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

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

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

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

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

MPLS PE-to-PE Traffic Statistics for NetFlow

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

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

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

MQC - Distribution of Remaining Bandwidth via Ratio

Platform: Cisco 10000 series (PRE-3)

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

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

MQC - Multi-Level Priority Queues

Platform: Cisco 10000 series (PRE-3)

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

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

MQC - Traffic Shaping Overhead Accounting for ATM

Platform: Cisco 10000 series (PRE-3)

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

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

NAS-Port ID Format C Enhancement

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

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

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

NetFlow Export of BGP Nexthop Information

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

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

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

OSPF RFC 3623 Graceful Restart

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

For detailed information about this feature, which is also referred to as the NSF - OSPF RFC 3623 Graceful Restart feature, see the following Cisco document:

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

Policing Support for GRE Tunnels

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

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

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

PPP-Max-Payload and IWF PPPoE Tag Support

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

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

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

PPPoE Agent Remote ID & DSL Line Characteristics Enhancement

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

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

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

PPPoE Session Limiting on Inner QinQ VLAN

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

For detailed information about this feature, see the *802.1p COS Bit Set for PPP and PPPoE Control Frames* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb/122sb31/sb8021p.htm

QoS: Classification, Policing, and Marking on LAC

Platform: Cisco 10000 series (PRE-3)

For detailed information about this feature, see "Chapter 2, Classifying Traffic," "Chapter 6, Policing Traffic," and "Chapter 7, Marking Traffic" in the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

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

QoS: Hierarchical Queuing for Ethernet DSLAMs

Platform: Cisco 10000 series (PRE-3)

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

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

Three-Level Scheduler Using MQC Hierarchical Queueing Framework

Platform: Cisco 10000 series (PRE-3)

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

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

VLAN Tag Based QoS

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

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

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

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

This section describes new and changed features in Cisco IOS Release 12.2(28)SB2. Some features may be new to Cisco IOS Release 12.2SB but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.2(28)SB2. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

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

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

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

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

This section describes new and changed features in Cisco IOS Release 12.2(28)SB2. Some features may be new to Cisco IOS Release 12.2SB but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.2(28)SB2. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

Table 8 shows features that have never before been released in any public Cisco IOS software image for the Cisco 10000 series and that released for the first time for the Cisco 10000 series in Cisco IOS Release 12.2(28)SB2. Other features may be new for the Cisco 10000 series in Cisco IOS Release 12.2(28)SB2, but have been released before in other public Cisco IOS software images for the Cisco 10000 series, and are therefore not included in Table 8.

Table 8 New Features for the Cisco 10000 Series in Cisco IOS Release 12.2(28)SB2

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

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

Platform: Cisco 10000 series

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

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

IEEE 802.1Q-in-Q VLAN Tag Termination

Platform: Cisco 10000 series

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

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

Lawful Intercept

Platform: Cisco 10000 series

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

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

MPLS Traffic Engineering Features

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

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

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

Platform: Cisco 10000 series

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

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

MPLS Traffic Engineering (TE)

Platform: Cisco 10000 series

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

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

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

Platform: Cisco 10000 series

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

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

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

Platform: Cisco 10000 series

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

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

MPLS Traffic Engineering (TE)—Forwarding Adjacency

Platform: Cisco 10000 series

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

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

MPLS Traffic Engineering (TE)—Interarea Tunnels

Platform: Cisco 10000 series

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

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

MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

Platform: Cisco 10000 series

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

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

MPLS Traffic Engineering (TE) MIB

Platform: Cisco 10000 series

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

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

MPLS Traffic Engineering—Overload Avoidance Support for IS-IS

Platform: Cisco 10000 series

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

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

MPLS Traffic Engineering (TE)—Scalability Enhancements

Platform: Cisco 10000 series

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

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

MPLS Traffic Engineering (TE)—SNMP Notification Support

Platform: Cisco 10000 series

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

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

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

Platform: Cisco 10000 series

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

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

NetFlow PXF Timers

Platform: Cisco 10000 series

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

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

RSVP Refresh Reduction and Reliable Messaging

Platform: Cisco 10000 series

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

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

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

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

This section describes new and changed features in Cisco IOS Release 12.2(28)SB. Some features may be new to Cisco IOS Release 12.2SB but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.2(28)SB. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If

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

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

Platforms: Cisco 7200 series, Cisco 7301

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

The following PA-A6 port adapters are supported:

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

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

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

4-Port Half-Height Channelized T3 Line Card

Platform: Cisco 10000 series

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

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

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

Platform: Cisco 10000 series

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

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

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

Platform: Cisco 7304

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

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

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

CWDM GBIC Support for the Network Services Engine 100

Platform: Cisco 7304

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

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

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

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

CWDM SFP Support for the Network Processing Engine 100

Platform: Cisco 7304

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

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

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

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

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

Platform: Cisco 7304

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

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

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

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

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

This section describes new and changed features in Cisco IOS Release 12.2(28)SB. Some features may be new to Cisco IOS Release 12.2SB but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.2(28)SB. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

Table 9 shows features that have never before been released in any public Cisco IOS software image for the Cisco 10000 series and that released for the first time for the Cisco 10000 series in Cisco IOS Release 12.2(28)SB. Other features may be new for the Cisco 10000 series in Cisco IOS Release 12.2(28)SB, but have been released before in other public Cisco IOS software images for the Cisco 10000 series, and are therefore not included in Table 9.

Table 9 New Features for the Cisco 10000 Series in Cisco IOS Release 12.2(28)SB

Feature Name
AAA CLI Stop Record Enhancement
Any Transport over MPLS (AToM): Frame Relay over MPLS (FRoMPLS)
ATM Conditional Debug Support
Dual Rate Three Color Policer
Hierarchical Input Policing
IGMPv3
Intelligent Service Gateway (ISG) Features
IP Multicast Load Splitting Across Equal-Cost Paths
IP SLAs - LSP Health Monitor
IPv6 Features
L2TP Congestion Avoidance
Layer 2 Local Switching

Table 9 New Features for the Cisco 10000 Series in Cisco IOS Release 12.2(28)SB (continued)

Feature Name
Link Fragmentation Interleave over Frame Relay (FRF.12)
Logging to Local Non-Volatile Storage (ATA Disk)
MLPPP with Link Fragmentation Interleave (LFI)
MPLS Carrier Supporting Carrier Features: • MPLS VPN—Carrier Supporting Carrier • MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution
MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV
MPLS HA Features: • NSF/SSO: MPLS LDP and LDP Graceful Restart • NSF/SSO: MPLS VPN • MPLS High Availability and • Cisco Express Forwarding: Command Changes • MPLS High Availability: Command Changes
MPLS LDP MD5 Global Configuration
MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session
Multicast-VPN: Multicast Support for MPLS VPN
Pseudowire Emulation Edge-to-Edge MIBs for Ethernet Services
RADIUS Server Load Balancing
Stateful Switchover (SSO) for Multilink PPP (MLP)
Template ACL/12-Bit ACE

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

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

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

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

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

Feature	Support on the NSE-100	Support on the NPE-G100	Support in the PFX Path
Turbo Access Control List Scalability Enhancements	Yes	Not applicable[1]	No[2]
Warm Reload	Yes	Yes	Not applicable[3]

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

AAA Features

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

AAA CLI Stop Record Enhancement

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

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

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

AAA Double Authentication Secured by Absolute Timeout

Platforms: Cisco 7200 series, Cisco 7301

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

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

AAA Per-User Scalability

Platforms: Cisco 7200 series, Cisco 7301

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

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

AAA-PPP-VPDN Non-Blocking

Platforms: Cisco 7200 series, Cisco 7301

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

ACL Default Direction

Platform: Cisco 10000 series

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

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

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

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

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

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

ATM Features

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

ATM Bulk VC Configuration

Platform: Cisco 10000 series

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

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

ATM Conditional Debug Support

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

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

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

ATM Multilink PPP Support on Multiple VCs

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

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

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

ATM OAM Ping

Platforms: Cisco 7200 series, Cisco 7301

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

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

ATM OAM Traffic Reduction

Platforms: Cisco 7200 series, Cisco 7301

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

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

ATM PVCs

Platform: Cisco 10000 series

The ATM line cards support the full range of virtual path identifier (VPI)/virtual channel identifier (VCI) pairs (unidirection only)—8-bit VPI range and 16 bit VCI range. Table 11 lists the maximum number of active virtual channels (VCs) supported on ATM line cards for Cisco IOS Release 12.2(28)SB.

Table 11 Active VCs on ATM Line Cards

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

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

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

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

ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping

Platform: Cisco 10000 series

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

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

ATM VC into VP Shaping

Platform: Cisco 10000 series

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

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

Attribute Screening for Access Requests

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

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

Platforms: Cisco 7200 series, Cisco 7301

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

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

BGP Features

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

BGP 4 MIB Support for per-Peer Received Routes

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

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

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

BGP Convergence Optimization

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Bit Error Rate Testing (BERT)

Platform: Cisco 10000 series

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

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

Bridged 1483 Encapsulated Traffic over ATM SVCs

Platforms: Cisco 7200 series, Cisco 7301

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

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

Byte-Based Weighted Random Early Detection

Platforms: Cisco 7200 series, Cisco 7301

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

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

CEF/dCEF - Cisco Express Forwarding

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

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

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

Clear IPC Statistics

Platform: Cisco 10000 series

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

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

Configurable MAC Address for PPPoE

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

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

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

Crashinfo Support

Platform: Cisco 10000 series

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

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

Define Interface Policy-Map AV Pairs AAA

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

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

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

DHCP Features

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

DHCP Accounting

Platform: Cisco 10000 series

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

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

DHCP Address Allocation Using Option 82

Platforms: Cisco 7200 series, Cisco 7301

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

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

DHCP Client Dynamic Subnet Allocation API

Platform: Cisco 7200 series

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

DHCP—Configurable DHCP Client

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

DHCP Lease Limit per ATM RBE Unnumbered Interface

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

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

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

DHCP ODAP Server Support

Platform: Cisco 10000 series

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

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

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

Platform: Cisco 10000 series

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

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

DHCP Option 82 Support for Routed Bridge Encapsulation

Platforms: Cisco 7200 series, Cisco 7301

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

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

DHCP Relay MPLS VPN Support

Platform: Cisco 10000 series

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

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

DHCP Relay Subscriber Identifier Suboption

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

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

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

DHCP Release and Renew CLI in EXEC Mode

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

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

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

DHCP Server—On-Demand Address Pool Manager

Platform: Cisco 10000 series

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

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

DHCP Server—Option to Ignore All BOOTP Requests

Platforms: Cisco 7200 series, Cisco 7301

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

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

DHCP—Static Mapping

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

DHCP—Statically Configured Routes Using a DHCP Gateway

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

DHCPv6 Prefix Delegation via AAA

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

For detailed information about this feature, see the "Prefix Delegation" section in the "Implementing ADSL and Deploying Dial Access for IPv6" chapter that is part of the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_dial6.htm

DHCPv6 Relay Agent

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

A client locates a DHCP server by using a reserved, link-scoped multicast address. Therefore, it is a requirement for direct communication between the client and the server that the client and the server be attached to the same link. However, in some situations in which ease of management, economy, or scalability is a concern, it is desirable to allow a DHCP client to send a message to a DHCP server that is not connected to the same link. A DHCP relay agent, which may reside on the client's link, is used to relay messages between the client and the server. DHCP relay agent operation is transparent to the client.

For more information, see the *Implementing Basic Connectivity for IPv6* chapter that is part of the *Cisco IOS IPv6 Configuration Library*:

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

Distributed Time-Based Access Lists

Platform: Cisco 10000 series

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

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

Dialer CEF

Platforms: Cisco 7200 series, Cisco 7301

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

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

DNS Spoofing

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

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

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

Dynamic ATM VP and VC Configuration Modification

Platform: Cisco 10000 series

The Dynamic ATM VP and VC Configuration Modification feature enables you to change the virtual circuit (VC) weight or virtual path (VP) shaping parameters without affecting the state of the VC or VP. In other words, the VC and VP remain up and operational (the VC or VP is not torn down at the segmentation and reassembly [SAR], and the session does not go down). The dynamic parameters

include ATM VP parameters (peak cell rate [PCR] or cell delay variation tolerance [CDVT]) and VC parameters (weight, PCR, sustainable cell rate [SCR], maximum burst size [MBS], and CDVT). When you change the VC parameters or the VP rate, there can be a momentary change in the shaped rate of the VP, in which the rate at which cells are sent may be over or under the configured rate. The session stays up, and no data is lost.

The range of integer values that are supported by the *weighting-value* argument of the **weight** command is 5 to 255.

Dynamic DNS Support for Cisco IOS Software

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123ya8/gt_ddns.htm

Dynamic Subscriber Bandwidth Selection

Platform: Cisco 10000 series

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

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

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

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gtmvesoo.htm

Embedded Event Manager 2.1

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gteem21.htm

Enabling OSPFv2 on an Interface Using the ip ospf area Command

Platform: Cisco 10000 series

For detailed information about this feature, which is also known as the Area Command in Interface Mode for OSPFv2 feature, see the following Cisco document:

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

Enhanced Tracking Support

Platform: Cisco 10000 series

For detailed information about this feature, including Enhanced Object Tracking, see the following Cisco document:

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

Entity/Environment Monitoring

Platforms: Cisco 7200 series, Cisco 7301

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

- For the Cisco 7200 series, see the *Cisco 7200 Series Router MIB Specifications Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps341/products_technical_reference_book09186a00805fee4b.html

- For the Cisco 7301, see the *Cisco 7301 Router MIB Specifications Guide*:

  http://www.cisco.com/en/US/products/hw/routers/ps352/products_technical_reference_book09186a00805fee95.html

Extended NAS-Port-Type and NAS-Port Support

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

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

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

Frame Relay Features

Cisco IOS Release 12.2(28)SB introduced support for the following Frame Relay features.

Frame Relay Fast Restart

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st19/19stfr72.htm

Frame Relay MIB Enhancements

Platforms: Cisco 7200 series, Cisco 7301

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

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

Frame Relay—show and debug Command Enhancements

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

For detailed information about this feature, which is also known as the Frame Relay show Command and debug Command Enhancements feature, see the following Cisco document:

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

Frame Relay VC Bundling

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Frame Relay PVC Bundles with IP and MPLS QoS Support* document:

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

Generic Routing Encapsulation (GRE) Tunnel Keepalive

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

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

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

Globalized Channelizations for SONET/SDH

Platform: Cisco 10000 series

The Globalized Channelizations for SONET/SDH feature enables the Cisco 10000 series 1-port channelized OC-12 line card and 4-port channelized STM-1 line card to support the following globalized channelization modes:

- SONET channelization:
  - STS-1 over DS3/T3
  - STS-1 over DS3/T3 over DS1
  - STS-1 over DS3/T3 over DS3 subrate
  - STS-1 over VT1.5 over DS1
  - STS-1 over VT2 over E1
- Synchronous Digital Hierarchy (SDH) channelization:
  - STM-1 over AU-3 over DS3/T3
  - STM-1 over AU-3 over DS3/T3 over DS3 subrate
  - STM-1 over AU-3 over TUG-2 over C-11 over DS1/T1
  - STM-1 over AU-3 over TUG-2 over C-12 over E1
  - STM-1 over AU-4 over TUG-3 over TUG-2 over C-11 over DS1/T1
  - STM-1 over AU-4 over TUG-3 over TUG-2 over C-12 over E1

IEEE 802.1p Support

Platform: Cisco 10000 series

The IEEE's 802.1p standard now allows a range of traffic prioritization of Layer 2 frames from critical to non-critical through a frame priority tag, providing a higher quality of service (QoS) on high-speed LANs. Network managers can implement traffic prioritization through infrastructure device upgrades. IEEE 802.1p is a key enabler to QoS by enabling "Prioritized Ethernet" with up to eight priorities in Ethernet and Token Ring networks.

IGMP State Limit

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

The IGMP State Limit feature provides protection against denial of service attacks caused by IGMP packets. The new CLI introduced by this feature allows you to configure a limit on the number of IGMP states that results from IGMP, IGMP Version 3 lite, and URL Rendezvous Directory (URD) membership reports on a per-interface or global basis. Membership reports in excess of the configured limits will not be entered in the IGMP cache, and traffic for those excess membership reports will not be forwarded.

For more information, see the *Customizing IGMP* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/chap10/mcbcigmp.htm

IGMPv3

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

For detailed information about this feature, see the *Customizing IGMP* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/chap10/mcbcigmp.htm

Improved show commands for MLP-ATM LFI

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

For detailed information about this feature, see the *Troubleshooting Enhancements for Multilink PPP over ATM Link Fragmentation and Interleaving* document:

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

Intelligent Service Gateway (ISG) Features

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

Cisco IOS Release 12.2(28)SB introduces support for the following Intelligent Service Gateway (ISG) features on the Cisco 7200 series, Cisco 7301, and Cisco 10000 series as explained in Table 12.

Table 12 ISG Features Supported per Platform

ISG Feature	Cisco 7301 Router	Cisco 7200 Series	Cisco 10000 Series
ISG: Authentication: DHCP Option 82 Line ID - AAA Authorization Support	Yes	Yes	No
ISG: Accounting: Postpaid	Yes	Yes	No
ISG: Accounting: Time-Based Prepaid	Yes	Yes	Yes
ISG: Accounting: Volume-Based Prepaid	Yes	Yes	No
ISG: Accounting: Per Session, Service & Flow	Yes	Yes	Yes
ISG: Accounting: Tariff Switching	Yes	Yes	No
ISG: Flow Control: Flow Redirect (L4, Captive Portal)	Yes	Yes	Yes
ISG: Flow Control: QoS Control: Dynamic Rate Limiting	Yes	Yes	Yes
ISG: Instrumentation: Advanced Conditional Debugging	Yes	Yes	Yes
ISG: Instrumentation: Session & Flow Monitoring (local and external)	Yes	Yes	No
ISG: Network Interface: IP Routed, VRF Aware MPLS	Yes	Yes	No
ISG: Network Interface: Tunneled (L2TP)	Yes	Yes	Yes
ISG: Policy Control: DHCP Proxy	Yes	Yes	No
ISG: Policy Control: Multidimensional Identity per Session	Yes	Yes	Yes
ISG: Policy Control: Policy: Domain Based (Auto-domain)	Yes	Yes	Yes
ISG: Policy Control: Policy Server: CoA (QoS, L4 Redirect, User ACL, TimeOut)	Yes	Yes	Yes
ISG: Policy Control: Policy Server: SSG-SESM Protocol	Yes	Yes	Yes
ISG: Policy Control: Policy: Triggers: Duration	Yes	Yes	No
ISG: Policy Control: Service Profiles	Yes	Yes	Yes
ISG: Policy Control: User Profiles	Yes	Yes	Yes
ISG: Session: Auth: PBHK	Yes	Yes	Yes
ISG: Session: Auth: Single Sign On	Yes	Yes	Yes
ISG: Session: Authentication (MAC, IP, EAP)	Yes	Yes	No
ISG: Session: Creation: Interface IP Session: L2	Yes	Yes	No
ISG: Session: Creation: Interface IP Session: L3	Yes	Yes	No
ISG: Session: Creation: IP Session: Protocol Event (DHCP)	Yes	Yes	No
ISG: Session: Creation: IP Session: Subnet & Source IP: L2	Yes	Yes	No
ISG: Session: Creation: IP Session: Subnet & Source IP: L3	Yes	Yes	No

Table 12 ISG Features Supported per Platform

ISG Feature	Cisco 7301 Router	Cisco 7200 Series	Cisco 10000 Series
ISG: Session: LifeCycle: Idle Timeout	Yes	Yes	Yes
ISG: Session: LifeCycle: POD	Yes	Yes	Yes
ISG: Session: Multi-Service Creation and Flow Control	Yes	Yes	Yes
ISG: Session: VRF Transfer	Yes	Yes	No

For detailed information about these features, see the *Cisco IOS Intelligent Service Gateway Configuration Guide* that is part of the *Cisco IOS ISG Configuration Library*:

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

Interface Alias Long Name Support

Platform: Cisco 10000 series

For detailed information about this feature, see the following *Interface Index Display and Interface Alias Long Name Support for SNMP* document:

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

IP Features

Cisco IOS Release 12.2(28)SB introduced support the following IP features.

IPMROUTE-STD-MIB

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

The IPMROUTE-STD-MIB, as defined in RFC 2932, is a module for IP multicast routing in a manner independent of the specific multicast routing protocol in use. Support for this MIB replaces the draft form of the IPMROUTE-MIB.

The IPMROUTE-STD-MIB supports all the MIB objects of the IPMROUTE-MIB and also supports the following four new MIB objects:

- ipMRouteEntryCount
- ipMRouteHCOctets
- ipMRouteInterfaceHCInMcastOctets
- ipMRouteInterfaceHCOutMcastOctets

The ipMRouteScopeNameTable MIB object is not supported because it is not relevant to multicast routers.

IP Multicast Load Splitting Across Equal-Cost Paths

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

For detailed information about this feature, see the *Load Splitting IP Multicast* document:

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

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

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

IP SLAs - LSP Health Monitor

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

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

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

IPv6 Access Services: DHCPv6 Prefix Delegation

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

DHCP for IPv6 can be used in environments to deliver stateless address assignment information. Stateless address assignment uses configuration parameters that do not require a server to maintain a dynamic state for individual clients, such as DNS server addresses and domain search list options.

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

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

IPv6 Features for the Cisco 10000 Series

Platform: Cisco 10000 series

Cisco IOS Release 12.0(28)SB supports the IPv6 Hardware: PXF Accelerated for IPv6 Forwarding feature for the Cisco 10000 series, which includes support for the following IPv6 features:

- IPv6 features:
  - IPv6 address types: Unicast
  - IPv6: ICMPv6
    (Note: A ping in the fast-path mode is not supported; the support rate is limited to 10 pings per second per interface.)
  - IPv6: IPv6 neighbor discovery
  - IPv6: IPv6 stateless autoconfiguration
  - IPv6: IPv6 MTU path discovery
  - IPv6: ICMPv6 redirect
  - IPv6: neighbor discovery duplicate address detection
  - IPv6: IPv6 static cache entry for neighbor discovery
  - IPv6 address types: Anycast
- IPv6 Switching Services features:
  - IPv6 switching: CEF/dCEF support
  - IPv6 switching: CEFv6 switched configured IPv6 over IPv4 tunnels
- IPv6 Routing features:
  - IPv6 routing: RIP for IPv6 (RIPng)
  - IPv6 routing: static routing

  - IPv6 routing: route redistribution
  - IPv6 routing: multiprotocol BGP extensions for IPv6
  - IPv6 routing: multiprotocol BGP link-local address peering
  - IPv6 routing: IS-IS support for IPv6
  - IPv6 routing: IS-IS multitopology support for IPv6
  - IPv6 routing: OSPF for IPv6 (OSPFv3)
- IPv6 Services and Management features:
  - IPv6 services: AAAA DNS lookups over an IPv4 transport
  - IPv6 services: standard access control lists
  - IPv6 services: DNS lookups over an IPv6 transport
  - IPv6 services: Secure Shell support over IPv6
  - IPv6 services: Cisco Discovery Protocol—IPv6 address family support for neighbor information
  - IPv6 services: CISCO-IP-MIB support
  - IPv6 services: CISCO-IP-FORWARDING-MIB support
  - IPv6 services: extended access control lists3
- IPv6 Tunnel Services features:
  - IPv6 tunneling: manually configured IPv6 over IPv4 tunnels
  - IPv6 tunneling: IPv6 over IPv4 GRE tunnels
- IPv6 Data Link Layer features:
  - IPv6 data link: ATM PVC and ATM LANE
  - IPv6 data link: Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet
  - IPv6 data link: Frame Relay PVC
  - IPv6 data link: Cisco High-Level Data Link Control
  - IPv6 data link: PPP service over packet over SONET, ISDN, and serial (synchronous and asynchronous) interfaces
    (Note: PPPoA, PPPoE, and PPP over a VLAN are not supported; PPP over a serial link is supported.)
  - IPv6 data link: VLANs using IEEE 802.1Q encapsulation

For more information about these IPv6 features, see the “Start Here: Cisco IOS Software Release Specifics for IPv6 Features” chapter of the *Cisco IOS IPv6 Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/ftipv6s.htm

ISDN Backup in MPLS Core

Platforms: Cisco 7200 series, Cisco 7301

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

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

In Service Software Upgrade (ISSU)

Platform: Cisco 10000 series

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

- ISSU - ARP
- ISSU - ATM
- ISSU - Frame Relay
- ISSU - HDLC
- ISSU - HSRP
- ISSU - PPP/MLP
- ISSU - QoS
- ISSU - SNMP

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

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

The ISSU feature includes support for the following MPLS features:

- ISSU - MPLS LDP
- ISSU - MPLS QoS
- ISSU - MPLS L3VPN

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

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

The ISSU feature is supported on the following line cards:

- 1-port channelized OC-12/STM-4
- 1-port Gigabit Ethernet
- 1-port half-height Gigabit Ethernet
- 1-port OC-12 ATM
- 1-port OC-12 Packet over SONET (PoS)
- l-port OC-48 PoS
- 4-port channelized OC-3/STM-1
- 4-port channelized half-height T3
- 4-port OC-3 ATM
- 6-port channelized T3
- 6-port OC-3 PoS
- 8-port ATM E3/DS3
- 8-port E3/DS3
- 8-port half-height Fast Ethernet
- 24-port channelized E1/T1

L2TP and L2TPv3 Features

Cisco IOS Release 12.2(28)SB introduces support for the following L2TP and L2TPv3 features.

L2TP Congestion Avoidance

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2scca.htm

L2TP Disconnect Cause Information

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtl2disc.htm

L2TP Extended Failover

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2tpef.htm

L2TP Redirect

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2tpmr.htm

L2TP Security

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2tsec.htm

L2TP Tunnel Connection Speed Labeling

Platforms: Cisco 7200 series, Cisco 7301

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

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

L2TPv3 Control Message Hashing

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

L2TPv3 Control Message Rate Limiting

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

Protocol Demultiplexing for L2TPv3

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

Layer 2 Local Switching

Platform: Cisco 10000 series

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

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

Layer 2 Local Switching: Frame Relay to Frame Relay

Platform: Cisco 10000 series

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

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

Layer 2 VPN Features

Cisco IOS Release 12.2(28)SB introduces support for the following Layer 2 VPN features.

L2VPN Pseudowire Redundancy

Platform: Cisco 7403

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

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

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

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

NSF/SSO: L2VPN Pseudowire Redundancy Support

Platforms: Cisco 7200 series, Cisco 7301

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

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

Local AAA Server

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

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

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

Local Template-Based ATM PVC Provisioning

Platform: Cisco 10000 series

The Local Template-Based ATM PVC Provisioning feature supports permanent virtual circuit (PVC) autoprovisioning for an infinite range of virtual path identifier (VPI)/virtual channel identifier (VCI) combinations on an ATM interface. This feature enables ATM PVCs to be provisioned automatically as needed from a local configuration, which makes the provisioning of large numbers of digital subscriber line (DSL) subscribers easier, faster, and less prone to error. ATM PVC autoprovisioning can be configured on a PVC, an ATM PVC range, or a virtual circuit (VC) class. If a VC class that is configured with ATM PVC autoprovisioning is assigned to the main interface, all the PVCs on that main interface will be autoprovisioned; this configuration is sometimes called an infinite range.

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

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

Logging to Local Non-Volatile Storage (ATA Disk)

Platform: Cisco 10000 series

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

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

MLP LFI over ATM Configuration Scaling

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, which is also known as the Link Fragmentation and Interleaving for Frame Relay and ATM Virtual Circuits feature, see the following Cisco document:

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

MPLS Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) and MPLS-related features.

MPLS (Multiprotocol Label Switching)

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

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

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

MPLS-Aware NetFlow

Platforms: Cisco 7200 series, Cisco 7301

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

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

MPLS Egress NetFlow Accounting

Platform: Cisco 10000 series

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

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

MPLS Embedded Management—High Capacity Counter

Platforms: Cisco 7200 series, Cisco 7301

As of Cisco IOS Release 12.2(28)SB, the MPLS IF MIB has a 64-bit structure to ensure that high-capacity loads can be handled.

MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/lsping28.htm

MPLS Label Distribution MIB: MPLS LDP Trap Enhancement

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsvnmb25.htm#wp1027129

MPLS Label Distribution Protocol (LDP)

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftldp13.htm

MPLS—LDP AutoConfiguration

Platform: Cisco 10000 series

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

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

MPLS—LDP MD5 Global Configuration

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sb_md5.htm

MPLS—LDP Session Protection

Platform: Cisco 10000 series

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

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

MPLS—Multilink PPP Support

Platforms: Cisco 7200 series, Cisco 7301

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

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

MPLS QoS—DiffServ Tunnel Mode Support

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

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

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

MPLS HA Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) High Availability (HA) features for the Cisco 10000 series.

Note In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series supports Route Processor Redundancy Plus (RPR+) and Stateful Switchover (SSO). However for broadband aggregation features, the Cisco 10000 series supports RPR+ only.

NSF/SSO: MPLS LDP and LDP Graceful Restart

Platform: Cisco 10000 series

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

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

NSF/SSO: MPLS VPN

Platform: Cisco 10000 series

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

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

MPLS High Availability

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

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

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

Command Changes in Relation to MPLS HA

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

For command changes in relation to Multiprotocol Label Switching (MPLS) high availability (HA), see the following documents:

- Cisco Express Forwarding: Command Changes

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

- MPLS High Availability: Command Changes

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

MPLS Traffic Engineering Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) features:

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

Platforms: 7200 series, Cisco 7301, Cisco 7304

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

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

MPLS Traffic Engineering (TE)

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

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

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

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

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

MPLS Traffic Engineering (TE)—Forwarding Adjacency

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

MPLS Traffic Engineering (TE)—Interarea Tunnels

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

MPLS Traffic Engineering (TE) MIB

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

MPLS Traffic Engineering (TE)—Scalability Enhancements

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

MPLS Traffic Engineering (TE)—SNMP Notification Support

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

MPLS VPN Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) features.

MPLS VPN—Carrier Supporting Carrier

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbb2scsc.htm

MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbbcsc13.htm

MPLS VPN—eiBGP Multipath Loadbalancing Enhancements

Platform: Cisco 7304, Cisco 10000 series

In this Cisco IOS release, the MPLS-VPN eiBGP Multipath Loadbalancing feature has been enhanced to support up to 96,000 VPN routes in a scenario in which there are four BGP paths and one IGP path to each BGP peer. In previous Cisco IOS releases, up to 48,000 VPN routes were supported.

It is important to note that the maximum number of load-balanced paths used per route decreases from 16 to 8 as a result of this feature. The number of load-balanced paths per route is determined using a round-robin algorithm, but the round-robin algorithm now can only use up to 8 paths instead of 16, like it could previously.

This is a functional enhancement that introduces no new configuration.

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

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

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

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

MPLS VPN—Half Duplex VRF (HDVRF) Support with Static Routing

Platform: Cisco 10000 series

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

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

MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

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

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

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

MPLS VPN—Inter-Autonomous System Support

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

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

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

MPLS VPN—MIB Support: MPLS VPN Trap Enhancement

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsvnmb25.htm#wp1027129

MPLS VPN—Show Running VRF

Platform: Cisco 10000 series

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

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

MPLS VPN—VPN-Aware LDP MIB

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *MPLS Label Distribution Protocol MIB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ldpmib13.htm#wp1015327

MPLS VPN—VRF-Select for PXF

Platform: Cisco 7304

VRF-Select is supported in the PXF processing path for a Cisco 7304.

For information about MPLS VPN VRF-Select, see the *MPLS VPN: VRF Selection Based on Source IP Address* document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a0080173d55.html

For additional information about this feature and all other features in the PXF-processing path, including restrictions, see the *Cisco 7304 Troubleshooting and Configuration Notes* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm#wp65935

Multicast-VPN: Multicast Support for MPLS VPN

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

For detailed information about this feature (which is also known as the Multicast VPN—IP Multicast Support for MPLS VPNs feature), see the following Cisco document:

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

MQC Policy Map Support on Configured VC Range

Platforms: Cisco 7200 series, Cisco 7301

The MQC Policy Map Support on Configured VC Range feature extends policy map functionality to simplify the configuration of ranges of ATM VCs. Using the **service-policy** command, this feature allows you to apply a QoS service policy to a range of VCs.

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/28sbvrng.htm

Multilink Frame Relay (FRF.16.1) Variable Bandwidth Class Support

Platforms: Cisco 7200 series, Cisco 7301

For detailed information about this feature, see the *Multilink Frame Relay (FRF.16.1)* document:

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

Multiple Action Policer for PXF

Platform: Cisco 7304

The Multiple Action Policer feature further extends the functionality of the Cisco IOS Traffic Policing feature (a single-rate policer feature). The Traffic Policing feature is a traffic policing mechanism that allows you to control the maximum rate of traffic sent or received on an interface. Both of these traffic policing mechanisms mark packets as conforming to, exceeding, or violating a specified rate. After a packet is marked, you can specify an action to be taken on the packet based on that marking.

With the Traffic Policing feature, you can specify only one conform action, one exceed action, and one violate action. Now with the Multiple Action Policer feature, you can specify multiple conform, exceed, and violate actions for the marked packets.

The Multiple Action Policer feature is introduced in the PXF processing path for the first time. For additional information about this feature and all other features in the PXF-processing path, including restrictions, see the *Cisco 7304 Troubleshooting and Configuration Notes* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm#wp65935

Multirouter Automatic Protection Switching (APS)

Platform: Cisco 10000 series

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

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

NetFlow MPLS Label Export

Platforms: Cisco 7200 series, Cisco 7301

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

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

Nonstop Forwarding and Stateful Switchover Features

Nonstop Forwarding

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

Cisco IOS Release 12.2(28)SB supports the following Nonstop Forwarding (NSF) features:

- Integrated IS-IS Nonstop Forwarding Awareness
- Nonstop Forwarding (NSF) Awareness
- Nonstop Forwarding (NSF) for BGP
- Nonstop Forwarding (NSF) for IS-IS
- Nonstop Forwarding with Stateful Switchover (NSF/SSO)

For detailed information about these features, see the *Cisco Nonstop Forwarding* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fsnsf20s.htm

Stateful Switchover

Platforms: Cisco 7304, Cisco 10000 series

Cisco IOS Release 12.2(28)SB supports the following Stateful Switchover (SSO) features:

- APS Stateful Switchover (APS SSO)

Note APS SSO is supported only on the Cisco 10000 series.

- Stateful Switchover (SSO) for ATM
- Stateful Switchover (SSO) for Frame Relay
- Stateful Switchover (SSO) for HDLC

- Stateful Switchover (SSO) for Multilink PPP (MLP)
- Stateful Switchover (SSO) for PPP

For detailed information about these features with the exception of the SSO - Multilink PPP (MLP) feature, see the *Stateful Switchover* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fssso20s.htm

For detailed information about the SSO - Multilink PPP (MLP) feature, see the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

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

Offload Server Accounting Enhancement

Platforms: Cisco 7200 series, Cisco 7301

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

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

OSPF ABR Type 3 LSA Filtering

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftabrt3f.htm

Packet Classification Using the Frame Relay DLCI Number

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/ftdlc26i.htm

peer pool backup Command

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpeerpl.htm

Per-Packet Load Balancing (PPLB)

Platform: Cisco 10000 series

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

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

Per-User QoS via AAA Policy Name

Platform: Cisco 10000 series

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

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

Per VRF AAA

Platform: Cisco 10000 series

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

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

PIM Multicast Scalability

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

The PIM Multicast Scalability feature enhances the Protocol Independent Multicast (PIM) protocol in Cisco IOS software by adding a new level of scalability. With this feature, edge devices can have a large number of multicast groups and users without increasing the CPU utilization of the router.

Policer Enhancement: Multiple Actions

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsmu26s.htm

Post-Switchover Core Dump

Platform: Cisco 10000 series

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

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

PPP MLP MRRU Negotiation Configuration

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

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

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

PPPoE Features

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

PPPoA/PPPoE Autosense for ATM PVCs

Platform: Cisco 10000 series

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

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

PPPoE Circuit-ID Tag Processing

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

PPPoE over Gigabit Ethernet Interface

Platform: Cisco 7200 series, Cisco 7301, Cisco 10000 series

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

PPPoE Relay

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpppoer.htm

PPPoE Service Selection

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpoess.htm

PPPoE Session Limit

Platform: Cisco 10000 series

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

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

PPPoE Session Limit per NAS Port

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/12b_nas.htm

PPPoE Session Recovery After Reload

Platforms: Cisco 7200 series, Cisco 7301 Cisco 10000 series

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

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

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet Services

Platform: Cisco 10000 series

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

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

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

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS Features for the Cisco 7200 Series and Cisco 7301

Cisco IOS Release 12.2(28)SB supports the following QoS features for the Cisco 7200 series and Cisco 7301.

QoS: ATM Cell-Based Policer

Platforms: Cisco 7200 series, Cisco 7301

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

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

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

Platforms: Cisco 7200 series, Cisco 7301

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

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

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

Platforms: Cisco 7200 series, Cisco 7301

Several MIB objects have been added to existing tables, and a new table has been added to the Class-Based Quality of Service (QoS) MIB (CBQoSMIB). These additions to the CBQoSMIB provide parity of the MIB across three specific Cisco IOS Releases—Cisco IOS Release 12.0S, 12.2SB, and 12.3T. As a result of these additions and revisions, the CBQoSMIB now supports the same features across all three of these platforms.

The CBQoSMIB now supports the following Cisco IOS features:

- QoS: ATM Cell-Based Policer

  The QoS: ATM Cell-Based Policer feature allows you to configure traffic policing for ATM cells. This feature allows you to specify traffic policing in cells, bytes, or percentage of bandwidth.

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

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

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

  The QoS: ATM-CLP and Layer 2 CoS-Based WRED feature extends the functionality of the Cisco Weighted Random Early Detection (WRED) software. With the QoS: ATM-CLP and Layer 2 CoS-Based WRED feature, WRED can take into account the Layer 2 class of service (CoS) value of a packet and the ATM cell loss priority (CLP) of a packet when calculating the drop probability of network traffic.

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

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

- QoS: Color-Aware Policer

  The QoS: Color-Aware Policer feature enables a “color-aware” method of traffic policing. This feature allows you to police traffic according to the color classification of a packet that is based on packet-matching criteria defined for two user-specified traffic classes: the conform-color class and the exceed-color class. These two traffic classes are created using the **conform-color** command, and the metering rates are defined using the **police** command.

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/12s_cap.htm

- Low Latency Queuing with Priority Percentage Support

  This feature allows you to configure bandwidth as a percentage within low latency queuing (LLQ).

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

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

- QoS: Percentage-Based Policing

  The QoS: Percentage-Based Policing feature allows you to configure traffic policing on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed burst (bc) size and the excess burst (be) size (used for configuring traffic policing) in milliseconds (ms). Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

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

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

- QoS: Percentage-Based Shaping

  The QoS: Percentage-Based Shaping feature allows you to configure traffic policing and traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed (conform) burst (bc) size and the excess (peak) burst (be) size (used for configuring traffic shaping) in milliseconds (ms). Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

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

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

- QoS: Time-Based Thresholds for WRED and Queue Limit

  The QoS: Time-Based Thresholds for WRED and Queue Limit feature allows you to specify the Weighted Random Early Detection (WRED) minimum and maximum thresholds or the queue limit threshold in milliseconds (ms). Previously, these thresholds could only be specified in packets or bytes. Now, all three units of measure are available. Once the threshold limits are configured in a policy map, the policy map can be used on multiple interfaces, including those with different amounts of bandwidth.

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

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

The following additional changes were made to the MIB tables:

- One new table was added (cbQosSetStats), and objects were added to an existing table (chQosSetCFG). These tables are associated with the various **set** commands available in the Cisco IOS software.

  For more information about the Cisco IOS **set** commands, see the Cisco command reference publications for the Cisco IOS release that you are using.

For a list of the specific MIB objects added, see the CISCO-CLASS-BASED-QOS-MIB-CAPABILITY.html file at the following URL:

http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&mibName=CISCO-CLASS-BASED-QOS-MIB-CAPABILITY

For more information about the preceding CBQoSMIB and the MIB objects and tables, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

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

QoS: Color-Aware Policer

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/12s_cap.htm

QoS: Frame Relay QoS Hierarchical Queueing Framework Support

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS: Match on ATM CLP

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS: Percentage-Based Policing

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS: Percentage-Based Shaping

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS: Percentage-Based and Time-Based Policing Parameters

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS: Per-Session Shaping and Queuing on LNS

Platforms: Cisco 7200 series, Cisco 7301

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

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

QoS Features for the Cisco 10000 Series

Cisco IOS Release 12.2(28)SB supports the following quality of service (QoS) features for the Cisco 10000 series:

- Dual Rate Three Color Policer
- Enhanced Random Early Detection (RED) Statistics
- Hierarchical Input Policing
- MLPPP with Link Fragmentation Interleave (LFI)
- Link Fragmentation Interleave over Frame Relay (FRF.12)
- Policy Map Scaling
- Random Early Detection (RED) with Queue-Limit

- Three Color Policer
- Three-Level Policy Maps
- VC Oversubscription

In addition to the Cisco 10000 series, the following features are also supported on the Cisco 7200 series, Cisco 7301, and Cisco 7304:

- Class-Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)
- Class-Based Marking
- Class-Based Policing
- Class-Based Shaping
- Class-Based Weighted Fair Queuing (CBWFQ)
- Diffserv Compliant WRED
- Low Latency Queueing (LLQ)
- Low Latency Queueing (LLQ) for Frame Relay
- Modular QoS CLI (MQC)
- Priority Queueing (PQ)
- QoS for Virtual Private Networks
- QoS Packet Marking
- QoS Policy Propagation via Border Gateway Protocol (QPPB)
- Random Early Detection (RED)
- Weighted RED (WRED)

For information about all features that are mentioned in this section, see the *Cisco 10000 Series Router Quality of Service Configuration Guide*:

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

In addition, Cisco IOS Release 12.2(28)SB supports the following QoS features for the Cisco 10000 series.

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

Platform: Cisco 10000 series

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

QoS: Broadband Aggregation Enhancements, Phase 1

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbbbrs1a.htm

QoS: Enhanced Show Commands for Active Policies

Platform: Cisco 10000 series

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

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

RADIUS Features

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

Framed-Route in RADIUS Accounting

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_fra22.htm

RADIUS NAS-IP-Address Configurability

Platforms: Cisco 7200 series, Cisco 7301

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

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

RADIUS Push for MOD CLI Policies

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

For detailed information about this feature, see the *Define Interface Policy-Map AV Pairs AAA* document:

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

RADIUS Server Load Balancing

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7403, Cisco 10000 series

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

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

RADIUS Server Reorder on Failure

Platforms: Cisco 7200 series, Cisco 7301

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/gt_rsrof.htm

radius-server source-port Command

Platform: Cisco 10000 series

The **radius-server source-ports extended** command enabled you to configure the NAS to use 200 ports in the range from 21645 to 21844 as the source ports for sending out RADIUS requests. With 200 source ports, up to 256*200 authentication and accounting requests can be outstanding at one time. During peak call volume, typically when a router first boots or when an interface flaps, the extra source ports allow sessions to recover more quickly on large-scale aggregation platforms.

To return to the default setting, in which ports 1645 and 1646 are used as the source ports for RADIUS requests, use the **no** form of this command.

For more information, see the *Cisco IOS Security Command Reference, Release 12.3* document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a008017cf42.html

RADIUS Timeout Set During Pre-Authentication

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftattr27.htm

RADIUS Tunnel Preference for Load Balancing and Fail-Over

Platform: Cisco 10000 series

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

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

RADIUS Attributes

Cisco IOS Release 12.2(28)SB introduces support for the following RADIUS attributes.

Connect-Info RADIUS Attribute 77

Platform: Cisco 10000 series

The Connect-Info RADIUS Attribute 77 feature introduces support for RADIUS attribute 77 (Connect-Info), which provides information about connection speeds, modulation, and compression for modem dial-in connections via RADIUS accounting “start” and “stop” records.

When the NAS sends attribute 77 in accounting “start” and “stop” records, you can measure—across the platform—the connect rates. That is, attribute 77 allows you to record “transmit” speed (the speed at which the NAS modem sends information) and “receive” speed (the speed at which the NAS receives information). These modem speeds for user sessions allow you to determine whether user modem connections renegotiate to lower speeds shortly into a session. If the transmit and receive speeds are different from each other, attribute 77 will report both speeds, which allows you to establish the modem connection speeds that customers gets from their session.

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

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/ra5f.htm

RADIUS Attribute 52 and 53 Gigaword Support

Platform: Cisco 10000 series

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

RADIUS Attribute 77 for DSL

Platform: Cisco 10000 series

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

RADIUS Attribute 82: Tunnel Assignment ID

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbrad_82.htm

RADIUS Attribute 91 Encrypted and Tagged VSA Support

Platform: Cisco 10000 series

For detailed information about this feature, see the *Encrypted and Tagged VSA Support for RADIUS Attribute 91* section in the following Cisco document:

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

RADIUS Attribute Screening

Platform: Cisco 10000 series

For detailed information about this feature, which is also known as the RADIUS Attribute Value Screening feature, see the following Cisco document:

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

Reserve Memory for Console Access

Platform: Cisco 10000 series

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

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

Route Processor Redundancy Plus (RPR+)

Platforms: Cisco 7304, Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fssso20s.htm

RSVP Refresh Reduction and Reliable Messaging

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

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

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

Secure Shell Version 2 Support

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

For detailed information about this feature, including the Secure Shell SSH Version 2 Client Support feature, also known as the SSHv2 feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_ssh2.htm

show Command Redirect

Platform: Cisco 10000 series

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

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

Sticky IP

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

For detailed information about this feature, which is also known as the RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/radattr8.htm

Subscriber Service Switch

Platforms: Cisco 7200 series, Cisco 7301

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

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

TCP MSS Adjustment

Platforms: Cisco 7200 series, Cisco 7301

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

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

Template ACL/12-Bit ACE

Platform: Cisco 10000 series

For detailed information about this feature, see "Chapter 19, Configuring Template ACLs" in the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

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

Three-level Hierarchical Policy Support in PXF

Platform: Cisco 7304

The Modular QoS CLI (MQC) enables users to configure hierarchical policy maps, in which a grandparent policy uses a parent policy, and a parent policy uses a child policy. Support for all three levels of hierarchy was previously not available on the Cisco 7304 router, which used to support two levels of hierarchy. This feature is available in the PXF-processing path.

This feature is the addition of a third level of hierarchy within the MQC. It does not introduce any new commands. For information on configuring the MQC, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt8/qcfmcli2.htm

For additional information about this feature and all other features in the PXF-processing path, including restrictions, see the *Cisco 7304 Troubleshooting and Configuration Notes* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm#wp65935

Turbo Access Control List Scalability Enhancements

Platform: Cisco 7304

In previous Cisco IOS releases, the ability of Turbo Access Control Lists to control PXF traffic could be limited. When the Turbo ACL classification tables grew large because of substantially-sized configurations and certain traffic patterns, all traffic that required ACL classification was punted to the Route Processor because the Turbo ACL table sizes exceeded the amount of available PXF memory.

This feature improves Turbo ACL scalability and enables support for large ACL tables.

This is a functional enhancement that introduces no new configuration.

UDI - Unique Device Identifier

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpepudi.htm

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

Platform: Cisco 10000 series

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

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

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

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft31addr.htm

VBR - NRT Oversubscription

Platform: Cisco 10000 series

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

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

Virtual Sub-Interface

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

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

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

Virtual Template Interfaces Limit Expansion

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

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

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

VLAN ID Rewrite

Platforms: Cisco 7200 series, Cisco 7301

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

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

VLANs over IP Unnumbered Subinterfaces

Platform: Cisco 10000 series

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtunvlan.htm

VPDN Features

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

Accounting of VPDN Disconnect Cause

Platforms: Cisco 7200 series, Cisco 7301

In the past, when a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) session failed or disconnected, the network access server (NAS) and Home GateWay (HGW) reported a very generic disconnect-cause code, such as "LOST CARRIER." These generic codes did not provide enough detailed information for accounting and debugging purposes. The Accounting of VPDN Disconnect Cause feature adds eight new disconnect-cause codes that describe the status of Virtual Private Dialup Network (VPDN) failures and disconnects more specifically than existing generic disconnect-cause codes. These new disconnect-cause codes can be found in the "RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values" appendix of the *Cisco IOS Security Configuration Guide, Release 12.2*:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00801fd174.html

RFC-2867 Tunnel Accounting

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

For detailed information about this feature, see the *RFC-2867 RADIUS Tunnel Accounting* document:

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

Shell-Based Authentication of VPDN Users

Platforms: Cisco 7200 series, Cisco 7301

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

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

Timer and Retry Enhancements for L2TP and L2F

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

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

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

Tunnel Authentication via Radius on LNS

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

For detailed information about this feature, see the *Tunnel Authentication via RADIUS on Tunnel Terminator* document:

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

VPDN Default Group Template

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

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

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

VPDN Group Session Limiting

Platforms: Cisco 7200 series, Cisco 7301

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

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

VPDN Multihop by DNIS

Platforms: Cisco 7200 series, Cisco 7301

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

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

VPN MIB Enhancements for per-VRF Session Counting

Platforms: Cisco 7200 series, Cisco 7301

An extension has been added to the virtual private dialup network (VPDN) CISCO-VPDN-MGMT-MIB that returns the total number of active sessions for each VPDN template. For customers that associate a VPDN template to each VPN routing and forwarding (VRF) instance, this MIB extension provides a way to monitor session usage per VRF.

Service providers can terminate sessions from multiple customer accounts on the same L2TP network server (LNS). Sharing of the LNS is done by creating one VRF per customer. Session limits on VPDN templates and VPDN groups are configured to control the allocation of sessions among customers and among users within the same customer account. A VPDN template is associated with each VRF, and its session limit restricts the total number of sessions for a customer account. Within that account, users may be assigned to different VPDN groups as their access requirements dictate. Session limits on VPDN groups further control the allocation of customer sessions among VPDN users. In such a setup, the service provider must use Simple Network Management Protocol (SNMP) to retrieve the total number of active sessions per customer to monitor their usage on the LNS.

Prior to the introduction of this MIB enhancement, only the total number of sessions on the LNS across all customer accounts could be retrieved through SNMP. This enhancement extends the CISCO-VPDN-MGMT-MIB to include a read-only table of VPDN template entries, with each entry reporting the number of active sessions across all VPDN groups that are associated with that template. The table entries can be accessed individually by using GET requests or consecutively using repeated GET-NEXT requests.

VPDN Session Disconnect AAA Attribute

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

The VPDN Session Disconnect AAA Attribute feature adds support for a new vendor-specific attribute (VSA) to be included in accounting stop records. The VSA provides information about the reason for the session disconnect and the identity of the device that initiated the disconnection. This feature introduces support for the **accounting** keyword of the vpdn-logging command in Cisco IOS Release 12.2(28)SB, and is enabled by entering the **vpdn-logging accounting** command and keyword.

VRF-Aware VPDN Tunnels

Platforms: Cisco 7200 series, Cisco 7301

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

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

VPN Routing/Forwarding (VRF) CLI Command

Platform: Cisco 10000 series

The Virtual Private Network (VPN) routing/forwarding (VRF) command enables you to enter comments about your VRF configuration.

description *description string*

no description

The following output is from a configuration example:

```
Router(config)# ip vrf V4
Router(config-vrf)# ?
IP VPN Routing/Forwarding instance configuration commands:
  default       Set a command to its defaults
  description   VRF specific description
  exit          Exit from VRF configuration mode
  export        VRF export
  import        VRF import
  maximum       Set a limit
  no            Negate a command or set its defaults
  rd            Specify Route Distinguisher
  route-target  Specify Target VPN Extended Communities
Router(config-vrf)# desc
Router(config-vrf)# description ?
  LINE  Up to 80 characters describing this VRF
Router(config-vrf)# description This Is My 4th VRF
Router(config-vrf)# end
```

```
Router# sh ru | beg V4
ip vrf V4
 description This Is My 4th VRF
 rd 1:406
 route-target export 1:400
 route-target import 1:400
```

Warm Reload

Platforms: Cisco 7200 series, Cisco 7301, Cisco 7304

The Warm Reload feature enables you to reload your routers without reading images from storage. That is, the Cisco IOS image reboots without ROM monitor mode (ROMMON) intervention by restoring the read-write data from a previously saved copy in the RAM and by starting execution without either copying the image from flash to RAM or self-decompressing the image. Thus, the overall availability of your system improves because the time to reboot your router is significantly reduced.

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

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

XML Interface to Syslog Messages

Platform: Cisco 10000 series

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

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

MIBs

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

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

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

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

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

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

Limitations and Restrictions

The following sections contain information about limitations and restrictions in Cisco IOS Release 12.2SB that can apply to the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 router, and Cisco 10000 series routers.

Limitations and Restrictions in Cisco IOS Release 12.2(28)SB

This section describes limitations and restrictions in Cisco IOS Release 12.2(28)SB and later releases.

High Availability Support for the Cisco 10000 Series

In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series supports Route Processor Redundancy Plus (RPR+), Stateful Switchover (SSO), and In Service Software Upgrade (ISSU). However for broadband aggregation features, the Cisco 10000 series supports RPR+ only.

ISSU Restriction for the Cisco 10000 Series

The In Service Software Upgrade (ISSU) feature for the Cisco 10000 series is not supported for MPLS VPN—Inter-Autonomous System (Inter-AS) configurations.

Per Precedence WRED Statistics

In the output of the **show policy-map interface** command, the Tail Drops counter indicates the number of packets dropped because the average queue length exceeded the maximum threshold for the given precedence. However, under burst conditions, it is possible that packets can be dropped because the queue is full. These packets are not counted as Tail Drops. The number of packets that are dropped under burst conditions when the queue is full are counted as Output Queue Drops.

RADIUS Attribute 31: PPPoX Calling Station ID

In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series does not support the RADIUS Attribute 31: PPPoX Calling Station ID feature.

Scaling Limits for L2TP Tunnels on the Cisco 10000 Series

For information about scaling limits for L2TP tunnels on the Cisco 10000 series, see the "Scaling Enhancements" section in the "Scalability and Performance" chapter of the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/scaling.htm#wp1030846

SNMP Version 1 BGP4-MIB Limitations

You may notice incorrect BGP trap OID output when you use the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise

OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). The problem is not due to any error with Cisco IOS software. This problem occurs because the BGP4-MIB does not follow RFC 1908 rules regarding version 1 and version 2 trap compliance. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

System Limits for Policy Maps on the Cisco 10000 Series

The maximum number of classes supported per policy map on a Cisco 10000 series in Cisco IOS Release 12.2(28)SB is 64. The maximum number of policy maps supported per system is 4096.

tunnel vrf Command Not Supported on the Cisco 10000 Series

The Cisco 10000 series does not support the **tunnel vrf** *vrf-name* command in Cisco IOS Release 12.2(28)SB. Therefore, you cannot configure a tunnel for which both the source address and the destination address are located in a VPN routing/forwarding (VRF) instance, for example, when a tunnel is established between a customer edge (CE) router and a provider edge (PE) router. All tunnel source and destination addresses must be located in the global routing table.

The Cisco 10000 series does support a configuration in which the IP address of the tunnel itself is located in a VRF instance, for example, when the tunnel extends a VRF instance from one PE router to another PE router.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2SB that can apply to the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 router, and Cisco 10000 series routers.

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml

Field Notices and Bulletins

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

http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/1654_pp.htm

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

- Product Bulletins—If you have an account with Cisco.com, you can find product bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find product bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.

Important Notes for Cisco IOS Release 12.2(31)SB

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(31)SB and later releases.

Detection Mechanism for the MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Node Protection, with RSVP Hellos Support Feature

When the detection mechanism for the MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Node Protection, with RSVP Hellos Support feature is configured with a refresh interval and missed refresh limit that are too short, a neighbor may be declared down while the neighbor is actually up, and a warning message may be generated. To prevent this situation, configure the refresh interval and missed refresh limit in the following ways:

- Ensure that the *interval-value* argument in the **ip rsvp signalling hello refresh interval** *interval-value* command is 200 milliseconds or longer.
- Ensure that the *msg-countip* argument in the **rsvp signalling hello** [**fast-reroute**] **refresh misses** *msg-count* command has a value of 4 or more.

The detection interval for the detection mechanism should be at least 800 milliseconds (that is, 200 milliseconds of the *interval-value* argument multiplied by the value 4 of the *msg-countip* argument) or longer.

Outdated ATA ROM Monitor Library (Monlib) [CSCsg64518]

Symptoms: The following symptoms may occur:

- When you enter the **dir** command for a disk from the ROM monitor (ROMMON) prompt, it make take too long to list the files or the command may time-out and fails to list the files.
- When you boot the router from a disk by entering the **boot** command or by initiating a switchover, it make take too long to load the image or the operation may time-out and the router fails to boot.

Conditions: These symptoms are observed on a Cisco router that has an ATA file system when the ATA ROM monitor library (Monlib) on the disk for which the **dir** command is entered or on which the boot image resides is very old. However, the symptoms can also occur because of other software issues or disk related-hardware issues.

Workaround: Upgrade the Monlib of the disk.

Further Problem Description:

To check the Monlib version of the disk, enter the **show disk0: filesys** command. In the output, look for the details under "ATA MONLIB INFO," as in the following example:

```
ATA MONLIB INFO
    Image Monlib size      69912
    Disk Monlib Size       69912
    Disk Space Available   73728
    Name                   NA
    End Sector             NA
```

```
    Start sector           NA
    Updated By             NA <-- Look for this information.
    Version                NA <-- Look for this information.
```

"NA" is very old image. You should see a Cisco IOS version that created the Monlib. The Cisco IOS version can be a good indicator of how old the Monlib is, as in the following example:

```
ATA MONLIB INFO
    Image Monlib size = 67288
    Disk monlib size = 70656
    Name = c10k-atafslib-m
    Monlib Start sector = 2
    Monlib End sector = 133
    Monlib updated by = C10K2-P11-M12.2(31)SB2 <--Look for the Cisco IOS software image
    Monlib version = 1 <-- Look for the MONLIB version no.
```

You can upgrade the Monlib through two methods:

- 1st Method: Enter the **upgrade filesystem monlib disk0:** command. Monlib software resides on the disk. By entering the above-mentioned command you upgrade the Monlib to the Monlib in the Cisco IOS software image that resides on the router without deleting the other files on the disk.

  There is a reserved space for the Monlib on the disk. If this reserved space is not sufficiently large enough to hold the new Monlib, the upgrade command may fail. (Note that this reserved space is not the disk space and should not be confused with the free space on the disk).

- 2nd Method: Upgrade by entering the **format** command for the disk, in which case the other files on the disk are deleted. When you format the disk, a reserved space is created and the Monlib is upgraded to the Monlib in the Cisco IOS software image that resides on the router.

Important Notes for Cisco IOS Release 12.2(28)SB

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(28)SB and later releases.

MPLS MTU Command Change

The behavior of the **mpls mtu** command has changed in Cisco IOS Release 12.2(28)SB and later releases. You cannot set the MPLS MTU value larger than the interface MTU value. This prevents problems such as dropped packets when MPLS MTU value settings are larger than interface MTU values. Cisco IOS software allows the MPLS MTU value to be higher than the interface MTU value only for interfaces that have a default interface MTU value of 1580 or less. For more information, see the following document:

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

Tuning I/O Buffers for Nonstop Forwarding (NSF)/Stateful Switchover (SSO) Functionality

For proper Nonstop Forwarding (NSF)/Stateful Switchover (SSO) functionality in scaled configurations, we recommend that you tune the number of I/O buffers on the Cisco 10000 series. (The default I/O buffer settings are good settings for standard configurations.) When NSF/SSO functionality is enabled, tune the I/O buffers by entering the following commands:

- **buffers small permanent 2500**
- **buffers small max-free 4000**

- **buffers small min-free 1000**
- **buffers middle permanent 2500**
- **buffers middle max-free 3500**
- **buffers middle min-free 1000**
- **buffers verybig permanent 1000**
- **buffers verybig max-free 2000**
- **buffers verybig min-free 150**

For more information about buffer tuning, see the *Buffer Tuning for all Cisco Routers* document:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a00800a7b80.shtml

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

Upgrading PCI Port Adapter Carrier Card ROMmon for the Cisco 7304 Router

Beginning in Cisco IOS Release 12.2(28)SB, the PCI Port Adapter Carrier Card (7300-CC-PA) requires a one-time ROMmon upgrade to function. If this upgrade is not performed, the PCI Port Adapter Carrier Card with the incompatible ROMmon will be deactivated until the PCI Port Adapter Carrier Card ROMmon upgrade is performed.

The upgraded ROMmon image is bundled with the Cisco IOS software image; no additional images need to be downloaded to perform the upgrade. The upgrade can be performed by answering a prompt that will appear when certain processes, including the Cisco IOS bootup process, recognize that the PA-CC ROMmon requires an upgrade. Other methods of upgrading PA-CC ROMmon exist.

For additional information on this process, see the *Upgrading PCI Port Adapter Carrier Card ROMmon* document:

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

Caveats

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

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

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

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

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Support: Tools & Resources: Bug Toolkit** (which is listed under Troubleshooting). Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have

requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

This section consists of the following subsections:

- Resolved Caveats—Cisco IOS Release 12.2(31)SB1f, page 82
- Resolved Caveats—Cisco IOS Release 12.2(31)SB1e, page 87
- Resolved Caveats—Cisco IOS Release 12.2(31)SB1d, page 87
- Resolved Caveats—Cisco IOS Release 12.2(31)SB1c, page 89
- Resolved Caveats—Cisco IOS Release 12.2(31)SB1b, page 91
- Resolved Caveats—Cisco IOS Release 12.2(31)SB1a, page 99
- Open Caveats—Cisco IOS Release 12.2(31)SB1, page 101
- Resolved Caveats—Cisco IOS Release 12.2(31)SB1, page 102
- Open Caveats—Cisco IOS Release 12.2(31)SB, page 117
- Resolved Caveats—Cisco IOS Release 12.2(28)SB4, page 121
- Resolved Caveats—Cisco IOS Release 12.2(28)SB3, page 122
- Resolved Caveats—Cisco IOS Release 12.2(28)SB2, page 124
- Resolved Caveats—Cisco IOS Release 12.2(28)SB1, page 137
- Open Caveats—Cisco IOS Release 12.2(28)SB, page 140

Resolved Caveats—Cisco IOS Release 12.2(31)SB1f

Cisco IOS Release 12.2(31)SB1f is a rebuild release for Cisco IOS Release 12.2(31)SB1. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB1f but may be open in previous Cisco IOS releases.

Basic System Services

- CSCse04560

  Symptoms: A TFTP client trying to transfer a file from a Cisco IOS device configured as a TFTP server and which is denied by an ACL receives a different result depending if the file is being offered for download or not. This may allow a third party to enumerate which files are available for download.

  Conditions: The **tftp-server** command is configured on the device and an ACL restricting access to the file in question has been applied as in this example:

  tftp-server flash:*filename1 access-list-number*

  access-list *access-list-number* **permit** *192.168.1.0 0.0.0.255* **access-list** *access-list-number* **deny** *any*

Workaround: The following workarounds can be applied:

1. Interface ACL Configure and attach an access list to every router interface active and configured for IP packet processing. Example:

   access-list *access-list-number* **remark** *--- the following hosts and networks area ALLOWED for TFTP access*
   access-list *access-list-number* **permit udp host** *source_1* **host** *interface_address_1* **eq** *69*
   access-list *access-list-number* **permit udp host** *source_2* **host** *interface_address_2* **eq** *69*
   access-list *access-list-number* **permit udp** *source source-wildcard* **host** *interface_address_1* **eq** *69*
   access-list *access-list-number* **permit udp** *source source-wildcard* **host** *interface_address_2* **eq** *69*
   access-list *access-list-number* **remark** *--- everyone else is DENIED for TFTP access*
   access-list *access-list-number* **deny udp any host** *interface_address_1* **eq** *69*
   access-list *access-list-number* **deny udp any host** *interface_address_2* **eq** *69*
   access-list *access-list-number* **remark** *--- any other traffic to/through the router is allowed*
   access-list *access-list-number* **permit ip any any**

   interface Ethernet0/0 **ip access-group** *access-list-number* **in**

   Once the tftp server in Cisco IOS is enabled and listening by default on all interfaces enabled for IP processing, the access list would need to deny traffic to each and every IP address assigned to any active router interface.

2. Control Plane Policing Configure and apply a CoPP policy. For example:

   access-list *access-list-number* **remark** *--- Do not police TFTP traffic from trusted hosts and networks* **access-list**
   access-list-number **deny udp host** *source_1* **any eq** *69*
   access-list *access-list-number* **deny udp** *source source-wildcard* **any eq** *69*
   access-list *access-list-number* **remark** *--- Police TFTP traffic from untrusted hosts and networks*
   access-list *access-list-number* **permit udp any any eq** *69*
   access-list *access-list-number* **remark** *--- Do not police any other traffic going to the router*
   access-list *access-list-number* **deny ip any any**

   class-map match-all *tftp-class* **match access-group** *access-list-number*

   policy-map *control-plane-policy ! Drop all traffic that matches the class tftp-class* **class** *tftp-class* **drop**

   control-plane service-policy input *control-plane- policy*

   Note CoPP is only available on certain platforms and Cisco IOS releases. Additional information on the configuration and use of the CoPP feature can be found at the following URL:
   http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a0080211f39.shtml

3. Infrastructure ACLs (iACL)
   Although often difficult to block traffic transitting your network, identifying traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network is possible. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper entitled “Protecting Your Core:

Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for iACLs:
http://www.cisco.com/warp/public/707/iacl.html

4. Configuring Receive Access Lists (rACLs)
For distributed platforms, rACLs may be an option starting in Cisco IOS Release 12.0(21)S2 for the Cisco 12000 series GSR and Cisco IOS Release 12.0 (24)S for the Cisco 7500 series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help identify and allow legitimate traffic to your device and deny all unwanted packets:
http://www.cisco.com/warp/public/707/racl.html

Note The suggested workarounds are an "all or nothing" solution. While the tftp-server feature in Cisco IOS allows per-file ACLs to be attached to every file being offered for download, the suggested workarounds are global and will either prevent or allow access to all files being shared. It is recommended to apply the suggested workarounds in addition to the existing per-file ACLs, instead of replacing them.

- CSCsj44081

  Cisco IOS software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message when it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

```
The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp
May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
```

  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

  Recommended Action: Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORR UPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

IP Routing Protocols

- CSCin95836

  Symptoms: A Cisco IOS device that is configured for NHRP may restart.

  Conditions: This symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCsb96034

  Symptoms: Routes redistributed from other routing protocols to BGP will be deleted and re-added after an NSF switchover, potentially causing traffic to go down for a long period of time.

  Conditions: This symptom may occur when the route is redistributed from other routing protocols (such as OSPF, ISIS, EIGRP) to BGP.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb21064

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

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

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

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

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

- 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.

- CSCse56501

  Symptoms: When two sockets are bound to the same port, the first File Descriptor always receives the requests.

  Conditions: This symptom is observed on a Cisco router when two sockets such as one IPv4 socket and one IPv6 socket are connected to the same UDP port.

  Workaround: Use different UDP ports for different sockets.

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.2(31)SB1e

There are no resolved caveats in Cisco IOS Release 12.2(31)SB1e. This release provides a debug option for the Sun and Sym files.

Resolved Caveats—Cisco IOS Release 12.2(31)SB1d

Cisco IOS Release 12.2(31)SB1d is a rebuild release for Cisco IOS Release 12.2(31)SB1. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB1d but may be open in previous Cisco IOS releases.

Basic System Services

- CSCse95758

  Symptoms: Customers can use an access list to restrict TFTP configuration transfers that are initiated via SNMP by using the command **snmp-server tftp-server-list access-list**. This restriction is not possible for the FTP, RCP, and SCP protocols.

  Conditions: This symptom is observed on any Cisco IOS platform that is configured for SNMP.

  The following sample configuration causes the platform to reject configuration file transfers via SNMP from all hosts except the TFTP server that is specified in access list 5:

  ```
  snmp-server tftp-server-list 5

  access-list 5 permit 10.1.1.1
  snmp-server community private RW 5
  snmp-server tftp-server-list 5
  ```

  Workarounds:

  1. Apply a more general access list to restrict traffic to and from the affected platform.
  2. Disallow configuration copy from SNMP by excluding CISCO-CONFIG-COPY-MIB using snmp views.
  3. Disable the SNMP server.

  Fixed Software Information:

  Access-List Support for CISCO-CONFIG-COPY-MIB

  The **snmp-server file-transfer access-group** command is introduced to restrict configuration transfers that are initiated via the Simple Network Management Protocol (SNMP). Supported transfer protocols are TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP).

  This command replaces the **snmp-server tftp-server-list** command.

  For detailed information about the snmp-server file-transfer access-group command, see the *Cisco IOS Network Management Command Reference, Release 12.4*.

- CSCsg70355

  Symptoms: Starting in calendar year 2007, daylight savings summer-time rules may cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.

  Conditions: The Cisco IOS configuration command:

  clock summer-time *zone* **recurring**

uses United States standards for daylight savings time rules by default. The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March. It changes the end date from the last Sunday of October to the first Sunday of November.

Workaround: A workaround is possible by using the **clock summer- time** configuration command to manually configure the proper start date and end date for daylight savings time. After the summer-time period for calendar year 2006 is over, one can for example configure:

clock summer-time *PDT* **recurring** *2 Sun Mar 2:00 1 Sun Nov 2:00*

(This example is for the US/Pacific time zone.)

Not A Workaround: Using NTP is not a workaround to this problem. NTP does not carry any information about time zones or summer time.

Miscellaneous

- 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: Permit only known trusted hosts and/or networks to connect to the router by using a vty access list:

  1. Configure SSH version 1 from the global configuration mode, as in the following example:

     ```
     config t
     ip ssh version 1
     end
     ```

  2. Create a vty access list, as in the following example:

     ```
     10.1.1.0/24 is a trusted network that
     is permitted access to the router, all
     other access is denied
     access-list 99 permit 10.1.1.0 0.0.0.255
     access-list 99 deny any
     line vty 0 4
     access-class 99 in
     end
     ```

  Further Problem Description:

  For information about configuring vty access lists, see the *Controlling Access to a Virtual Terminal Line* document:

  http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapte r09186a0080716ec2.html

  For information about SSH, see the *Configuring Secure Shell on Routers and Switches Running Cisco IOS* document:

  http://www.cisco.com/warp/public/707/ssh.shtml

- CSCsh69391

  Symptoms: Police counters may be incorrect on Multilink Frame Relay (FRF.16.1) input interface.

Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 and that runs Cisco IOS Release 12.2(31)SB1b when packets arrive on an FRF.16.1 input interface that is configured with an input hierarchical policy map.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB1c

Cisco IOS Release 12.2(31)SB1c is a rebuild release for Cisco IOS Release 12.2(31)SB1. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB1c but may be open in previous Cisco IOS releases.

Basic System Services

- CSCek58840

  Symptoms: When a new PPP session is set up, the following warning message is generated, and the session fails:

  ```
  LAC: %IDMNGR-3-ALLOCFAIL: Warning: Failed to allocate memory for keylist in event_init
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB1. The PPP sessions start failing after the router has been up for about two weeks with many policy-map changes on the PVCs, a few cleared sessions by the clients, and one switchover.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsh28948

  Symptoms: When executing the **show running-config** command (or its command alias **more:system running-config**) or the **write memory** command (or its command aliases **copy run start** or **copy system:running-config nvram:startup-config**), the CPU usage suddenly increases dramatically (spikes).

  Conditions: This symptom has been observed on a Cisco 10000 series that terminates thousands of PTA sessions. The symptom does not occur when there are no active PTA sessions or when only LAC sessions are active.

  Workaround: There is currently no known workaround.

Miscellaneous

- CSCsg00072

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

  Symptom 1: The PXF engine may crash continuously.

  Condition 1: This symptom is observed on a Cisco 10000 series that has a PRE-2 and that is configured for LFI over ATM when IPCP is negotiated.

  Workaround 1: Disable the LFIoATM bundle interface.

  Symptom 2: Multilink PPP over ATM (MLPoA) member links may flap because of keepalive failures.

Condition 2: This symptom is observed on a Cisco 10000 series that has a PRE-2 when keepalives are enabled on the bundle interface.

Workaround 2: Disable keepalives on the bundle interface.

- CSCsh12653

  Symptoms: When an ISG receives VSAs that cannot be parsed by the SIP parser, the ISG disconnects the established session and does not respond with a CoA Nak message.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG when an incorrect VSA is sent via a CoA message and when the SIP parser returns a DENY message to the ISG.

  Following are examples of incorrect VSAs:

  - a vc-weight that is larger than the maximum that is allowed:

    cisco-avpair = “atm:vc-weight=3000”

  - a non-existent service-policy name:

    cisco-avpair = “atm:vc-qos-policy-out=non_exist_policy”

    cisco-avpair = “atm:vc-watermark-max=1”

  Workaround: There is no workaround.

- CSCsh51788

  Symptoms: An ISG that receives incorrect VSAs for a policy map may no longer accept any VSAs even if the VSAs are correct.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and that runs Cisco IOS Release 12.2(28)SB, Release 12.2(31)SB, or Release 12.2(31)SB1.

  Workaround: There is no workaround.

- CSCsh55593

  Symptoms: ACEs in an ACL that are configured to match IP packets with options may not match the specified options. This situation may cause packets without options to match an ACE that is configured to match only IP packets with options. Also, this situation may cause packets to be unexpectedly permitted or dropped, or, if the ACL is used in a QoS or PBR configuration, packets may be routed incorrectly.

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

  Workaround: Do not configure ACEs to match IP packets with options. Rather, if your intent is to drop all IP packets with options, enter the **ip option drop** global configuration command.

Resolved Caveats—Cisco IOS Release 12.2(31)SB1b

Cisco IOS Release 12.2(31)SB1b is a rebuild release for Cisco IOS Release 12.2(31)SB1. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB1b but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeg52893

  Symptoms: VTY or TTY sessions may hang after unsuccessful authentication attempts to an external AAA server. For a line that is still considered active, the output of the **show line** *line-number* command, shows the following:

  ```
  Modem state: Ready, Carrier Dropped
  ```

  When you enable the **debug tacacs** command, the following debug statement is generated during the authentication failure:

  ```
  No sock_ctx found while handling request timeout
  ```

  Conditions: This symptom is observed on a Cisco platform when external authentication fails before the maximum authentication attempts are reached locally.

  Workaround: When the symptom has occurred, reload the router to clear the hung VTY or TTY sessions. For a NAS with internal modems, you may be able to clear the hung VTY or TTY sessions by entering the **clear port** *slot*/*port* EXEC command.

  To prevent the symptom from occurring, configure the maximum authentication attempts on the Cisco platform to be lower than the maximum authentication attempts on the external AAA server by entering the **aaa authentication attempts login** *number-of-attempts* global configuration command, in which the *number-of-attempts* argument is a value that is smaller then the maximum authentication attempts that are configured on the external AAA server.

EXEC and Configuration Parser

- CSCsc76550

  Symptoms: The RP may crash with a watchdog timeout error for the IP input process.

  Conditions: This symptom is observed on a Cisco router when you delete a subinterface that processes traffic.

  Workaround: Shut down the subinterface before you delete the subinterface.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

IP Routing Protocols

- CSCek42585

  Symptoms: After a link flap has occurred, a BGP connection may not be established between a Cisco router and a third-party vendor router.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBB and that functions as a PE router. The symptom may also affect other releases.

  Workaround: Enter the **neighbor** *ip-address* **transport connection-mode active** command on the PE router.

  Further Problem Description: The symptom occurs because the Cisco router sends "Open Confirm" and "Keepalive" messages in one single TCP packet instead of two TCP packets. This situation causes some third-party vendor routers to incorrectly implement BGP and prevents BGP sessions from being established.

- CSCse49697

  Symptoms: You may not be able to disable the BGP Next-Hop Address Tracking feature.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA but may also affect other platforms and other releases. When you enter the **no bgp nexthop trigger enable** command, which should disable the BGP Next-Hop Address Tracking feature, the command does appear in the configuration but the feature remains enabled.

  Workaround: First remove the BGP configuration, then remove the BGP Next-Hop Address Tracking feature from the BGP configuration, and then re-enable the BGP configuration.

- 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.

- CSCse97513

  Symptoms: A BGP session from a Cisco router to a third-party vendor router that functions as a BGP neighbor may not come up after you have reloaded the Cisco router or after you have removed and reconfigured a BGP neighbor command.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(27)SBB4 but is both platform- and release-independent.

  Workaround: Contact Cisco TAC for a workaround that involves a hidden command.

Miscellaneous

- 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.

- CSCek54768

  Symptoms: E1 interfaces may go down when a line card is reset or removed even when the line card has APS enabled and an APS cutover is triggered. The interfaces do come back up within a few seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has a pair of 4-port channelized OC-3 line cards that are configured for SR-APS. The line cards are configured with E1 interfaces under either SONET or SDH.

  Workaround: Enter the **force** command in APS group configuration mode on both the router on which the line card is reset or removed and on the router at the far end to ensure that the line card that is reset or removed does not receive or transmit the active traffic.

  Note that the chances of the symptom occurring may be reduced when the line card that is reset or removed is not the active line card.

  Further Problem Description: This symptom occurs only when a line card is reset or removed, not when an APS switchover is triggered by a fiber cable that is removed.

  The symptom occurs because of a change in the E1 clock source that may occur when the line card is reset or removed and that causes alarms to be received. The symptom is more likely to occur when the line card has a large configuration and when the E1 interfaces are set to "clock source line."

- CSCek59190

  Symptoms: When you reload a Cisco 10000 series, tracebacks are generated when the router comes back up.

  Conditions: This symptom is observed when the router has dual PREs that function in SSO mode and a 4-port channelized STM-1/OC-3 line card that is configured for Multi-Router APS (MR-APS).

  Workaround: There is no workaround.

- 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.

- CSCsb40304

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

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

  The vulnerable cryptographic library is used in the following Cisco products:

  – Cisco IOS, documented as Cisco bug ID CSCsd85587
  – Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  – Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999

- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM)

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

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

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

- 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.

- CSCsd93977

  Symptoms: While a router boots, the **xconnect** command on a serial interface may be rejected because of the relative sequence of the commands.

  Conditions: This symptom is observed on a Cisco router that has channelized interfaces.

Workaround: After the router has completed the boot process, copy the startup configuration to the running configuration.

- CSCsd99936

  Symptoms: The IfOutOctets MIB counter may not increment properly for a dot1q subinterface that is configured for L2VPN.

  Conditions: This symptom is observed on a Cisco 10000 series hat runs Cisco IOS Release 12.2SB or Release 12.2SBB that is configured for Xconnect. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCse75551

  Symptoms: A tree trace request may return incorrect results about the number of equal-cost MPLS paths between the router on which the tree trace request originates and the router that is the target of the tree trace request.

  Conditions: This symptom is observed when a tree trace request is issued on a router for a target IP address and when some of the equal-cost paths between this router (that is, the originating router) and the target router traverse another router on which a single interface provides a connection to multiple downstream neighbors.

  Workaround: Do not use a single interface to connect to multiple downstream neighbors. Rather, use separate interfaces to connect to each of the downstream neighbors.

- CSCsf09638

  Symptoms: The deletion of the ifIndex does not synchronize to a standby RP that functions in the STANDBY HOT state.

  Conditions: This symptom is observed on a Cisco router when a PortChannel or PortChannel subinterfaces are created or deleted and when a switchover occurs.

  Workaround: There is no workaround.

- CSCsf19418

  Symptoms: A router may reload unexpectedly when you enter the **show mpls ldp graceful-restart** command.

  Conditions: This symptom is observed when either of the following conditions are present:

  - When the command output has a “Down Neighbor Database” entry that expires by reaching the reconnect timeout limit while the command output is generating the neighbor address list.
  - When the command output is paged at the “--More--” string within the context of displaying addresses.

  Workaround: Do not enter the **show mpls ldp graceful-restart** command when a graceful-restart database entry is about to expire. When the command output is paged at the “--More--” string within the context of displaying addresses and when the Down Neighbor Database entry may have expired, type the letter “Q” to abort any further output of addresses.

- CSCsg17790

  Symptoms: MPLS traffic may be dropped for a few seconds during an RP switchover.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS LDP and occurs because of a timing issue.

  Workaround: There is no workaround.

- 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.

- CSCsg50061

  Symptoms: When queries are performed by using an old Cisco MIB, that is, a MIB in the format OLD-CISCO-xxx-MIB in which "xxx" defines the MIB, high CPU usage may occur on the PRE-3 and a CPUHOG condition may occur in the SNMP ENGINE process:

  ```
  SYS-3-CPUHOG Task is running for (2000)msecs, more than (2000)msecs (91/91),
  process = SNMP ENGINE.
  ```

  Conditions: This symptom is observed on a Cisco 10000 series and is most likely to occur when queries are performed that use SNMP requests with multi-variable-bindings in a single PDU, for example, when you use the OLD-CISCO-CHASSIS-MIB and when a get request is done on "chassis.1.0 chassis.2.0 chassis.3.0 chassis.4.0", that is, on chassisType.0, chassisVersion.0, chassisId.0, and romVersion.0.

  Workaround: Do not use the old Cisco MIBs. These MIBS were depreciated many years ago and support for them has not been maintained. Rather, use the current standard MIBs. If you must use the old Cisco MIBs, ensure that the management application does not attempt to poll the OLD-CISCO-CHASSIS-MIB (and possibly others) using PDUs with multi-variable-bindings.

  Further Problem Description: To prevent access to these old Cisco MIBs, an SNMP view access control configuration should be used. The following configuration prevent access to the OLD-CISCO-CHASSIS-MIB and the OLD-CISCO-SYS-MIB by using the community string "public":

  ```
  snmp-server view no_old system excluded
  snmp-server view no_old chassis excluded
  snmp-server community public view no_old RW
  ```

- CSCsg67551

  Symptoms: LDP sessions flap after a switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router and that is configured for EIGRP and BGP.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reload the router.

- CSCsg74796

  Symptoms: A Cisco 10000 series that has a PRE-3 may generate an "MCE_HT-3-TOOBIG" error message, after which the PRE-3 crashes.

  Conditions: This symptom is observed when packets that are larger than 400 bytes are forwarded via IP CEF from the Network Management Ethernet (NME) interface to interfaces that have PXF enabled.

  Workaround: Disable IP CEF forwarding on the NME interface by entering the **no ip route-cache cef** command followed by the **no ip route-cache** command.

- CSCsg82372

  Symptoms: The **show atm vc | include** *pattern* command may take a long time to complete. This situation may be accompanied by high CPU usage.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB and that has at least one ATM line card installed on which ATM VCs are configured.

Workaround: Do not use the **include** keyword. Rather, enter the **show atm vc** command for specific VCs.

- CSCsg85441

  Conditions: When you configure a large number of individual PVCs (about 52,000) and enter the **show running-config** command, it may take about 50 seconds before the command output is displayed.

  Symptoms: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may also affect other platforms.

  Workaround: There is no workaround.

- CSCsg95072

  Symptoms: The **show atm vc** command may be missing VCs.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB or a rebuild of Release 12.2(31)SB when at least one ATM line card is installed and VCs are configured.

  Workaround: You can display the ATM VC information by using a more specific command: enter the **show atm vc interface atm** *card*/*subcard*/*port* command.

  Further Problem Description: The missing VCs tend to be from select ATM subinterfaces.

- CSCsg99945

  Symptoms: When you enter the **show running-config** command, the CPU usage may reach and remain at 99 percent for approximately 20 seconds.

  Conditions: This symptom is observed on a Cisco router only when there are more than several thousand VCs that are configured for PPPoX.

  Workaround: There is no workaround.

- CSCsh20989

  Symptoms: A router that generates traffic may not use the correct WRED profile in the output policy map.

  Conditions: This symptom is observed on a Cisco 10000 series that has an PRE-3 and occurs only for IPv4 and IPv6 traffic that is subjected to WRED on an output port.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCsg36389

  Symptoms: A router may crash because of a bus error when you remove a policy map or fragmentation from an interface. Before the router crashes, the following error message and a traceback are generated:

  ```
  %ALIGN-1-FATAL: Corrupted program counter TLB (load or instruction fetch) exception,
  CPU signal 10, PC = 0x0
  -Traceback=
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB and occurs only when fragmentation is enabled. However, the symptom is platform-independent.

  Workaround: Configure map-class fragmentation with Frame Relay traffic shaping (FRTS).

Resolved Caveats—Cisco IOS Release 12.2(31)SB1a

Cisco IOS Release 12.2(31)SB1a is a rebuild release for Cisco IOS Release 12.2(31)SB1. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB1a but may be open in previous Cisco IOS releases.

Basic System Services

- 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.

Miscellaneous

- CSCir00590

  Symptoms: VCs may enter an inactive state, preventing sessions from coming up over the VCs.

  Conditions: This symptom is observed on a Cisco 10000 series when you perform an OIR of the line card on which the VC are configured after at least one HA switchover has occurred.

  Workaround: Reload the router.

- CSCsd95631

  Symptoms: When you enter the **show atm vp** command for ATM VPs, a negative number of data VCs is displayed, which does not represent the actual number of VCs per VP.

  Conditions: This symptom is observed on a Cisco 10008 that runs Cisco IOS Release 12.3(7)XI. However, the symptom is not platform-specific, nor release-specific.

  Workaround: There is no workaround.

- CSCsf30762

  Symptoms: When bidirectional traffic passes a 1-port Gigabit Ethernet half-height line card, the Gigabit Ethernet ingress and egress interface counters report zero packets/second and zero bits/second.

  Conditions: This symptom is observed on a Cisco 10000 series when there is a large number (at least 10,000) of interfaces and/or broadband sessions and when traffic is sent over the Gigabit Ethernet interface of a 1-port Gigabit Ethernet half-height line card.

  Workaround: There is no workaround.

- 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.

- CSCsg18289

  Symptoms: Applying a line loopback onto an ATM interface has no effect.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **loopback line** command on an ATM interface. The output of the **show interfaces atm** command shows that “loopback set” and “loopback line” appear in the configuration. However, the “loop” LED on the line card does not illuminate either. Traffic through the interface continues uninterrupted.

  Workaround: There is no workaround.

- CSCsg24451

  Symptoms: Some line cards may be reported as deactivated when the router boots.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB and usually occurs for Gigabit Ethernet or Fast Ethernet line cards.

  Workaround: Enter the **hw-mod subslot** *slot*/*subslot* **reset** command for each affected line card.

  Alternate Workaround: Reload the router again.

- CSCsg45686

  Symptoms: The following warning message may be generated when PPPoX sessions are being established:

  ```
  %C10K_BBA_SESSION-4-WRN2EVENT: Temporarily unable to add session to VC session list
  ```

  Although this warning message is a low-priority message, the number of messages may be quite high when a large number of sessions is being established.

  Conditions: This symptom is observed on a Cisco 10000 series when an operation fails during the attempt to establish a session.

  Workaround: There is no workaround. However, the error message has no system impact, and the session is established during a next attempt.

Wide-Area Networking

- CSCsg31095

  Symptoms: Per-user DNS and WINS attributes are ignored.

  Conditions: This symptom is observed on a Cisco router when RADIUS returns per-user DNS and WINS attributes that are the last attributes for the user profile.

  Workaround: Move the DNS and WINS attributes to a position in the RADIUS profile that ensures that they are not the last attributes.

Open Caveats—Cisco IOS Release 12.2(31)SB1

Cisco IOS Release 12.2(31)SB1 is a rebuild release for Cisco IOS Release 12.2(31)SB. This section describes possibly unexpected behavior by Cisco IOS Release 12.2(31)SB1. All the caveats listed in this section are open in Cisco IOS Release 12.2(31)SB1. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCsa96960

  Symptoms: MPLS OAM echo request packets may be forwarded from a different interface than the interface that is reported in an MPLS echo reply that is sent in response to an LSP traceroute.

  Conditions: This symptom is observed on a Cisco router when an LSP traceroute is sent under the following conditions:

  – The penultimate hop has multiple parallel paths, at least one of which has MPLS enabled.

  – One or more of the parallel paths have MPLS disabled.

  Workaround: Ensure that MPLS is enabled on all equal-cost paths at the penultimate hop.

- CSCse75551

  Symptoms: A tree trace request may return incorrect results about the number of equal-cost MPLS paths between the router on which the tree trace request originates and the router that is the target of the tree trace request.

  Conditions: This symptom is observed when a tree trace request is issued on a router for a target IP address and when some of the equal-cost paths between this router (that is, the originating router) and the target router traverse another router on which a single interface provides a connection to multiple downstream neighbors.

  Workaround: Do not use a single interface to connect to multiple downstream neighbors. Rather, use separate interfaces to connect to each of the downstream neighbors.

- CSCsf97637

  Symptoms: When a Cisco router is the originator of an MPLS LSP Traceroute, a third-party vendor router that functions as a transit router may return a “DSMAP Mismatch Error” message.

  Conditions: This symptom is observed when a Cisco router is the originator of an echo request and when MPLS OAM is not supported or is disabled on a Cisco router that is located upstream from a third-party vendor router that also functions as a transit router.

  Workaround: Enable MPLS OAM on the Cisco router that functions as a transit router by entering the **mpls oam** command.

  Further Problem Description: When a downstream router ID is sent as “224.0.0.2”, the DSMAP TLV field “address type” is set to “IPv4 numbered” by Cisco routers. In this situation, the “address type” should be set to “IPv4 unnumbered” instead.

Resolved Caveats—Cisco IOS Release 12.2(31)SB1

Cisco IOS Release 12.2(31)SB1 is a rebuild release for Cisco IOS Release 12.2(31)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB1 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCef29931

  Symptoms: When a Telnet connection to a router that is configured for secure login fails, memory corruption may occur on the router, and the router may reload.

  Conditions: This symptom is observed when the **login block-for** *seconds* **attempts** *tries* **within** *seconds* command is enabled on the router and when a user enters an incorrect password for the *tries* argument.

  When the Telnet connection fails, the router enters the quiet mode. When the router leaves the quiet mode, the router is able to accept Telnet connections. However, when the Telnet connections fails again, memory corruption occurs before the router enter the quite mode, and the router reloads.

  Workaround: There is no workaround.

- CSCse68964

  Symptoms: When a PTA session is created with a traffic classifier (TC) service, the Parent-Session-ID attribute of the accounting packets of the TC service on the ISG does not match the Acct-Session-Id of the parent session after 16^2 (that is, 000000EE) Acct-Session-Ids have been used.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG and that is configured with QinQ subinterfaces over which PTA sessions are established.

  Workaround: There is no workaround.

- CSCsg03830

  Symptoms: The **tacacs-server directed-request** command appears in the running configuration when is should be disabled. When you disable the command by entering **no tacacs-server directed-request** and reload the router, the command appears to be enabled once more.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for CSCsa45148, which disables the **tacacs-server directed-request** command by default.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa45148. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Temporary Workaround: Each time after you have reloaded the router, disable the command by entering **no tacacs-server directed-request**.

IP Routing Protocols

- CSCei77227

  Symptoms: A Cisco router that functions in a multicast VPN environment may crash.

Conditions: This symptom is observed when you check the unicast connectivity and then unconfigure a VRF instance.

Workaround: There is no workaround.

- CSCse67198

  Symptoms: A router may hang when you send a VRF ping to an outside NAT address of a directly connected router.

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

  Workaround: There is no workaround.

- CSCse68877

  Symptoms: A label mismatch may occur between the CEF table and the BGP table, and a new label may not be installed into the CEF table.

  Conditions: This symptom is observed after a BGP flap has occurred on a Cisco router that is configured or MPLS VPN but that does not function in an inter-autonomous system and that does not have multiple VRFs.

  Workaround: There is no workaround. After the symptom has occurred, enter the **clear ip route** command for the affected VRF.

- CSCse99493

  Symptoms: A router that is configured for NAT Overload may crash while performing dynamic translation from many ports to one port.

  Conditions: This symptom is observed after more than 5000 translations have been performed.

  Workaround: There is no workaround.

- 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.

- CSCsf06946

  Symptoms: After you have removed a loopback interface from the configuration on the primary RP while the same loopback interface is required as part of another configuration, for example, as an update source for a BGP neighbor, the standby RP does not reload successfully when you reset it.

  Conditions: This symptom is observed on a Cisco router and occurs only in an HA environment.

  Workaround: Remove all configurations that reference the loopback interface before you remove the loopback interface.

Miscellaneous

- CSCek38430

  Symptoms: The standby PRE reloads unexpectedly.

Conditions: This symptom is observed on a Cisco 10000 series when either of the following events occur:

- Multiple users simultaneously add and delete service policies.
- Multiple users periodically enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an ATM subinterface. For example, the users enter the commands with intervals of 5 to 10 seconds during a period of 2 or 3 minutes.

Workaround: There is no workaround.

- CSCek40192

  Symptoms: Traffic convergence takes more than 50 ms after an Automatic Protection Switching (APS) switchover has occurred.

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

  Workaround: There is no workaround.

- CSCek44373

  Symptoms: The standby RP may generate "%SYS-2-MALLOCFAIL: Memory allocation" failures and may or may not reset repeatedly.

  Conditions: These symptoms are typically observed in highly scaled configurations that consist, for example, of many BGP peers or PPPOA sessions. The symptoms occur during the SSO configuration-synchronization phase and bulk-synchronization phase when the standby RP comes online, during the configuration of the router, after a switchover, or when peer interfaces and/or routing neighbors flap. The symptom is more likely to occur on an RP that does not contain so much physical I/O memory and/or operates at a relatively slow CPU speed.

  Workaround: Scale down the configuration, or reduce the number of BGP peers or PPPOA sessions. If the peer neighbors or interfaces flap, determine the root cause, and correct the flapping problem.

- CSCek48136

  Symptoms: A router may crash when QoS policy changes occur for a large number of VCs.

  Conditions: This symptom is observed on a Cisco router when the QoS changes are made via an automated script.

  Workaround: Modify the VCs manually, one by one.

- CSCek48575

  Symptoms: A router may crash when you first enter the **ip portbundle** command for PPPoE sessions in a port-bundle host key (PBHK) configuration and when you then change an ACL.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and that has a configuration such as the following:

  ```
  ip portbundle
   length 3
   match access-list 103
   source Loopback2
  ```

  Workaround: There is no workaround.

- CSCek51309

  Symptoms: A router may reload when a QoS policy is attached to a number of PPPoL2TP sessions on an LNS and when the physical link or sessions are flapping. The QoS policy contains a shaping and queuing configuration.

Conditions: This symptom is observed on a Cisco router that functions as an LNS when there are many route changes, either because a physical interface flaps or because the PPPoL2TP sessions flap.

Workaround: There is no workaround.

Further Problem Description: The symptoms are specific to L2TP sessions and queuing features in the policy map.

- CSCek53084

  Symptoms: Attachment circuit (AC) and AToM clients show up as compatible while they have no peer on the other side.

  Conditions: This symptom is observed on a Cisco router that is configured for In-Service Software Upgrade (ISSU) when you downgrade from Cisco IOS Release 12.2(31)SB to Cisco IOS Release 12.2(28)SB or one of it's rebuilds.

  Workaround: There is no workaround.

- CSCek55284

  Symptoms: When you upgrade the Cisco IOS software image from Cisco IOS Release 12.2(28)SB3 to Cisco IOS Release 12.2(31)SB by entering the **issu loadversion** command, the standby RP remains in the RPR mode, preventing the upgrade from proceeding.

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

  Workaround: There is no workaround.

- CSCsb71154

  Symptoms: When a VC that is configured under a VP goes down, PPPoE sessions can still be established over the VC.

  Conditions: This symptom is observed on a Cisco 10000 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface or after you have reloaded the router.

  Workaround: There is no workaround.

- CSCsc14052

  Symptoms: A Cisco 10000 series may crash and generate one of the following error messages:

  ```
  PXF DMA Error - Command Packet Handle Out of Range
  ```

  or:

  ```
  PXF DMA - Small Free Packet Handle Access Out of Range
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that processes L2TP traffic and that has a heavy CPU load.

  Workaround: There is no workaround.

- CSCsd25699

  Symptoms: MLP traffic fails during a PRE failover of the protect router.

  Conditions: This symptom is observed on a Cisco 10000 series when a PRE failover occurs on the protect router because of an MR-APS cable break failover from the protect router to the working router.

  Workaround: If the active controller is brought up after the MR-APS failover, manually reverse APS.

- CSCsd65283

  Symptoms: A router may crash when you enter the **connect** command.

Conditions: This symptom is observed when one of the VCs that is being configured in the **connect** command is down.

Workaround: Ensure that both VCs are up when you enter the **connect** command.

- CSCsd98686

  Symptoms: The following error message and traceback may be displayed:

  ```
  %XDR-6-CLIENTISSUBADTXTFM: Failed to xmit_transform message - to slot 6, client CEF
  push, context 0

  -Traceback= 41437E50 4141D584 41432B64 4141D674 41421558 414219DC 41416388 413F4738
  413F4EA0 403E11D0 402652A8 40402AD0 404F23F8 404F23E4
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for SSO and that has dCEF enabled by default. The symptom occurs when you disable dCEF and then re-enable it, for example by entering the no **ip cef** command followed by the **ip cef distributed** command or the **no ip routing** command followed by the **ip routing** command.

  Workaround: There is no workaround.

- CSCse01989

  Symptoms: When you apply a channel group to a Gigabit Ethernet interface that has the **negotiation auto** command enabled, the **negotiation auto** command is unexpectedly enabled on the port-channel interface. This situation causes a synchronization failure on the standby RP, in turn, causing the standby RP to reset.

  Conditions: This symptom is observed on a Cisco router that has redundant RPs in an HA configuration.

  Workaround: Manually remove the auto-negotiation configuration from the port-channel interface by entering the **no negotiation auto** command.

- CSCse08652

  Symptoms: When you configure MVPN over an MLPoATM interface, multiple PXF crashes may occur.

  Conditions: This symptom is observed on a Cisco 10000 series when you first enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the MLPoATM interface and then enter the **show pxf cpu queue** *interface* command on the MLPoATM interface. After these commands, the PXF crashes start. This situation may cause the boot flash to be fully consumed.

  Workaround: There is no workaround.

- CSCse11078

  Symptoms: When you enter the **aps force** or **aps manual** command on a Cisco 10000 series router that has interfaces that are configured for Multi-Router APS (MR-APS), the standby PRE may not properly reflect the MR-APS state of the interfaces.

  Conditions: This symptom is observed in a configuration with two Cisco 10000 series routers that are configured with dual PREs that function in SSO mode.

  Workaround: There is no workaround.

- CSCse25431

  Symptoms: A LAC may generate an “HQF_WARN_HQF_OVERSUBSCRIPTION_DETECTED” error message when it is oversubscribed with a high number of sessions. The LAC may crash when it is severely oversubscribed.

Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC when you scale PPPoEoQinQ sessions with QoS configured and when you oversubscribe to a very high rate. The oversubscription is configured on a subinterface via an MQC policy that is enabled through the **shape average percent** *percent* command.

Workaround: Do not configure the oversubscription factor above the supported factor of 50:1.

- CSCse36785

  Symptoms: Packets that are switched via CEF to a service network with DHCP-based IP subscribers may be dropped at an ISG.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when both of the following conditions occur:

  – A subscriber sets the DHCP broadcast bit in a DHCP request to zero, as a Microsoft DHCP host typically does.

  – The subscriber connection occurs via Dynamic VPN selection, that is, the subscriber connects to the ISG via a global interface but the IP address is assigned by VPN services that are selected by the subscriber.

  Workaround: If the DHCP client is a router that runs a Cisco IOS software image, enter the **ip dhcp-client broadcast** command on router. If the DHCP client runs Microsoft software, there is no workaround.

- CSCse36890

  Symptoms: Multicast packets that traverse GRE tunnels over a Gigabit EtherChannel (GEC) bundle interface may be dropped because of multicast RPF failures.

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

  Workaround: Do not use a GEC bundle. Rather, configure the GRE tunnels on regular GE interfaces.

- CSCse41596

  Symptoms: A Cisco router does not update the IP address of a RADIUS proxy session, and the RADIUS proxy session is terminated after the IP address timer expires.

  Conditions: This symptom is observed only when the router functions both as an Intelligent Service Gateway (ISG) and as a DHCP server.

  Workaround: There is no workaround.

- CSCse42494

  Symptoms: A router crashes when it has more than 65,536 L2TP sessions in a multiple-hop configuration. At a multiple-hop router, an L2TP session is created inbound and outbound for each user session. This means that the number 65,536 is exceeded when more than 32,768 sessions are traversing the tunnel.

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

  Workaround: Configure less than 32,768 user sessions (half of 65,536).

- CSCse57312

  Symptoms: The MQC output policer does not add the L2 header as part of its calculation.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only for multicast traffic on Ethernet and ATM interfaces.

  Workaround: There is no workaround.

- CSCse65884

  Symptoms: The **atm pvp** *vpi* **l2transport** command may disappear from the configuration.

Conditions: This symptom is observed after you have reloaded the router.

Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reconfigure the command.

- 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.

- CSCse70667

  Symptoms: A router crashes during an attempt to access the interface policy-map statistics.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with invalid policy maps that have VLAN classes with invalid filter types.

  Workaround: There is no workaround.

- CSCse77610

  Symptoms: Different bandwidth percentages may be assigned to police bandwidths than the actual percentages that were configured.

  Conditions: This symptom is observed on a Cisco 10000 series that is equipped with a PRE3 and that has one or more percentage-based policed policy maps that are applied to PPPoEoVLAN sessions via a virtual template or via a RADIUS configuration.

  You can diagnose the symptoms by entering the **show policy-map interface virtual-access** *interface-number* command and by comparing the bandwidth (bps) value of the police sections against what is expected for the session.

  A percentage-based policed policy map may involve the following configuration:

  police percent *percentage burst-time* **ms** *burst-excess-time* **ms conform-action transmit exceed-action drop violate-action drop**

  Possible Workaround: Do not configure percentage-based policers. Rather, configure explicit bandwidths for policers.

- CSCse77758

  Symptoms: The secondary RP may fail to boot (that is, reach the SSO mode) after the **ipv6 unicast-routing** command is disabled on the primary RP. During the reboot of the secondary RP, the following message is displayed on its console:

  ```
  %Cannot disable IPv6 CEF on this platform
  ```

On the primary RP, the following messages are displayed on its console:

```
Config Sync: Starting lines from PRC file: -no ipv6 cef
Config Sync: Bulk-sync failure, Reloading Standby
```

Conditions: This symptom is observed on a Cisco router that has dual RPs and that runs Cisco IOS Release 12.2SB.

Workaround: First, re-enable IPv6 by entering the **ipv6 unicast-routing** command on the primary RP. Then, reboot the secondary RP.

- CSCse77804

  Symptoms: When you downgrade the Cisco IOS software image from Cisco IOS Release 12.2(33)SB to Release 12.2(28)SB, the download fails.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PREs (PRE A and PRE B) and that is configured for ISSU when the following sequence of events occurs:

  1. The active PRE is switched over from PRE A to PRE B.
  2. The **loadversion** command is issued from PRE B, which is the active PRE.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when PRE A is the active PRE and when the **loadversion** command is issued from PRE A.

- CSCse78987

  Symptoms: The PXF engine may crash because of an invalid sequence of DMA commands.

  Conditions: This symptom is observed on a Cisco 10000 series when a multicast packet is replicated on an interface on which an Intelligent Services Gateway (ISG) session is established.

  Workaround: There is no workaround.

- CSCse79681

  Symptoms: The PXF engine of a PRE-3 may crash while processing IP upstream traffic.

  Conditions: This symptom is observed on a Cisco 10000 series when there is no input feature such as an input ACL or a QoS feature on the interface in the upstream direction. In this situation, traffic is processed by an output feature such as an output ACL or QoS feature.

  Workaround: There is no workaround.

- CSCse81709

  Symptoms: Frame-Relay end-to-end keepalives (EEKs) on an MFR interface may be stuck in the down state after an SSO has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PRE-3 processors.

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

- CSCse83989

  Symptoms: When you reset or insert a line card while traffic is flowing, the line card may reset continuously.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 1-port channelized OC-12 line card and a 4-port channelized OC-3 line card.

  Workaround: Stop the traffic that is destined for the line card before you reset or insert the line card.

- CSCse86477

  Symptoms: A router crashes when you detach a map class from a Frame Relay DLCI interface.

  Conditions: This symptom is observed on a Cisco router that is configured with an output policy with Frame Relay traffic shaping.

  Workaround: There is no workaround.

- CSCse87221

  Symptoms: Tracebacks are generated during an SSO switchover.

  Conditions: This symptom is observed on a Cisco router when you enter the **redundancy force-failover main-cpu** command.

  Workaround: There is no workaround.

- CSCse87499

  Symptoms: A platform that is configured for Cisco IOS Redundancy Facility (RF) may reload unexpectedly.

  Conditions: This symptom is observed when an RF client fails while the standby RP attempts to transition to the hot standby state.

  WorkAround: There is no workaround.

- CSCse88338

  Symptoms: A router crashes when you first enter the **clear subscriber session all** command and then enter the **show ip subscriber dangling** *number-of-seconds* command.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG while processing traffic.

  Workaround: Do not enter the **show ip subscriber dangling** *number-of-seconds* command or the **clear ip subscriber dangling** *number-of-seconds* command.

- CSCse89636

  Symptoms: The following error messages and tracebacks are generated on a PRE-3 when an ISSU switchover occurs from a PRE-2 that runs Cisco IOS Release 12.2(27)SBB5 to a PRE-3 that runs Cisco IOS Release 12.2(31)SB:

  ```
  %LFD-3-INVINSTALLER: Wrong installer 4 for packet 0/0 update (was 1) %LSD-3-LABEL:
  can’t create rewrite for label=0
  ```

  Conditions: This symptom is observed on a Cisco 10000 series but could occur on any platform when you perform an ISSU switchover.

  Workaround: There is no workaround.

- CSCse91107

  Symptoms: NSF does not function properly for VPN traffic, causing packet loss. This situation can be verified in the output of the **show ip bgp vpnv4 all labels** command.

  Conditions: This symptom is observed on an MPLS PE router after an ISSU upgrade.

  Workaround: There is no workaround.

- CSCse93747

  Symptoms: When you configure QoS on an ATM PVC under a point-to-point subinterface, the router may not accept and save an output service policy when an input service policy is already present on the interface.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE-2 or PRE-3.

Workaround: First configure the output service policy and then configure the input service policy.

- CSCse94304

  Symptoms: A PRE crashes, and CPUHOG error messages are generated.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in an MR-APS configuration with another Cisco 10000 series and that has MLP configured.

  Workaround: Disable MLP.

- CSCse94879

  Symptoms: When you upgrade from Cisco IOS Release 12.2(27)SBB5 to Release 12.2(27)SBB6 by using ISSU, a traffic interruption of about 30 seconds may occur on an OC-12 POS line card.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PRE-2 processors and one or more OC-12 POS line cards. The symptom could also occur with other releases.

  Workaround: There is no workaround.

  Further Problem Description: The upgrade should reload the OC-12 POS line card but not reset the line card. Instead, an internal error occurs on the line card, causing the line card to crash. However, the line card automatically reboots and successfully recovers, and traffic resumes after about 30 seconds of interruption.

- CSCse96084

  Symptoms: “Suspend/Activate service-policy” messages flood the console when there are thousands of sessions hosted on the router.

  Conditions: This symptom is observed on a Cisco 10000 series when the sessions come up or go down.

  Workaround: Disable console logging on the router.

  Further Problem Description: The messages are internal messages that should not appear on the console.

- CSCse97283

  Symptoms: ARPs may be lost. This situation may cause adjacencies to go down, which, in turn, may cause peer routers to stop responding.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only when buffer memory is extremely congested for one minute or more. For example, extreme congestion occurs when the “low buffer hdl drop(s)” counter in the output of the **show pxf cpu stat drop 1** increments at a rate that is equal to the incoming ARP traffic rate.

  Workaround: There is no workaround.

- CSCse99137

  Symptoms: A Cisco router that functions as an Intelligent Service Gateway (ISG) returns the wrong value in Cisco Vendor Specific Attribute (VSA) 250 (ssg-account-info) in a RADIUS packet.

  Conditions: This symptom is observed when the ISG responds to a service query from a Cisco Subscriber Edge Services Manager (SESM) or service provider portal server.

  Workaround: There is no workaround.

- CSCsf03188

  Symptoms: A router crashes when you use TFTP to download a configuration to the running configuration and when the downloaded configuration clears the controllers.

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

Workaround: There is no workaround.

- CSCsf05044

  Symptoms: In a very large-scale MLPP configuration, that is, more than 300 MLP bundles, when a PRE-2 HA switchover occurs on a Cisco 10000 series, the following error message and/or a traceback may be generated on the connected Cisco 10000 series at the far end:

  ```
  ttcm_add_mlp_member: unable to install mlp link
  ```

  Conditions: This symptom is observed during the renegotiation of the links and line protocol of the interfaces and bundles.

  Workaround: There is no workaround.

- CSCsf05685

  Symptoms: A router that functions as a DHCP server and DHCP relay may fail to issue or renew a lease.

  Conditions: This symptom is observed after a class name is uploaded onto the DHCP server, which causes the parameters of DHCP-initiated sessions for an ISG to be changed.

  Workaround: There is no workaround.

- CSCsf08208

  Symptoms: The username attribute is not present in the accounting stop records.

  Conditions: This symptom is observed when a PPP session is brought up with Transparent Auto logon (TAL).

  Workaround: There is no workaround.

- CSCsf08287

  Symptoms: After a PRE failover as occurred, the Multi-Router APS (MR-APS) state is mismatched between the active PRE and the standby PRE.

  Conditions: This symptom is observed on a Cisco 10000 series when the PREs function in SSO mode and when a 1-port OC-12 ATM line card or 4-port OC-3 ATM line card is connected to an ADM and is configured for MR-APS.

  Workaround: There is no workaround.

- CSCsf10896

  Symptoms: The parent session ID attribute is not present in the accounting records for prepaid services.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when accounting is enabled for any prepaid service.

  Workaround: There is no workaround.

- CSCsf11149

  Symptoms: When the CISCO-TAP2-MIB is implemented in the PXF engine, the PRE-3 does not tap packets. The PRE-3 does tap packets via the RP, which means a limitation in scale.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB, that has a PRE-3, and that has the Lawful Intercept feature enabled.

  Workaround: There is no workaround.

- CSCsf12056

  Symptoms: A LAC does not tap upstream packets via the CISCO-TAP2-MIB.

Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC and that has the Lawful Intercept feature enabled.

Workaround: There is no workaround.

- CSCsf12124

  Symptoms: The policer conform, exceed, and violate counters (both packets and bytes) in the output of the **show policy-map interface** command may stop incrementing and freeze at a certain value.

  When this situation occurs, usually, the bytes counters freeze first, and then, after some time, the packet counters freeze too. This situation may also cause the "policer drop-rate bps counter" to become stuck at zero because the "policer drop-rate bps counter" is based on changes in the bytes counters.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and occurs when the counters are very large, that is, at or very near their limits.

  Temporary Workaround: Remove and then re-apply the policy map on the interface to reset the counters to zero.

- CSCsf13802

  Symptoms: eBGP sessions may go down when they are established on MFR subinterfaces with several VPNs between a Cisco 10000 series that functions as a PE router and a Cisco 7200 series that functions as a CE router.

  Conditions: This symptom is observed when the Cisco 10000 series has input and output service policies and Frame Relay fragmentation configured in a map class that is applied to DLCIs on the MFR subinterfaces. The symptom occurs while there is no traffic on the MFR link between the PE and CE routers.

  Workaround: Remove either the service policies or Frame Relay fragmentation from the map class.

- CSCsf15121

  Symptoms: Packets that are encapsulated via PPPoE and that are generated by a Cisco 10000 series and sent to a PPPoE client may take into account the padding of the incoming frame in the length field of the PPPoE header. This situation may cause problems for certain protocol stacks.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC or PTA router and that terminates PPPoEoX sessions. The symptom occurs for all types of PPPoEoX sessions: PPPoEoA, PPPoEoARPA, PPPoEoVLAN, and PPPoEoQinQ. The incoming frames are Ethernet or PPPoEoA frames, which can be padded because of the 64-byte minimum frame size requirement of Ethernet.

  The symptom is caused by the fix for caveat CSCsd13298, which uses the full incoming frame size as the length field of the PPPoE header of the outgoing packet.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd13298. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCsf15164

  Symptoms: When a PRE-2 crashes and when the router is configured with a redundant PRE-2, a "PCI Retry Expire" error may occur after the crashinfo file has been generated.

  Conditions: This symptom is observed on a Cisco 10000 series and may occur even when the redundant PRE is not booted but remains in ROMmon.

  Workaround: There is no workaround.

Further Problem Description: Note that the “PCI Retry Expire” error is not the original cause for the crash, but is a secondary issue.

- CSCsf19377

  Symptoms: A Cisco 10000 series that is configured for MPLS AToM may crash.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround.

- CSCsf24720

  Symptoms: The PXF engine may crash when tapping is enabled.

  Conditions: This symptom is observed on a Cisco 10000 series that has the Lawful Intercept feature enabled when a truncation of the padding of a packet occurs, causing the Lawful Intercept feature to generate a replica.

  Workaround: There is no workaround.

- CSCsf25920

  Symptoms: The line protocol for an MFR interface may be up and the DLCIs may be in the active state even though the LMI is down.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB and occurs for MFR interfaces.

  Workaround: There is no workaround.

- CSCsf27677

  Symptoms: When you perform an In-Service Upgrade (ISU) upgrade (that is, a hardware upgrade) from a PRE-2 to a PRE-3, the Cisco 10000 series may crash and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x40378AAC-
  ```

  Conditions: This symptom is observed on a Cisco 10000 series but may occur on any platform when you perform an In-Service Software Upgrade (ISU). A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl? bugid=CSCse89636. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCsf96715

  Symptoms: The PXF engine may crash while a PPPoX session is established between a LAC and an LNS.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC and that has a QoS configuration.

  Workaround: Disable the QoS configuration on the LAC.

- CSCsf98115

  Symptoms: AAA output counters for Tx bytes and octets remain zero or are incorrect for LAC sessions.

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

  Workaround: There is no workaround.

- CSCsg00438

  Symptoms: Some Cisco 10000 series line cards may become stuck.

  Conditions: This symptom is observed when the router functions in a redundant configuration and occurs after you have reloaded the router.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, power-cycle the affected line cards or perform an OIR of the affected line cards.

- CSCsg03152

  Symptoms: A PRE-3 may run out of PXF buffer memory, causing all interfaces on the Cisco 10000 series to lose connectivity even though the output of a **show** command shows that the interfaces are in the up/up state.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router and that processes MFR traffic that is fragmented to various packet sizes in the direction of a CE router. The symptom occurs when you remove and re-add a service policy to a map class that is applied to MFR subinterfaces.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCsc30497

  Symptoms: When NAS-port based pre-authorization fails, the PPPoE session limit per VLAN is no longer applied, that is, the local limit is no longer applied to a particular interface.

  Conditions: This symptom is observed in Cisco IOS Release 12.3YM but may also occur in other releases.

  Workaround: There is no workaround.

- CSCse70647

  Symptoms: A router that functions as a BRAS or LNS crashes and generates one of the following error messages (or an error message that is similar to one of the following error messages):

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x607C0374
  ```

  or

  ```
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 206BCF18, data 21CD607D.
  -Process= "PPPoA Manager", ipl= 0, pid= 220
  ```

  or

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

  Conditions: This symptom is observed during PPP negotiations with a Microsoft PPP client that requests WINS or DNS data. Note that the symptom does not occur on a router that functions as a LAC.

  Workaround: There is no workaround. However, entering the **ppp max-failure 100** command may reduce the chances that the symptom occurs.

- CSCse78979

  Symptoms: PPPoA sessions do not synchronize to the standby PRE while VCs are recreated with a changed encapsulation type.

  Conditions: This symptom is observed on a Cisco 10000 series when you change the encapsulation type on the interface from MUX to SNAP and then back to MUX while PPPoA sessions are coming up. The symptom may be platform-independent.

Workaround: There is no workaround.

- CSCse81359

  Symptoms: After you have shut down a Frame Relay over MPLS (FRoMPLS) connection, the **xconnect** command is unexpectedly removed from the standby PRE, preventing the FRoMPLS connection from coming up after an HA switchover has occurred.

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

  Workaround: When you enter the **connect** command on the active PRE, also enter the **xconnect** command and any other configuration from the connect submode on the standby PRE to ensure that the complete configuration is retained on the standby PRE after an HA switchover has occurred.

- CSCse96387

  Symptoms: In a large scale Broadband Access Aggregation (BBA) environment, PPP negotiation may become stuck in a state in which one side is closed and the other side is constantly attempting to request options. This situation may cause all sessions to become stuck in a bad state that you must manually clear in order to recover from the state.

  Conditions: This symptom is observed on a Cisco router when a large volume of sessions comes up all at once as is common in an PPPoA BBA environment.

  Workaround: If you think you are encountering this caveat, please contact Cisco Technical Support Services for assistance and possible configuration tuning to minimize the chance that the symptom occurs again.

  Further Problem Description: If this is an option for your configuration, you can also reduce the rate of the incoming sessions to minimize the chance that the symptom occurs again.

- CSCse98867

  Symptoms: A router may reload when a multilink bundle goes down while packets are flowing.

  Conditions: This symptom is observed on a router that is configured for Multilink PPP (MLP) with hardware compression.

  Workaround: There is no workaround.

- CSCsf03371

  Symptoms: A router may crash after more than 260,000 PPPoX sessions have flapped.

  Conditions: This symptom is observed on a Cisco router when the **aaa new-model** command is disabled.

  Workaround: Enter the **aaa new-model** command.

- CSCsf06190

  Symptoms: Some PPP sessions do not properly synchronize to the standby RP.

  Conditions: This symptom is observed on a Cisco router that is configured for HA when many PPP interfaces flap at the same time.

  Workaround: There is no workaround.

- CSCsf12042

  Symptoms: PPP over Ethernet over Ethernet (PPPoEoE) and PPPoE over Q-in-Q (PPPoEoQ-in-Q) sessions fail to be established.

  Conditions: This symptom is observed on a Cisco router when the connections are made via Fast Ethernet or Gigabit Ethernet interfaces. Note that the symptom does not affect PPP over Ethernet over ATM (PPPoEoA) sessions.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(31)SB

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(31)SB. All the caveats listed in this section are open in Cisco IOS Release 12.2(31)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

IP Routing Protocols

- CSCse60837

  Symptoms: A router may crash when a switchover occurs from the active RP to the standby RP while the MVPN Extranet configuration is being deleted.

  Conditions: This symptom is observed on a Cisco router when the MVPN Extranet configuration is deleted via a script. When the MVPN Extranet configuration is deleted manually, the symptom does not occur.

  Workaround: There is no workaround.

Miscellaneous

- CSCej66992

  Symptoms: The statistic counters for a parent policy and for parts of a child policy may be incorrect in the output of the **show policy-map interface** *interface-name* command.

  Conditions: This symptom is observed on a Cisco 10000 series when an egress policy map is attached to an interface, when the egress policy map has a nested child service policy, and when you modify class maps in the child policy.

  Workaround: Remove the child policy map from the parent policy map before you modify the child class maps. Then, re-attach the child policy to the parent.

- CSCek45720

  Symptoms: A back-to-back ping does not traverse a native VLAN on a Cisco 10000 series.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB and occurs with both a PRE-2 and a PRE-3.

  Workaround: There is no workaround.

- CSCek47048

  Symptoms: PPPoA sessions do not come up after you have cleared them.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **clear pppatm interface atm** *interface-number* command to clear the sessions. Only a third of the sessions can be brought up afterwards.

  Workaround: Shut down the ATM interface, wait a short time, and bring up the ATM interface. Doing so enables all session to come up.

  Note that the sessions may recover automatically after four hours.

  Further Problem Description: When the symptom occurs, I/O memory is slowly depleted and is eventually exhausted.

- CSCsb71154

  Symptoms: When a VC that is configured under a VP goes down, PPPoE sessions can still be established over the VC.

Conditions: This symptom is observed on a Cisco 10000 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface or after you have reloaded the router.

Workaround: There is no workaround.

- CSCsc32700

  Symptoms: A router may not resume to forward VPN traffic after you have entered the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco router that function as a PE router in a VPN environment.

  Workaround: There is no workaround.

- CSCsd23425

  Symptoms: QoS statistics are not reflected properly in the output of the **show policy-map session uid** *uid-number* command.

  Conditions: This Symptom is observed on a Cisco 10000 series is has a PRE2 and that functions as a LAC.

  Workaround: There is no workaround.

- CSCsd47447

  Symptoms: A router crashes when a non-VLAN user class is configured under a parent policy with an action such as the **set qos-group** command.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs because a non-VLAN user class under a parent policy is an illegal configuration.

  Workaround: Do not configure a non-VLAN user class under a parent policy. However, note that you can configure a VLAN user class under a parent policy.

- CSCse25431

  Symptoms: A LAC may generate an "HQF_WARN_HQF_OVERSUBSCRIPTION_DETECTED" error message when it is oversubscribed with a high number of sessions. The LAC may crash when it is severely oversubscribed.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC when you scale PPPoEoQinQ sessions with QoS configured and when you oversubscribe to a very high rate. The oversubscription is configured on a subinterface via an MQC policy that is enabled through the **shape average percent** *percent* command.

  Workaround: Do not configure the oversubscription factor above the supported factor of 50:1.

- CSCse48598

  Symptoms: Traffic on a native VLAN interface is not forwarded.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB and occurs only when the VLAN interface is the native VLAN. Traffic is forwarded properly on other VLANs.

  Workaround: There is no workaround.

- CSCse75238

  Symptoms: A router may crash when the service-policy information of a session is displayed.

  Conditions: This symptom is observed when tens of thousands of sessions are established on a PTA router that has a service-policy instance for each session via a policy map on a virtual template.

  Workaround: There is no workaround.

- CSCse81340

  Symptoms: A Cisco 10000 series that functions as a PE router in an MPLS VPN network may crash in the LDP process after multiple switchovers have occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE3, 800 NSR peers, 400 NSF peers, and 400 static peers, and that is loadbalanced to the network core.

  Workaround: There is no workaround.

- CSCse93327

  Symptoms: A Cisco 10000 series may crash when you modify a class map.

  Conditions: This symptom is observed when the QoS configuration is scaled to a high number of VLAN classes and when you attempt to delete a child class with a WRED configuration from a policy that is attached to a VLAN group class.

  Workaround: First, remove the WRED configuration from the class. Then, delete the class.

  Alternate Workaround: Detach the service policy from the interface, delete the class, and then re-attach the service policy to the interface.

TCP/IP Host-Mode Services

- CSCsd54305

  Symptoms: BGP sessions that are established between two route reflectors (RRs) flap continuously because TCP times out for keepalives.

  Conditions: This symptom is observed on a Cisco router that functions as an RR in an MPLS VPN Interautonomous System (InterAS) scenario and occurs when the RR receives VPNv4 prefixes from a PE router. In this situation, the BGP session between the RR and the second RR flaps.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(31)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

IP Routing Protocols

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml.

Miscellaneous

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml.

TCP/IP Host-Mode Services

- 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.

Resolved Caveats—Cisco IOS Release 12.2(31)SB

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(31)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- 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.

Resolved Caveats—Cisco IOS Release 12.2(28)SB4

Cisco IOS Release 12.2(28)SB4 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB4 but may be open in previous Cisco IOS releases.

EXEC and Configuration Parser

- CSCsd72511

  Symptoms: When TACACS+ command accounting is enabled, SNMPv3 community strings may not be encrypted.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2.(25)SEE. The symptom also affects other releases.

  Workaround: There is no workaround.

Miscellaneous

- CSCek51309

  Symptoms: A router may reload when a QoS policy is attached to a number of PPPoL2TP sessions on an LNS and when the physical link or sessions are flapping. The QoS policy contains a shaping and queuing configuration.

  Conditions: This symptom is observed on a Cisco router that functions as an LNS when there are many route changes, either because a physical interface flaps or because the PPPoL2TP sessions flap.

  Workaround: There is no workaround.

  Further Problem Description: The symptoms are specific to L2TP sessions and queuing features in the policy map.

- CSCse71784

  Symptoms: When you configure an IP address as the tunnel source and the tunnel interface has been disconnected, shut down, or reconfigured, the tunnel interface line protocol can no longer come up.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S or Release 12.2SB.

  Workaround: Do not configure an IP address as the tunnel source. Rather, at both ends of the tunnel, configure the source interface or the interface name as the tunnel source.

Wide-Area Networking

- CSCse70647

  Symptoms: A router that functions as a BRAS or LNS crashes and generates one of the following error messages (or an error message that is similar to one of the following error messages):

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x607C0374
  ```

  or

  ```
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 206BCF18, data 21CD607D.
  -Process= "PPPoA Manager", ipl= 0, pid= 220
  ```

  or

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

  Conditions: This symptom is observed during PPP negotiations with a Microsoft PPP client that requests WINS or DNS data. Note that the symptom does not occur on a router that functions as a LAC.

  Workaround: There is no workaround. However, entering the **ppp max-failure 100** command may reduce the chances that the symptom occurs.

- CSCse96387

  Symptoms: In a large scale Broadband Access Aggregation (BBA) environment, PPP negotiation may become stuck in a state in which one side is closed and the other side is constantly attempting to request options. This situation may cause all sessions to become stuck in a bad state that you must manually clear in order to recover from the state.

  Conditions: This symptom is observed on a Cisco router when a large volume of sessions comes up all at once as is common in an PPPoA BBA environment.

  Workaround: If you think you are encountering this caveat, please contact Cisco Technical Support Services for assistance and possible configuration tuning to minimize the chance that the symptom occurs again.

  Further Problem Description: If this is an option for your configuration, you can also reduce the rate of the incoming sessions to minimize the chance that the symptom occurs again.

- CSCsf06190

  Symptoms: Some PPP sessions do not properly synchronize to the standby RP.

  Conditions: This symptom is observed on a Cisco router that is configured for HA when many PPP interfaces flap at the same time.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(28)SB3

Cisco IOS Release 12.2(28)SB3 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB3 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCin93236

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

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCeh31423. See the information in the Bug Toolkit:

http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh31423

Workaround: There is no workaround.

IP Routing Protocols

- CSCeh83666

  Symptoms: A router may crash or fail to allocate a port.

  Conditions: This symptom is observed on a Cisco router that is configured for NAT Overload and occurs because the “prev_block” pointer may be dereferenced when it is NULL.

  Workaround: There is no workaround.

Miscellaneous

- CSCsb72921

  Symptoms: A QoS policy map that includes the **priority** and **police** commands in the same class may be rejected.

  Conditions: This symptom is observed on a Cisco router when you migrate from Cisco IOS Release 12.2S to either Release 12.2SB or Release 12.2SBC.

  Workaround: Edit the policy manually; enter the **police** command before you enter the **priority** command, and save the configuration.

  Further Problem Description: The symptom occurs because the bandwidth allocations are checked while the policy is being configured. In earlier Cisco IOS releases such as Release 12.2(25)S, the bandwidth allocations are checked only when the complete policy is attached to the interface. Because the **police** command provides the bandwidth limit for the **priority** command in this configuration, you must enter the **police** command before you enter the **priority** command.

- CSCsd44856

  Symptoms: A Cisco 10000 series crashes when you unconfigure MLP.

  Conditions: This symptom is observed when you first remove the controller and then remove a member of a bundle that belongs to the controller.

  Workaround: First remove all the bundles from the controller before you remove the controller.

- CSCsd80857

  Symptoms: An LFIB entry in the PXF engine may become corrupted, preventing from forwarding traffic.

  Conditions: This symptom is observed on a Cisco 10000 series when first a VRF is removed and then a link flap occurs.

  Workaround: Clear the affected route.

- CSCse25130

  Symptoms: IPCP renegotiations of an MLP interface may time out during renegotiation after an MR-APS failure has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in an MR-APS configuration with another Cisco 10000 series.

Workaround: There is no workaround.

- CSCse39760

  Symptoms: A PA-CC does not recover when you perform a soft or hard OIR of the standby RP.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with dual RPs after a switchover has occurred that causes the standby RP to become the active RP. In this situation, when you perform a soft or hard OIR of the standby RP, the PA-CC does not recover because the PA-CC fails to initialize.

  Workaround: There is no workaround.

- CSCse47922

  Symptoms: WRED random drops that occur in different ToS and DSCP classes do not correlate with the configured thresholds as you would expect.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCse61834

  Symptoms: When you modify an ATM PVC by entering the **pvc** *vpi/vci* command, any subsequent modifications in the VC class that is assigned to this PVC do not take effect.

  Conditions: This symptom is observed when the PVC is preconfigured with a VC class when the following events occur:

  1. You make a configuration change in the PVC.
  2. You change the configuration in the VC class.

  The configuration change in the VC class does not take effect.

  Workaround: First complete the configuration changes in the VC class. Then, change the configuration in the PVC.

Resolved Caveats—Cisco IOS Release 12.2(28)SB2

Cisco IOS Release 12.2(28)SB2 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB2 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeg63395

  Symptoms: A large latency may occur when packets are forwarded by a router.

  Conditions: This symptom is observed on a Cisco router when a DoS attack is launched from another router towards a POS interface of the Cisco router.

  Workaround: There is no workaround. Although the symptom causes performance degradation, it does not cause loss of functionality.

- CSCin99433

  Symptoms: Without configuring any command related to Kerberos other than a Kerberos password command, a configuration synchronization failure may occur because of a PRC mismatch.

  Conditions: This symptom is observed when you boot a Cisco router that is configured for AAA.

Workaround: There is no workaround.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

- CSCsd27777

  Symptoms: When you enter the **clear subscriber session all** command while traffic is being processed, the CPU usage of the router increases to 99 percent and sessions go down gradually. At the same time, the router automatically reinitiates sessions, and "%SSSMGR-3-MEMORY_LOW" and "%IDMGR-3-INVALID_ID:" error messages are generated. Eventually, the router generates "%TCP-6-NOBUFF:" and "%SYS-2-MALLOCFAIL" errors messages, and either resets all its interfaces or reloads.

  Conditions: This symptom is observed on a Cisco 10000 series that runs 16,000 PTA sessions with ISG features and 16,000 plain L2TP sessions. On all sessions, stateless traffic is being processed. The symptom is not specific to a Cisco 10000 series and may occur on other platforms that function in a similar configuration.

  Workaround: Do not clear all sessions at once via the **clear subscriber session all** command.

- CSCse11615

  Symptoms: When you enter the **enable** privileged EXEC command, an "Access Denied" message is generated.

  Conditions: This symptom is observed on a Cisco router when you have configured AAA authentication and when the **enable password** global configuration command is configured.

  Workaround: Configure the password for the **enable password** global configuration command to be no more than two characters.

  Alternate Workaround: Remove the **enable password** global configuration command from the startup configuration.

Miscellaneous

- CSCef82084

  Symptoms: Spurious memory accesses occur on a Cisco 7200 series and ALIGN-3-SPURIOUS error messages are generated.

  Conditions: This symptom is observed on a Cisco 7200 series that processes traffic through a serial interface.

  Workaround: There is no workaround.

- CSCeh40183

  Symptoms: A router reloads unexpectedly when the **show policy interface** EXEC command is entered.

Conditions: This symptom is observed on a Cisco router when two users are connected to the router and simultaneously enter the **show policy interface** EXEC command.

Workaround: Ensure that only one user at a time enters the command.

- CSCei27448

  Symptoms: A router may crash while displaying the output of the **show ip pim mdt bgp** command.

  Conditions: This symptom is observed when withdraws for a MDT source group are received by PIM from BGP while you enter the **show ip pim mdt bgp** command.

  Workaround: There is no workaround. To reduce the chance of the router crashing, change the *screen-length* argument in the **terminal length** *screen-length* command to 0. Doing so prevents the router from pausing between multiple output screens. (The default of the *screen-length* argument is 24.)

- CSCek03591

  Symptoms: A traffic class is deleted even when there is traffic that matches the ACL for the traffic class.

  Conditions: This symptom is observed when a subscriber session is configured with a traffic class that is configured with a Layer 4 redirect feature and idle timeout.

  Workaround: There is no workaround.

- CSCek20952

  Symptoms: The following error message may be generated when you configure a police statement in a policy map:

  ```
  Maximum rate for the policer is 0, conform action is drop
  ```

  Conditions: This symptom is observed on a Cisco router that functions in a L2VPN configuration with QoS features.

  Workaround: There is no workaround.

- CSCek25822

  Symptoms: A PRE crashes when you enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs whether or not the router processes traffic.

  Workaround: Do not enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Further Documentation: The above-mentioned configuration is not supported on the Cisco 10000 series.

- CSCek30152

  Symptoms: When a T3/E3 Serial SPA is configured in Kentrox mode with a small bandwidth between 22 kbps and 250 kbps, either in T3 or E3 mode, the firmware miscalculates the bandwidth allocation and allows up to 24M of traffic to pass through.

  Conditions: This symptom is observed on a Cisco 7304 and a Cisco 12000 series.

  Workaround: Do not configure such a small bandwidth when the T3/E3 Serial SPA is configured in Kentrox mode. The minimal bandwidth on a T3/E3 Serial SPA that is configured in Kentrox mode is either 1500 kbps in T3 mode or 1000 kbps in E3 mode.

- CSCek35146

  Symptoms: When you remove and re-insert an MSC-100 card in which one or two SPAs are installed, the SPAs may become disabled for 10 to 12 minutes, after which they recover automatically.

  Conditions: This symptom is observed on a Cisco 7304 when you perform either a physical OIR or a soft-OIR by entering the **hw-module slot** *slot-number* **stop** command followed by the **hw-module slot** *slot-number* **start** command. The symptom occurs only when the time between the removal and the re-insertion is 2 to 3 seconds.

  Workaround: Do not re-insert the MSC-100 card too quickly after you have removed it. Wait at least 10 seconds before you re-insert the card.

- CSCek37011

  Symptoms: A line card may crash when you attempt to remove the child policy from the HQoS parent.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the line card has an interface that is configured as follows:

  - The interface faces the MPLS core.
  - The interface has an HQoS policy with a child policy.
  - The HQoS policy has a classification that is based on the MPLS EXP bits.

  Workaround: There is no workaround.

- CSCek39877

  Symptoms: A 4-port OC-3 ATM line card may not perform an APS switchover when a signal degrade (SD) or signal fail (SF) condition is present.

  Conditions: This symptom is observed on a Cisco 10000 series when bit errors occur on the on the 4-port OC-3 ATM line card.

  Workaround: There is no workaround.

- CSCek44427

  Symptoms: An interface of a T3/E3 serial SPA passes traffic even though the output of the **show controller** command shows that there is a “Loss of Frame” alarm. When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the SPA, the alarm is not cleared.

  Conditions: This symptom is observed on a Cisco platform that is configured with a T3/E3 serial SPA.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface at the remote end.

  Further Problem Description: The symptom does not affect proper operation of the platform or the traffic. However, the incorrect alarm status may affect network management utilities.

- CSCin96524

  Symptoms: Control plane traffic may be dropped from a multilink interface.

  Conditions: This symptom is observed only when the multilink interface is oversubscribed and does not occur under normal traffic conditions.

  Workaround: Reduce the traffic rate.

  Alternate Workaround: Apply some type of queueing mechanism on the interface.

- CSCin97726

  Symptoms: On a Cisco 7500 router, the console of the active RSP may hang.

  Conditions: This symptom is observed when the router functions in RPR mode and when you attempt to access the standby RSP file system from the console of the active RSP, for example, by entering the **write memory** command or the **dir slavedisk0:** command.

  Note that the symptom is not specific to the Cisco 7500 series and may also occur on other platforms.

  Workaround: There is no workaround.

  Further Problem Description: Normal operation of the router is not affected, but the console becomes inaccessible.

- CSCsb01043

  Symptoms: When a Turbo ACL classification table grows beyond a certain size, a memory allocation failure may occur or the router may crash.

  If the router runs Cisco IOS Release 12.1E or 12.3, memory corruption may occur, causing the router to crash. If the router runs Cisco IOS Release 12.2S, an error message similar to the following may appear during a Turbo ACL compilation, the compilation will fail, and a recompilation is forced:

  ```
  %SYS-2-CHUNKBADELESIZE: Chunk element size is more than 64k for TACL Block -Process=
  "TurboACL", ipl= 0, pid= 82
  ```

  These symptoms do not occur because of an out-of-memory condition.

  Conditions: This symptom is observed on a Cisco router that is configured for Turbo ACL. The Cisco 10000 series is not affected.

  Workaround: Monitor the output of the **show access-lists compiled** command and force the Turbo ACL tables to be cleared if a table is at risk of growing large enough to trigger the symptoms.

  The tables that have significant sizes are the first and third tables shown next to “L1:” and the first table shown next to “L2:”. When the number after the slash for one of these tables is greater than 16384 for the “L1” tables or greater than 32768 for the “L2” table, the table is already too large and the symptom may occur any moment.

  When the number is in the range from 10924 to 16384 inclusive for the “L1” tables or the range from 21846 to 32768 inclusive for the “L2” tables, the table size will be too large on the next expansion. An expansion occurs when the number to the left of the slash reaches 90 percent of the value to the right of the slash. When the value to the left of the slash approaches 90 percent of the value to the right, enter the **no access-list compiled** command followed by the **access-list compiled** command to disable and re-enable Turbo ACL. Doing so causes the tables to be cleared and, therefore, delay the expansion. This workaround may be impractical when there is a high rate of incoming packets and when entries are added frequently to the tables.

  Alternative Workaround: Disable Turbo ACL by entering the **no access-list compiled** command.

  Note that neither of these workarounds are supported on a Cisco 7304 that is configured with an NSE-100: there is no workaround for this platform.

- CSCsb13836

  Symptoms: A Cisco 7304 may crash because of a bus error during normal operation when a external flash card is present.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2(20)S4 or Release 12.2(20)S8. The symptom may also occur in other releases.

  Workaround: Do not use an external flash card. Rather, use an internal flash card.

- CSCsb33258

  Symptoms: An RP crashes during BGP convergence when MVPNs are configured.

  Conditions: This symptom is observed on a Cisco router after a duplicate BGP MDT extended community message is received that specifies a different Route Descriptor (RD) for an MDT that already exists for the specified MDT source and group address.

  Workaround: There is no workaround.

- CSCsb64858

  Symptoms: A switch or router may crash while processing a longest match lookup in the CEF table.

  Conditions: This symptom is observed on a Cisco platform when a packet is punted because of an exception such as the occurrence of an ICMP redirect message while a longest match lookup is performed in the CEF table.

  Workaround: Disable ICMP redirect messages by entering the **no ip redirects** interface configuration command on all interfaces of the router.

- CSCsb83990

  Symptoms: All on-demand VCs may become stuck in the inactive state because of insufficient bandwidth on one ATM interface.

  Conditions: This symptom is observed on a Cisco 10000 series when the creation of a VC fails because there are no more VCCIs, a line card failure occurs, or a toaster failure occurs. Each of these situations cause the ATM bandwidth to be depleted, and, in turn, prevent bandwidth from being available for any other ATM subinterfaces.

  Workaround: There is no workaround.

- CSCsc08491

  Symptoms: A virtual-access subinterface may not forward any traffic.

  Conditions: This symptom is observed on a Cisco router with a virtual-access application that causes virtual-access subinterface to be created.

  Workaround: There is no workaround.

- CSCsc37472

  Symptoms: The output rate counters for a member link of a multilink interface do not increment when you look at the output of the **show interfaces** command.

  Conditions: This symptom is observed on a Cisco 10000 series when packets are properly delivered through the member link of the multilink interface.

  Workaround: Look at the PXF counters in the output of the **show pxf cpu queue multilink** *interface* or **show pxf cpu subblock multilink** *interface* commands.

- 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.

- CSCsc78707

  Symptoms: The **mpls l2transport route** command may be rejected as an invalid input.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCsc86262

  Symptoms: When you configure OAM on an ATM subinterface in an AToM configuration, the ATM subinterface goes down.

  Conditions: This symptom is observed on a Cisco 7304 that has a NSE-100 and that functions as a PE router in an MPLS backbone.

  Workaround: There is no workaround. Note that the symptom does not occur when you disable the PXF engine.

- CSCsc90843

  Symptoms: A router that is configured with a multilink bundle may reload unexpectedly with the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions: This symptom is observed on a Cisco router when you attempt to remove a service policy from a multilink interface.

  Workaround: There is no workaround.

- CSCsd00354

  Symptoms: The output of the **show policy-map interface** command shows the output queue packets and bytes counters as zero.

  Conditions: This symptom is observed on a Cisco 10000 series on queues for which a policer is applied.

  Workaround: Use the policer's counters in the output of the **show policy-map interface** command to determine the number of forwarded and dropped packets and bytes for the queue.

- CSCsd14277

  Symptoms: A ping does not pass through a Fast Ethernet interface that functions in AToM port mode.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that has the **xconnect** interface configuration command enabled on the interface of a 1-port Fast Ethernet port adapter (PA-FE) that is installed in a port adapter carrier card (7300-CC-PA).

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

Alternate Workaround: Enter the **shutdown** interface configuration command, the **xconnect** interface configuration command, and then the **no shutdown** interface configuration command on the affected interface.

- CSCsd25699

  Symptoms: MLP traffic fails during a PRE failover of the protect router.

  Conditions: This symptom is observed on a Cisco 10000 series when a PRE failover occurs on the protect router because of an MR-APS cable break failover from the protect router to the working router.

  Workaround: If the active controller is brought up after the MR-APS failover, manually reverse APS.

- CSCsd35958

  Symptoms: A Cisco 7304 that is configured with an NPE-G100 processor and ATM VCs may reload unexpectedly.

  Conditions: This symptom is observed when a hierarchical policy on an ATM VC has the **shape average** command enabled.

  Workaround: Do not use a hierarchical policy on an ATM VC.

- 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.

- CSCsd44475

  Symptoms: A ping may fail when packets pass from an MPLS VPN into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that functions as a PE router, and that is connect to the MPLS core via a serial interface.

  Possible Workaround: Do not use a serial interface to connect the PE router to the MPLS core. Rather, use another type of interface.

  Further Problem Description: The symptom occurs because the tunnel adjacency is not complete in the PXF engine, preventing packets from being correctly punted and the adjacency from becoming complete.

- CSCsd49072

  Symptoms: The output of the **show policy-map interface** command shows incorrect statistics for a DSCP-based WRED policy. Also, when the class-map parameters are dynamically changed, the WRED statistics are lost.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsd49196

  Symptoms: After you have configured ingress NetFlow on an interface, the output of the **show ip cache verbose flow** command may show incorrect values in the “Active” seconds column.

Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S9, Release 12.2(20)S10, or Release 12.2(25)S8 when the **ip flow ingress** command is configured on an interface. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCsd58203

  Symptoms: The output of the **show ip cache flow** command, may shows some flows with a size of 4294M, which is the maximum size that can fit in a 32-bit value (2^32). Note that you can view the flows more easily in the output of the **show ip cache flow | i M|Pkts** command.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(25)S7. The symptom may occur in other releases.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is of a cosmetic nature. Proper operation of the router is not affected.

- CSCsd62942

  Symptoms: The PXF engine on a Cisco 7304 that functions as a PE router may crash when traffic passes from the MPLS core to a CE router.

  Conditions: This symptom is observed when the traffic from the MPLS core is de-aggregated on the PE router into CE-facing interfaces that are configured into a VRF and that perform IP load-sharing and occurs while the PXF engine is active on the PE router.

  Workaround: Disable IP-load-sharing on any interfaces that are configured into a VRF, such as the CE-facing interfaces.

  Alternate Workaround: Disable PXF packet-processing on the PE router.

- CSCsd68445

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

  1. Symptom 1: You may not be able to apply a QoS policy map with class-based shaping that is configured in the default class on a dot1q subinterface, and the following error messages may be generated:

     Configuring this shaping class will impact guarantees in other classes under this policy-map

     Condition 1: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(27)SBC2 when a hierarchical QoS policy is configured in the following way and when the shape rate is higher than the CIR rate:

     policy-map child-qos
     class *user-defined-class*
     priority
     police cir *cir-rate*
     bc *Bc* **be** *Be*
     conform-action transmit
     exceed-action drop

     policy-map parent-qos
     class class-default
     shape average *shape-rate*
     service-policy child-qos

     Workaround 1: There is no workaround.

2. Symptom 2: You may not be able to apply a QoS policy map with class-based shaping that is configured in the default class on a dot1q subinterface, and the following error messages may be generated:

   Configuring this shaping class will impact guarantees in other classes under this policy-map

   Condition 2: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(27)SBC2 when a single policy map with class-based shaping is configured in the following way:

   policy-map shaping-qos
   class class-default
   shape average *shape-rate*

   Workaround 2: Perform the following steps:

   a. Configure a new class map that has the same characteristics as the original class default as in the example below, in which the new class map is called "my-class-default":

      class-map match-all my-class-default
      match any

   b. Configure the new policy map by using the just created class-default equivalent class ("my-class-default") as following example, in which the new policy map is called "my-policy-map":

      policy-map my-policy-map
      class my-class-default
      shape average *shape-rate*

   c. Apply the service policy ("my-class-default") to the dot1q subinterface.

- CSCsd68659

  Symptoms: When you change the **atm dsx3mode** command for the framing of one port of a 8-port E3/DS3 ATM line card (ESR-8E3/DS3-ATM), all ports on the line card are affected.

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

  Workaround: There is no workaround.

- CSCsd69402

  Symptoms: Pre-classification on a GRE tunnel does not function.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 processor.

  Workaround: There is no workaround.

- CSCsd71131

  Symptoms: A service policy may be suspended when you enter the **clear interface** command for a multilink interface that has six members.

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

  Workaround: There is no workaround.

- CSCsd76528

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

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

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

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

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

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

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

- CSCsd83503

  Symptoms: NetFlow updates only MPLS-related egress records but not IPv4 ingress records.

  Symptoms: This symptom is observed on a Cisco 10000 series that has an PRE-2 and that has the **ip route-cache flow** command enabled on its main ATM and GE interfaces and the **mpls netflow egress** command enabled on its ATM subinterfaces (on which PVCs are configured) and GE subinterfaces.

  Note that the **ip route-cache flow** command is automatically converted into the **ip flow ingress** command and the **mpls netflow egress** command is automatically converted into the **ip flow egress** command, and these commands are stored in NVRAM. The symptom occurs after you have reloaded the PRE-2.

  Workaround: Disable and re-enable the **ip flow ingress** command on the main interfaces.

- CSCsd88288

  Symptoms: Packet loss may occur on a GRE tunnel on which CEF is enabled.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs the c7300-js-mz image of Cisco IOS Release 12.2(25)S8. The symptom may also occur in Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: Disable PXF on the Cisco 7304. If this is not an option, there is no workaround.

- CSCsd91238

  Symptoms: The success rate of pings decreases when you increase the packet size of the pings, and the output of the **show ip traffic** command shows increasing ICMP checksum errors.

  Conditions: This symptom is observed on a Cisco 7304 that has a an NSE-100, that runs Cisco IOS Release 12.2(28)SB, and that is configured with a 2-port OC-3 ATM line card (7300-2OC3ATM-SMI) when MLP and VRF are enabled on a virtual template that automatically configures the ATM PVC bundle on the line card.

  Workaround: Disable VRF forwarding on the virtual template.

  Alternate Workaround: Disable PPP on the ATM PVC bundle.

- CSCsd93728

  Symptoms: A router that functions as an LNS may crash while processing traffic over L2TP connections, and the following error message is generated:

  ```
  Cause 00000010 (Code 0x4): Address Error (load or instruction fetch) exception
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(28)SB and that is configured for QoS. The symptom occurs during normal operation.

Workaround: There is no workaround.

- CSCsd98928

  Symptoms: A router may crash when you enter the **show policy-map interface** command while an automated script completes the policy map and then removes the policy map during cleanup.

  Conditions: This symptom is observed on a Cisco router when you enter the **show policy-map interface** command while, at the same time, the automated script removes the policy map.

  Workaround: There is no workaround.

- CSCse00469

  Symptoms: When you boot the router, the SuperACL process causes a high CPU usage for an extended time, and not all configured policy maps are compiled.

  Conditions: This symptom is observed on a Cisco 10000 series when there are hundreds (or more) policy maps in the configuration.

  Workaround: Reduce the number of policy maps. If this is not an option, there is no workaround.

- CSCse00609

  Symptoms: Serial interfaces go down after an RP switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that has serial interfaces configured on either a channelized OC-3 or channelized OC-12 line card.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred. Bring the serial interfaces back up by resetting the line card.

- CSCse01030

  Symptoms: When an ATM interface has a QoS policy, locally generated traffic such as OSPF DPP traffic may not be transmitted.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCse06387

  Symptoms: A Cisco 7304 may reload unexpectedly after two HA switchovers have occurred.

  Conditions: This symptom is observed when 4000 virtual circuits are configured on the router.

  Workaround: There is no workaround.

- CSCse20029

  Symptoms: A router that is configured for MPLS and NetFlow may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco router that has the **vpdn enable** and **ip vrf** commands enabled.

  Workaround: There is no workaround.

- CSCse51608

  Symptoms: When you enter the **xconnect** command, the command is not accepted.

  Conditions: This symptom is observed on a Cisco 7200 series, irrespective of which interface the command is entered for.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCek01499

  Symptoms: When a CE router that is configured for MPLS reloads, a software-forced crash may occur on the connected PE router because of memory corruption.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has two RPs that function in SSO mode. The symptom does not occur when the router has only a single RP.

  Workaround: There is no workaround.

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml.

Wide-Area Networking

- CSCeh58376

  Symptoms: A serial interface on a channelized port adapter may stop forwarding traffic through the router but traffic to and from the router over the interface may still go through. The Tx accumulator "value" counter in the output of the **show controllers cbus** Exec command does not exceed the value 2, as is shown in the following example:

  ```
  Router#sh controllers cbus | include Serial5/1/0.1/2/6/2:0
  Serial5/1/0.1/2/6/2:0, txq E8001B40, txacc E8000412 (value 2), txlimit 26
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S when QoS is configured on at least one interface on the VIP in which the channelized port adapter is installed. The symptom occurs after the affected interface has flapped very frequently because of OSI layer 1 errors. The symptom may also occur in other releases.

  Workaround: Remove and reconfigure the controller of the affected interface.

- CSCek24091

  Symptoms: A PPP session fails to come up, and the following debug message is generated:

  ```
  PPP SSS: stale named authen method list "default"
  ```

  Conditions: This symptom is observed only when a service policy is applied and when the default PPP authentication method list is used.

  Workaround: Use a PPP authentication method list other than the PPP authentication default method list.

- CSCek32043

  Symptoms: cRTP may become disabled on an interface when you disable and re-enable the **ip rtp header-compression** command on the interface.

  Conditions: This symptom is observed on a Cisco router that functions in an MLP configuration when the link (such as a Frame Relay link) and the MLP bundle clone from the same virtual template.

  Workaround: Reset the interface.

- CSCsc28120

  Symptoms: A Cisco 7301 may crash when a service policy is removed from an interface that is configured for Frame Relay encapsulation.

  Conditions: This symptom is observed when a service policy is configured on an interface before the encapsulation is changed to Frame Relay. When the service policy is then removed, the router crashes.

  Workaround: Remove the service policy before you change the encapsulation to Frame Relay.

- CSCsd71360

  Symptoms: PPP Multilink fragment loss occurs as the result of premature lost fragment timeouts. This can be seen in the lost fragment count in the output of the **show ppp multilink** command, as well as debug traces produced by the **debug ppp multilink events** command.

  Conditions: This symptom has been observed with Cisco IOS Release 12.2(28)SB and Release 12.4(6)T, but not with Cisco IOS Release 12.2(27)SBC2 or Release 12.4(4)T.

  Workaround: Configure the **ppp timeout multilink lost-fragment 1** command under the Multilink interface or the Virtual-Template interface corresponding to the multilink bundle.

Resolved Caveats—Cisco IOS Release 12.2(28)SB1

Cisco IOS Release 12.2(28)SB1 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB1 but may be open in previous Cisco IOS releases. Cisco IOS Release 12.2(28)SB1 support the Cisco 7304 only.

IP Routing Protocols

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml.

Miscellaneous

- CSCek35146

  Symptoms: When you remove and re-insert an MSC-100 card in which one or two SPAs are installed, the SPAs may become disabled for 10 to 12 minutes, after which they recover automatically.

  Conditions: This symptom is observed on a Cisco 7304 when you perform either a physical OIR or a soft-OIR by entering the **hw-module slot** *slot-number* **stop** command followed by the **hw-module slot** *slot-number* **start** command. The symptom occurs only when the time between the removal and the re-insertion is 2 to 3 seconds.

  Workaround: Do not re-insert the MSC-100 card too quickly after you have removed it. Wait at least 10 seconds before you re-insert the card.

- CSCsb13836

  Symptoms: A Cisco 7304 may crash because of a bus error during normal operation when a external flash card is present.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2(20)S4 or Release 12.2(20)S8. The symptom may also occur in other releases.

  Workaround: Do not use an external flash card. Rather, use an internal flash card.

- CSCsc86262

  Symptoms: When you configure OAM on an ATM subinterface in an AToM configuration, the ATM subinterface goes down.

  Conditions: This symptom is observed on a Cisco 7304 that has a NSE-100 and that functions as a PE router in an MPLS backbone.

  Workaround: There is no workaround. Note that the symptom does not occur when you disable the PXF engine.

- CSCsd44475

  Symptoms: A ping may fail when packets pass from an MPLS VPN into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that functions as a PE router, and that is connect to the MPLS core via a serial interface.

  Possible Workaround: Do not use a serial interface to connect the PE router to the MPLS core. Rather, use another type of interface.

  Further Problem Description: The symptom occurs because the tunnel adjacency is not complete in the PXF engine, preventing packets from being correctly punted and the adjacency from becoming complete.

- CSCsd49072

  Symptoms: The output of the **show policy-map interface** command shows incorrect statistics for a DSCP-based WRED policy. Also, when the class-map parameters are dynamically changed, the WRED statistics are lost.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsd49196

  Symptoms: After you have configured ingress NetFlow on an interface, the output of the **show ip cache verbose flow** command may show incorrect values in the “Active” seconds column.

Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S9, Release 12.2(20)S10, or Release 12.2(25)S8 when the **ip flow ingress** command is configured on an interface. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCsd58203

  Symptoms: The output of the **show ip cache flow** command, may shows some flows with a size of 4294M, which is the maximum size that can fit in a 32-bit value (2^32). Note that you can view the flows more easily in the output of the **show ip cache flow | i M|Pkts** command.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(25)S7. The symptom may occur in other releases.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is of a cosmetic nature. Proper operation of the router is not affected.

- CSCsd62942

  Symptoms: The PXF engine on a Cisco 7304 that functions as a PE router may crash when traffic passes from the MPLS core to a CE router.

  Conditions: This symptom is observed when the traffic from the MPLS core is de-aggregated on the PE router into CE-facing interfaces that are configured into a VRF and that perform IP load-sharing and occurs while the PXF engine is active on the PE router.

  Workaround: Disable IP-load-sharing on any interfaces that are configured into a VRF, such as the CE-facing interfaces.

  Alternate Workaround: Disable PXF packet-processing on the PE router.

- CSCsd69402

  Symptoms: Pre-classification on a GRE tunnel does not function.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 processor.

  Workaround: There is no workaround.

- CSCsd88288

  Symptoms: Packet loss may occur on a GRE tunnel on which CEF is enabled.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs the c7300-js-mz image of Cisco IOS Release 12.2(25)S8. The symptom may also occur in Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: Disable PXF on the Cisco 7304. If this is not an option, there is no workaround.

- CSCsd91238

  Symptoms: The success rate of pings decreases when you increase the packet size of the pings, and the output of the **show ip traffic** command shows increasing ICMP checksum errors.

  Conditions: This symptom is observed on a Cisco 7304 that has a an NSE-100, that runs Cisco IOS Release 12.2(28)SB, and that is configured with a 2-port OC-3 ATM line card (7300-2OC3ATM-SMI) when MLP and VRF are enabled on a virtual template that automatically configures the ATM PVC bundle on the line card.

  Workaround: Disable VRF forwarding on the virtual template.

  Alternate Workaround: Disable PPP on the ATM PVC bundle.

- CSCse01030

  Symptoms: When an ATM interface has a QoS policy, locally generated traffic such as OSPF DPP traffic may not be transmitted.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCse06387

  Symptoms: A Cisco 7304 may reload unexpectedly after two HA switchovers have occurred.

  Conditions: This symptom is observed when 4000 virtual circuits are configured on the router.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(28)SB

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(28)SB. All the caveats listed in this section are open in Cisco IOS Release 12.2(28)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsc17888

  Symptoms: FRoMPLS traffic does not pass through the first port of an 8-port multichannel T1/E1 8PRI (PA-MC-8TE1+).

  Conditions: This symptom is observed on a Cisco router that functions as a CE router in an AToM environment when the ports of the PA-MC-8TE1+ are configured for E1. Note that the symptom does not occur for IP traffic and L3 traffic on the first port of the PA-MC-8TE1+, nor for the remaining seven E1 ports.

  Workaround: There is no workaround.

- CSCsd27777

  Symptoms: When you enter the **clear subscriber session all** command while traffic is being processed, the CPU usage of the router increases to 99 percent and sessions go down gradually. At the same time, the router automatically reinitiates sessions, and "%SSSMGR-3-MEMORY_LOW" and "%IDMGR-3-INVALID_ID:" error messages are generated. Eventually, the router generates "%TCP-6-NOBUFF:" and "%SYS-2-MALLOCFAIL" errors messages, and either resets all its interfaces or reloads.

  Conditions: This symptom is observed on a Cisco 10000 series that runs 16,000 PTA sessions with ISG features and 16,000 plain L2TP sessions. On all sessions, stateless traffic is being processed. The symptom is not specific to a Cisco 10000 series and may occur on other platforms that function in a similar configuration.

  Workaround: Do not clear all sessions at once via the **clear subscriber session all** command.

- CSCsd38237

  Symptoms: The active RP or PRE may reload in the "db_record_set_field" function when the router runs out of memory resources.

Conditions: This symptom is observed on a Cisco router that is configured with many sessions and occurs because the ID manager cannot not enqueue the “db_field” to the “db_record” when the router runs out of memory resources.

Workaround: Limit the number of sessions on the router to ensure that there are sufficient memory resources.

IP Routing Protocols

- CSCeh91717

  Symptoms: When IPv4 routes are imported into a VRF, the routes in the VRF CEF table are marked as “unusable” and “no label”.

  Conditions: This symptom is observed on a Cisco router when the “BGP Support for IP Prefix Import from a Global Table into a VRF Table” feature is enabled and when you enter the **import ipv4 unicast** command under a VRF.

  Workaround: There is no workaround.

- CSCej72829

  Symptoms: Some BGP SSO peers become disabled.

  Conditions: This symptom is observed after an SSO switchover occurs on a Cisco router.

  Workaround: There is no workaround. Note that after five minutes the BGP SSO peers are automatically re-enabled.

- CSCsc37461

  Symptoms: A PE router that functions in an MPLS VPN configuration may take a long time to converge.

  Conditions: This symptom is observed when an interface goes down and when an MP-BGP next hop that points to this interface is no longer reachable. This MP-BGP next hop remains unreachable until the Interior Gateway Protocol (IGP) finds an alternate path. If the BGP scanner runs while the MP-BGP next hop is unreachable, VRF routes that use this MP-BGP next hop may be removed from the VRF routing table. However, usually, when the next BGP scanner runs, these VRF routes are updated and then re-imported into VRF routing table.

  Workaround: The probability for the symptom to occur depends on the elapse time between the interface going down and the IGP convergence and can be decreases by tuning the IGP parameters for a faster convergence.

- CSCsd17747

  Symptoms: When you enter the **ip pim vrf register-source** command on an interface and then delete the interface or its IP address, the command remains in the configuration. This situation causes the bulk synchronization to fail and the standby RP to reset continuously after an RP switchover has occurred. Then, because the register source (the interface) cannot be found, a BEM failure occurs.

  Conditions: These symptoms are observed when the interface forwards traffic from a nondefault VRF and when the interface has a register source configured.

  Workaround: Remove the **ip pim vrf register-source** command from the interface before you delete the interface or its IP address.

Miscellaneous

- CSCef47220

  Symptoms: A path trace buffer value may be displayed as UNSTABLE in the output of the **show controllers** command when you enter this command for an AU-3 port and look for the overhead bytes.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 4-port channelized OC-3 line card with an E1 interface that is configured for AU-3. The E1 interface has the **overhead j1 length 16 transmit-message** *string* command enabled.

  Workaround: There is no workaround.

- CSCef47280

  Symptoms: A T1 interface that is configured for AU-4 mapping on a 4-port channelized OC-3 line card does not come up.

  Conditions: This symptom is observed on a Cisco 10000 series when the T1 interface interoperates with a third-party vendor test analyzer device.

  Workaround: There is no workaround.

- CSCeg11769

  Symptoms: When class-based weighted fair queueing (CBWFQ) is configured, the router may not match the input packet rate.

  Conditions: This symptom is observed on a Cisco router that is configured for ATM and Frame Relay.

  Workaround: There is no workaround.

- CSCeg69418

  Symptoms: You cannot re-enable Home Agent (HA) functionality on a router after you have first unconfigured it.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured for mobile IP.

  Workaround: There is no workaround.

- CSCeg88253

  Symptoms: Loss of packets may occur on video queues.

  Conditions: This symptom is observed on a Cisco 10000 series that has Class-Based Weighted Fair Queueing (CBWFQ) configured on a PPP over Ethernet over ATM (PPPoEoA) link and occurs when traffic is being processed.

  Workaround: There is no workaround.

- CSCeh54607

  Symptoms: On a router that processes a high traffic rate, the output of the **show processes cpu** command shows 100 percent CPU usage.

  Conditions: This symptom is observed on a Cisco router when the following conditions are present:

  - The router processes 70 PTA PPPoE sessions.
  - There are 70,000 packets per second with 120 bytes per packet upstream.
  - There are 5600 packets per second with 1500 bytes per packet downstream.

  Workaround: Reduce the traffic rate.

- CSCei38741

  Symptoms: Tracebacks are generated on a Cisco 10000 series that is configured with serial interfaces.

  Conditions: This symptom is observed when you change the encapsulation on a serial interface from PPP to Frame Relay.

  Workaround: Before you change the encapsulation from PPP to Frame Relay, enter the **no encapsulation ppp** command.

- CSCei54002

  Symptoms: A QoS group that is set through QoS Policy Propagation via BGP (QPPB) may not function.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE2.

  Workaround: Use QPPB to set the IP precedence.

- CSCej02774

  Symptoms: When you use the **BREAK** key to interrupt the image boot process and then enter the **dir** command from the ROMmon prompt, a recurring "Arithmetic Overflow Exception" may occur.

  Conditions: This symptom is observed on a Cisco 10000 series that has 104480 Kbytes of main memory and occurs only when a file system device driver is recursively loaded because you used the **BREAK** key to interrupt the image boot process and then entered the **dir** command without first resetting the ROMmon.

  Workaround: Let the image boot and then enter the **dir** command. If you must interact with the file system via the ROMmon when the boot process has been interrupted, enter the **reset** command. If autoboot is enabled, use the **BREAK** key immediately after the banner line appears on screen.

- CSCej46675

  Symptoms: A ping over an MLP connection may fail.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 336 bundles with 3 links each. Note that the symptom does not occur when the router has 100 bundles with 10 links each or 126 bundles with 8 links each.

  Workaround: There is no workaround.

- CSCej63166

  Symptoms: A router that is configured as an LSR may generate a "%LSD-4- LABEL_RESOURCE" error message when you attempt to extend the label range.

  Conditions This symptom is observed when the LSR is configured with a limited label range when you attempt to extend the label range.

  Workaround: Enter the **no mpls label range** command and reconfigure the extended label range.

- CSCej87817

  Symptoms: Policing does not drop any packets after the packets are sent or received at a rate that is much higher than the committed information rate (CIR).

  Conditions: This symptom is observed on a Cisco 7500 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCek00986

  Symptoms: A configuration does not synchronize to the standby RP and a traceback is generated.

Conditions: This symptom is observed on a Cisco router that has dual RPs and that has the **crypto key zeroize rsa** command enabled.

Workaround: There is no workaround.

- CSCek03591

  Symptoms: A traffic class is deleted even when there is traffic that matches the ACL for the traffic class.

  Conditions: This symptom is observed when a subscriber session is configured with a traffic class that is configured with a Layer 4 redirect feature and idle timeout.

  Workaround: There is no workaround.

- CSCek11664

  Symptoms: A forwarded packet may be lost on a PPPoE session.

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

  Workaround: There is no workaround.

- CSCek21091

  Symptoms: PPPoX multicast traffic is process-switched by default. This is improper behavior.

  Conditions: This symptom is observed when the **no ip mroute-cache** command is enabled for virtual-template interfaces, causing IP multicast traffic to be process-switched.

  Workaround: Enter the **ip mroute-cache** command for each virtual-template interface.

- CSCek25123

  Symptoms: When you apply a HQoS policy that has a shape parameter of 1 Gb in its parent policy to a subinterface, a traceback is generated. When there are more than 112 subinterfaces, you cannot apply the policy map to interfaces that exceed the 112th subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series when you apply or remove a HQoS policy to or from a subinterface and when the bandwidth in the parent policy map is 1 Gb.

  Workaround: There is no workaround.

- CSCek25822

  Symptoms: A PRE crashes when you enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs whether or not the router processes traffic.

  Workaround: Do not enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Further Documentation: The above-mentioned configuration is not supported on the Cisco 10000 series.

- CSCek27708

  Symptoms: A 1-port channelized OC-12 or 4-port channelized OC-3 line card may reset.

  Conditions: This symptom is observed on a Cisco 10000 series when you run a script that configures the line card with 768 E1 or T1 interfaces with either SDH or SONET framing.

  Workaround: There is no workaround.

- CSCek31331

  Symptoms: Gigabit Ethernet line cards flap and go down.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with multiple pairs of Gigabit Ethernet line cards when traffic flows at or is approaching the line rate.

Workaround: Either turn on or turn off negotiation on the affected pair of line cards and the point of traffic generation.

- CSCek34834

  Symptoms: Input drops or packet drops may occur when a 1-port Gigabit Ethernet half-height line card is processing IMIX traffic.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port Gigabit Ethernet half-height line card.

  Workaround: There is no workaround.

- CSCek36080

  Symptoms: A Cisco router that functions as an Intelligent Services Gateway (ISG) may reload when an error condition occurs in the control plane.

  Conditions: This symptom is observed under a rare conditions when an error occurs while a session that contains auto services is brought up or while a service profile that contains auto services is activated. The symptom occurs because of a timing issue.

  Workaround: Do not use auto services in the user profile.

- CSCek56991

  Symptoms: A Cisco 7200 series may send a corrupted packet via a 2-port T3 serial, enhanced port adapter (PA-2T3+). The rate of corrupted packets is very low.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB, Release 12.4T, or Release 12.4(4)XD3 and occurs when the router functions under high stress conditions such as a high CPU load and an oversubscribed interface of the PA-2T3+.

  Workaround: Avoid a high CPU load and oversubscription of the interface of the PA-2T3+.

- CSCin97726

  Symptoms: On a Cisco 7500 router, the console of the active RSP may hang.

  Conditions: This symptom is observed when the router functions in RPR mode and when you attempt to access the standby RSP file system from the console of the active RSP, for example, by entering the **write memory** command or the **dir slavedisk0:** command.

  Note that the symptom is not specific to the Cisco 7500 series and may also occur on other platforms.

  Workaround: There is no workaround.

  Further Problem Description: Normal operation of the router is not affected, but the console becomes inaccessible.

- CSCsa56416

  Symptoms: In order for Ethernet over MPLS (EoMPLS) to function properly in either port mode or VLAN mode, the Ethernet controller must operate in promiscuous mode, that is, all MAC address filtering must be disabled. On the 8-port Fast Ethernet (FE) line card, there is one single register that controls the enabling and disabling of address filtering for the whole line card. Therefore, if even one single EoMPLS circuit is created on any of the eight ports of the line card, address filtering is disabled for all eight ports, that is all eight ports operate promiscuous mode. This situation is not desirable.

Conditions: This symptom is observed on a Cisco 10000 series that is configured for EoMPLS when you create an AToM circuit by entering the **xconnect** command on an Ethernet controller of the 8-port FE line card. In this situation, promiscuous mode is automatically enabled on the Ethernet controller and remains enabled for all eight ports of the line card until the last AToM circuit is removed from the Ethernet controller by entering the **no xconnect** command.

Workaround: There is no workaround.

- CSCsb10347

  Symptoms: Multilink interfaces remain down after an SSO switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for LFIoFR and occurs only when traffic is flowing while an SSO switchover occurs. When there is no traffic, the interfaces come up normally.

  Workaround: There is no workaround.

- CSCsb32888

  Symptoms: Forcing **release** or **renew** commands on a BVI interface fails.

  Conditions: The symptom has been observed on the Cisco 7200 platform.

  Workaround: There is no workaround.

- CSCsb36094

  Symptoms: Policing in the outward direction is not performed for IP packets with an “IP Options” payload.

  Conditions: This symptom is observed on a Cisco 10000 series that processes incoming IP packets with the “IP Options” field. The policing actions are ignored for the outgoing IP packet.

  Workaround: There is no workaround.

- CSCsb79060

  Symptoms: A T1 interface that is configured on a channelized OC-3 line card or OC-12 line card may send a Loss of Framing (LoF) alarm, causing the T1 interface to enter the down/down state. Even after you have entered the **loopback local** command, have configured HDLC encapsulation, and have configured the clock source as internal, the T1 interface does not transition to the up state.

  Another symptom is that the framing may be good, but the TX data path is not good, causing the T1 interface to enter the up/down state. The output counters on the PRE increment, but the packets never actually leave the channelized line card.

  Conditions: These symptoms are observed on a Cisco 10000 series.

  Workaround: Reload the channelized line card by entering the **hw-module slot** *slot-number* **reset** command.

- CSCsb97334

  Symptoms: After you reload the router, a glean adjacency is not resolved if the prefix is a tunnel destination.

  Conditions: This symptom is observed on a Cisco 7304 that has a tunnel configured when the destination is another tunnel.

  Workaround: Ping the tunnel interface of the destination to resolve the adjacency.

- CSCsc18999

  Symptoms: When you enter the **clear subscriber sessions all** command, the router reloads.

Conditions: This symptom is observed when Transparent Autologon (TAL) is used with ISG for control over DHCP addressing and when the router is using nearly all available CPU cycles and RAM.

Workaround: Do not you enter the **clear subscriber sessions all** command.

- CSCsc27712

  Symptoms: An ATM Permanent Virtual Path (PVP) goes down after a couple of minutes of non-activity.

  Conditions: This symptom is observed on a Cisco router when you enter the **atm pvp** command and leave the connection idle for a couple of minutes.

  Workaround: There is no workaround.

- CSCsc37472

  Symptoms: The output rate counters for a member link of a multilink interface do not increment when you look at the output of the **show interfaces** command.

  Conditions: This symptom is observed on a Cisco 10000 series when packets are properly delivered through the member link of the multilink interface.

  Workaround: Look at the PXF counters in the output of the **show pxf cpu queue multilink** *interface* or **show pxf cpu subblock multilink** *interface* commands.

- CSCsc48372

  Symptoms: The police function stops working when a PQ class map is removed and redefined for a policy map and when any class that is defined above the PQ class map is deleted. In this situation, all packets that match the PQ classes are marked as violated packets.

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

  Workaround: Remove the service policy and re-apply the service policy to the affected interfaces.

- CSCsc58937

  Symptoms: When you run the CISCO-FLASH-MIB, various traps are missing even though the operation is reported as successfully completed.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SNMP.

  Workaround: There is no workaround.

- CSCsc60444

  Symptoms: A “PXF DMA Toaster Stall Error” may occur, the microcode may unexpectedly be reloaded onto the PXF engine, and the reusable bandwidth may be incorrectly shaped.

  Conditions: These symptoms are observed on a Cisco 10000 series when a hierarchical policy map is attached to a Gigabit Ethernet interface and when the hierarchical policy map has a shaped rate that exceeds the link rate.

  Workaround: Do not attach a policy map that has a shaped rate that exceeds the link rate.

- CSCsc71353

  Symptoms: The **xconnect** command is not accepted.

  Conditions: This symptom is observed on a Cisco 7304 when you attempt to configure the **xconnect** command on an IMA port adapter that is configured for AAL0 encapsulation.

  Workaround: There is no workaround.

- CSCsc84834

  Symptoms: An adjacency is not established when a GRE tunnel is configured.

Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100.

Workaround: Ping the next hop through the GRE tunnel.

- CSCsc97102

  Symptoms: When you create or delete an PPPoX session, the address conversion from the RP to the eXternal Column Memory (XCM) is incorrect, as is shown by a traceback that is displayed on the console of the standby PRE.

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

  Workaround: There is no workaround.

- CSCsd00354

  Symptoms: The output of the **show policy-map interface** command shows the output queue packets and bytes counters as zero.

  Conditions: This symptom is observed on a Cisco 10000 series on queues for which a policer is applied.

  Workaround: Use the policer's counters in the output of the **show policy-map interface** command to determine the number of forwarded and dropped packets and bytes for the queue.

- CSCsd08662

  Symptoms: A Cisco 7200 series may crash when you apply a service policy with a priority action on a control plane.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

  Workaround: There is no workaround.

  Further Problem Description: A service policy with a priority action is not supported on a control plane. See the following Cisco document:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide0 9186a008052446b.html

- CSCsd14277

  Symptoms: A ping does not pass through a Fast Ethernet interface that functions in AToM port mode.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that has the **xconnect** interface configuration command enabled on the interface of a 1-port Fast Ethernet port adapter (PA-FE) that is installed in a port adapter carrier card (7300-CC-PA).

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

  Alternate Workaround: Enter the **shutdown** interface configuration command, the **xconnect** interface configuration command, and then the **no shutdown** interface configuration command on the affected interface.

- CSCsd25699

  Symptoms: MLP traffic fails during a PRE failover of the protect router.

  Conditions: This symptom is observed on a Cisco 10000 series when a PRE failover occurs on the protect router because of an MR-APS cable break failover from the protect router to the working router.

  Workaround: If the active controller is brought up after the MR-APS failover, manually reverse APS.

- CSCsd25713

  Symptoms: A Cisco 7304 crashes because of an address error (load or instruction fetch) exception when you remove a virtual template that is applied to at least one ATM subinterface by entering the **no interface virtual-template** command.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(27)SBC1 and may also occur in Release 12.2(28)SB.

  Workaround: Dot no apply a virtual template to an ATM interface.

- CSCsd38522

  Symptoms: Very high CPU usage may occur on a Cisco 10000 series when several thousand PPPoX PTA sessions are established and when the Port-Bundle Host Key (PBHK) feature is enabled. This situation can be observed in the output of the **show processes cpu** command.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured as an Intelligent Service Gateway (ISG) and that has the PBHK feature enabled with the default traffic class.

  Workaround: Apply an explicit traffic class to the port bundle, that is, apply an IP ACL that has the IP address of the Subscriber Edge Services Manager (SESM) as its destination IP address. Doing so reduces the CPU usage considerably.

- CSCsd39557

  Symptoms: Non-priority traffic is dropped, and priority traffic is sent at a very low rate.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when hierarchical shaping is configured on an ATM VC with a priority class in the next layer, as in the following example:

  ```
  policy-map atm-pri600 class From2_0 priority 150
  policy-map hiershape class class-default shape average 1000000 service-policy atm-pri600
  interface ATM4/0.401 point-to-point pvc 1/401 vbr-nrt 600 600 service-policy out hiershape
  ```

  Workaround: There is no workaround to prevent the symptom from occurring. You can restore the flow by first removing the policy from the interface and then by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCsd41107

  Symptoms: A Cisco 10000 series that functions as an LNS with a highly scaled configuration may reload unexpectedly.

  Conditions: This symptom is observed when the router runs very low on available processor memory. When this situation occurs, the following error messages are generated:

  ```
  GENERAL-2-CRITEVENT: Unable to malloc current_if_info C10K_BBA_SESSION-3-ERREVENT: No VCCI found for LNS session (26831)
  ```

  Workaround: Reduce or limit the number of L2TP tunnels and/or the number of PPP sessions that are being terminated on the LNS.

- CSCsd44475

  Symptoms: A ping may fail when packets pass from an MPLS VPN into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that functions as a PE router, and that is connect to the MPLS core via a serial interface.

  Possible Workaround: Do not use a serial interface to connect the PE router to the MPLS core. Rather, use another type of interface.

Further Problem Description: The symptom occurs because the tunnel adjacency is not complete in the PXF engine, preventing packets from being correctly punted and the adjacency from becoming complete.

- CSCsd49072

  Symptoms: The output of the **show policy-map interface** command shows incorrect statistics for a DSCP-based WRED policy. Also, when the class-map parameters are dynamically changed, the WRED statistics are lost.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsd51700

  Symptoms: A serial interface that is connected to an OSPP neighbor may flap during an SSO switchover, causing OSPF NSF to terminate during the switchover.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for NSF and occurs after multiple (10 or more) SSO switchovers.

  Workaround: There is no workaround.

- CSCsd52476

  Symptoms: Some members of a multilink interface may flap when you enter the **write memory** command on the PRE. Flapping occurs randomly each time the router reloads.

  Conditions: There symptoms are observed on a Cisco 10000 series that is configured for SSO, MR-APS, and MLP with Link Fragmentation Interleave (LFI).

  Workaround: There is no workaround.

- CSCsd57076

  Symptoms: A router crashes when you attach a service policy at the PVC level on an ATM interface.

  Conditions: This symptom is observed on a Cisco 7200 series when a bandwidth action is configured in the service policy and when traffic is passing through the interface.

  Workaround: There is no workaround.

- CSCsd64632

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

  3. Symptom 1: After one or two switchovers have occurred, SSH services become disabled because the RSA key is lost.

     Condition 1: This symptom is observed on a Cisco router that functions in either RPR+ or SSO mode.

     Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the lost settings via the console or a vty connection.

  4. Symptom 2: After one or two switchovers have occurred, the encrypted SNMP information or private setting becomes lost.

     Condition 1: This symptom is observed on a Cisco router that functions in RPR+ mode.

     Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the lost settings via the console or a vty connection.

- CSCsd87487

  Symptoms: Multilink interfaces remain down after an SSO switchover.

Conditions: This symptom is observed on a Cisco 10000 series that is configured for LFIoATM or MLPoATM and occurs only when traffic is flowing while an SSO switchover occurs. When there is no traffic, the interfaces come up normally.

Workaround: There is no workaround.

- CSCsd93555

  Symptoms: On a Cisco 7304 that has an NSE-100, it is possible to configure Link Fragmentation and Interleaving (LFI) over MLP and an egress QoS policy on a multilink interface. This is an inappropriate configuration because neither of these features can work effectively in the NSE-100 architecture.

  Conditions: This symptom is observed on a Cisco 7304 with an NSE-100. Note that LFI over MLP and an egress QoS policy on a multilink interface is an appropriate configuration on a Cisco 7304 with an NPE-G100 and works fine on a Cisco 7304 with an NPE-G100.

  Workaround: Disable LFI over MLP by entering the **no ppp multilink interleave** command. Disable QoS on a multilink interface by entering the **no service-policy output** *policy-map-name* command.

TCP/IP Host-Mode Services

- CSCek01499

  Symptoms: When a CE router that is configured for MPLS reloads, a software-forced crash may occur on the connected PE router because of memory corruption.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has two RPs that function in SSO mode. The symptom does not occur when the router has only a single RP.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCej58338

  Symptoms: A ping may fail across an ISDN BRI channel even though the ISDN B channel is up.

  Conditions: This symptom is observed on a Cisco router when routing protocols are enabled on the ISDN BRI channel.

  Workaround: Clear the BRI B channel.

- CSCek24091

  Symptoms: A PPP session fails to come up, and the following debug message is generated:

  ```
  PPP SSS: stale named authen method list "default"
  ```

  Conditions: This symptom is observed only when a service policy is applied and when the default PPP authentication method list is used.

  Workaround: Use a PPP authentication method list other than the PPP authentication default method list.

- CSCsb71154

  Symptoms: When a VC that is configured under a VP goes down, PPPoE sessions can still be established over the VC.

Conditions: This symptom is observed on a Cisco 10000 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface or after you have reloaded the router.

Workaround: There is no workaround.

- CSCsc28120

  Symptoms: A Cisco 7301 may crash when a service policy is removed from an interface that is configured for Frame Relay encapsulation.

  Conditions: This symptom is observed when a service policy is configured on an interface before the encapsulation is changed to Frame Relay. When the service policy is then removed, the router crashes.

  Workaround: Remove the service policy before you change the encapsulation to Frame Relay.

- CSCsd01322

  Symptoms: A PPP session is created with an IP address that is 0.0.0.0.

  Conditions: This symptom is observed on a Cisco router when a RADIUS profile uses the "ip:addr-pool" attribute to assign an IP address and when AAA authorization fails because there is no IP address available in the address pool.

  Workaround: Enter the **ppp ipcp address required** command to prevent a PPP session from being created with an IP address of 0.0.0.0.

- CSCsd06110

  Symptoms: A router may exhaust its I/O memory.

  Conditions: This symptom is observed on a Cisco router when you clear 10,000 tunnels on which about 45,000 PPP sessions are established. The symptom occurs only under extreme stress situations.

  Workaround: Clear the tunnels and sessions in stages.

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page*:

  http://www.cisco.com/warp/public/108/index.shtml

- *Troubleshooting Bus Error Exceptions*:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

- *Why Does My Router Lose Its Configuration During Reboot?*:

  http://www.cisco.com/warp/public/63/lose_config_6201.html

- *Troubleshooting Router Hangs*:

  http://www.cisco.com/warp/public/63/why_hang.html

- *Troubleshooting Memory Problems*:

  http://www.cisco.com/warp/public/63/mallocfail.shtml

- *Troubleshooting High CPU Utilization on Cisco Routers*:

  http://www.cisco.com/warp/public/63/highcpu.html

- *Troubleshooting Router Crashes*:

  http://www.cisco.com/warp/public/122/crashes_router_troubleshooting.shtml

- *Using CAR During DOS Attacks*:

  http://www.cisco.com/warp/public/63/car_rate_limit_icmp.html

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2SB. These documents consist of hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, feature modules, and other documents.

Documentation is available online on Cisco.com.

Use these release notes with the following resources:

- Release-Specific Documents, page 153
- Platform-Specific Documents, page 155
- Feature Modules, page 156
- Cisco Feature Navigator, page 156
- Cisco IOS Software Documentation Set, page 156

Release-Specific Documents

This section provides information about release-specific documents.

Cisco IOS Release 12.2SB

See the *Cisco IOS Release 12.2SB Documentation Roadmap* for detailed information about release-specific documents for Cisco IOS Release 12.2SB:

http://www.cisco.com/en/US/products/ps6566/products_documentation_roadmap09186a00806786c3.html

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 7304 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 7304 technical documentation on http://www.cisco.com/univercd/home/index.htm at

    Routers: **Cisco 7304**

- Cisco 10000 Series Routers
  - Cisco 10000 series home page on Cisco.com at

    Products & 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(28)SB

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

Cisco Feature Navigator

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

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

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

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command reference publications, and several other supporting documents.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

- Configuration guides on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Reference Guides**: **Configuration Guides**

- Command references on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Configure**: **Command References**

- Configuration guides and command references on http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Cisco IOS Release 12.2 Configuration Guides and Command References**

Cisco IOS Release 12.2 Documentation Set Contents

Table 13 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 13 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 13 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 13 Cisco IOS Release 12.2 Documentation Set (continued)

Modules	Major Topics
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • *New Features in Release 12.2 T* • *Release Notes* (Release note and caveat documentation for 12.2-based releases and various platforms)	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco.com. From Cisco.com, click the following path: **Support: Software Downloads: Network Management Software: Cisco Network Management Toolkit: Cisco MIBs**.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 153.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.