Release Notes for Cisco IOS Release 12.2(27)SBC

August 8, 2007

Cisco IOS Release 12.2(27)SBC5

OL-8093-01 Rev. Q0

These release notes support Cisco IOS Release 12.2SB up to and including Cisco IOS Release 12.2(27)SBC5. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and related documents.

Note Cisco IOS Release 12.2(27)SBC and its rebuilds support only the Cisco 7304. Release 12.2SB supports the Cisco 7304 and other platforms.

Note For information about the end-of-life milestones and dates and about product migration options for Cisco IOS Release 12.2(27)SBC, see the *End-of-Sale/End-of-Life Announcement for Cisco IOS Software Release 12.2(27)SB* product bulletin: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/prod_eol_notice0900aecd80481a49.html

Cisco IOS Release 12.2(27)SBC is tailored for service provider and large-scale enterprise networks. One of the main purposes of Release 12.2(27)SBC is 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 45 and the *Caveats for Cisco IOS Release 12.2* document. The caveats document is updated for every maintenance release and is located on Cisco.com.

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

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

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

Contents

Introduction

Cisco IOS Release 12.2SB is based on Cisco IOS Release 12.2 and Release 12.2S, up to and including Release 12.2(25)S3. All features that are supported for the Cisco 7304 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 16 and the "Caveats" section on page 45.

Early Deployment Releases

These release notes describe the Cisco 7304 router 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 7304

Cisco IOS ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(27)SBC5	No new software features.	No new hardware features.	06/22/2006
12.2(27)SBC4	No new software features.	No new hardware features.	04/24/2006
12.2(27)SBC3	No new software features.	No new hardware features.	03/16/2006
12.2(27)SBC2	No new software features.	No new hardware features.	01/26/2006
12.2(27)SBC1	No new software features.	No new hardware features.	10/31/2005

Table 1 Early Deployment Releases for the Cisco 7304 (continued)

Cisco IOS ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(27)SBC	See the "New Software Features in Cisco IOS Release 12.2(27)SBC" section on page 19.	See the "New Hardware Features in Cisco IOS Release 12.2(27)SBC" section on page 16.	09/12/2005
	See the "New Software Features Inherited from Cisco IOS Release 12.2S" section on page 21.	See the "New Hardware Features Inherited from Cisco IOS Release 12.2S" section on page 17.	

System Requirements

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

Memory Recommendations

The memory recommendation tables have not been included in the Cisco IOS Release 12.2SB release notes to improve the usability of the release notes documentation. The memory recommendations that were provided by these tables are available through Cisco Feature Navigator.

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

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

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

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

www.cisco.com/go/fn

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

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

Determining Memory Recommendations for Software Images (Feature Sets)

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

Step 1 From the Cisco Feature Navigator home page, click **Search by Software/Image Name/Product Code/Platform**.

Step 2 To find the memory recommendations for the latest Cisco IOS release, click the release under the Cisco IOS Quick Pick Latest Release area. For other releases, go to Step 3.

a. Choose **All Platforms** from the Platform drop-down list

b. Choose **All Feature Sets** from the Feature Set drop-down list.

The Search Results table will list all the software images (feature sets) that support the release that you chose, plus the DRAM and flash memory recommendations for each image.

Step 3 If the release is not listed in the Cisco IOS Quick Pick Latest Release area, choose **IOS** from the Software drop-down list, and click **Continue**.

a. Choose a release from the Major Release drop-down list, and click **Continue** again.

b. Choose a specific release from the Release drop-down list.

c. Choose **All Platforms** from the Platform drop-down list

d. Choose **All Feature Sets** from the Feature Set drop-down list.

The Search Results table will list all the software images (feature sets) that support the release that you chose, plus the DRAM and flash memory recommendations for each image.

Supported Hardware

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

Supported Platforms

Cisco IOS Release 12.2SB supports the following platform:

- Cisco 7304 router (with a Network Services Engine 100 [NSE-100] or Network Processing Engine G-100 [NPE-G100])

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 16.

For additional information about supported hardware for these platforms and this release, see the Hardware/Software Compatibility Matrix in the Cisco Software Advisor at the following location:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Supported Port Adapters for the Cisco 7304

Table 2 lists the port adapters that are supported for the Cisco 7304 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, (27) would mean that a port adapter was introduced in Cisco IOS Release 12.2(27)SBC. If a cell in this column contains an em dash (—), support for the port adapter was inherited from Cisco IOS Release 12.2, from Cisco IOS Release 12.2S, or from another release and was included in the initial base release of Cisco IOS Release 12.2SB.

Note Port adapters must be installed in the Port Adapter Carrier Card (7300-CC-PA) for the Cisco 7304. shared port adapters (SPAs) must be installed in the Modular Services Card 100 (7304-MSC-100) for the Cisco 7304.

Table 2 Supported Port Adapters for the Cisco 7304

Cisco Product Number[1]	Adapter Description	In	7304 Routers
ATM Port Adapters			
PA-A1-OC3SM	1-port ATM OC3 single mode (IR)	—	No
PA-A1-OC3MM	1-port ATM OC3 multimode	—	No
PA-A2-4T1C-OC3SM=	ATM CES, 4 T1 CES ports, 1 OC3 ATM SM port	—	No
PA-A2-4T1C-T3ATM=	ATM CES, 4 T1 CES ports, 1 T3 ATM port	—	No
PA-A2-4E1XC-OC3SM=	CES OC3, 4 E1 ports, 120 ohms	—	No
PA-A2-4E1XC-E3ATM=	CES E3/E1, 120 ohms	—	No
PA-A3-OC3MM	1-port ATM Enhanced OC3c/STM1 multimode	—	Yes
PA-A3-OC3SMI	1-port ATM Enhanced OC3c/STM1 single mode (IR)	—	Yes
PA-A3-OC3SML	1-port ATM Enhanced OC3c/STM1 single mode (LR)	—	Yes
PA-A3-OC12MM	1-port ATM Enhanced OC12/STM4 multimode	—	No
PA-A3-OC12SMI	1-port ATM Enhanced OC12/STM4 single mode (IR)	—	No
PA-A3-E3	1-port ATM Enhanced E3	—	Yes
PA-A3-T3	1-port ATM Enhanced DS3	—	Yes
PA-A3-8E1IMA	8-port ATM Inverse Mux E1, 120 ohms	—	Yes
PA-A3-8T1IMA	8-port ATM Inverse Mux T1	—	Yes
Channel Port Adapters			
PA-4C-E=	1-port Enhanced ESCON Channel	—	No
Dynamic Packet Transport (DPT) Port Adapters			
PA-SRP-OC12MM=	DPT-OC12 multimode	—	No
PA-SRP-OC12SMI=	DPT-OC12 single mode (IR)	—	No
PA-SRP-OC12SML=	DPT-OC12 single mode (LR)	—	No

Table 2 Supported Port Adapters for the Cisco 7304 (continued)

Cisco Product Number[1]	Adapter Description	In	7304 Routers
PA-SRP-OC12SMX=	DPT-OC12 single mode extended reach	—	No
SRPIP-OC12MM=	DPT-OC12 multimode	—	No
SRPIP-OC12SMI=	DPT-OC12 single mode (IR)	—	No
SRPIP-OC12SML=	DPT-OC12 single mode (LR)	—	No
SRPIP-OC12SMX=	DPT-OC12 single mode extended reach	—	No
Ethernet/Fast Ethernet/Gigabit Ethernet Port Adapters			
PA-4E	4-port Ethernet 10BASE-T	—	Yes
PA-4E1G/75	4-port E1 G.703 Serial, 75 ohms/unbalanced	—	Yes
PA-4E1G/120	4-port E1 G.703 Serial, 120 ohms/balanced	—	Yes
PA-5EFL	5-port Ethernet 10BASE-FL	—	No
PA-8E	8-port Ethernet 10BASE-T	—	Yes
PA-FE-FX	1-port Fast Ethernet 100BASE-FX	—	Yes
PA-FE-TX	1-port Fast Ethernet 100BASE-TX	—	Yes
PA-2FE-FX	2-port Fast Ethernet 100BASE-FX	—	Yes
PA-2FE-TX	2-port Fast Ethernet 100BASE-TX	—	Yes
PA-GE	1-port Gigabit Ethernet	—	Yes
FDDI Port Adapters			
PA-F/FD-MM	1-port FDDI Full Duplex multimode	—	No
PA-F/FD-SM	1-port FDDI Full Duplex single mode	—	No
High-Speed Serial Port Adapters			
PA-H	1-port High-Speed Serial Interface (HSSI)	—	Yes
PA-2H	2-port High-Speed Serial Interface (HSSI)	—	Yes
Multichannel Serial Port Adapters			
PA-MC-T3	1-port multichannel T3	—	Yes
PA-MC-E3	1-port multichannel E3	—	Yes
PA-MC-2T3+	2-port multichannel T3	—	Yes
PA-MC-2T1	2-port multichannel T1, integrated CSU/DSUs	—	Yes
PA-MC-2E1/120	2-port multichannel E1, G.703 120-ohm interface	—	Yes
PA-MC-4T1	4-port multichannel T1, integrated CSU/DSUs	—	Yes
PA-MC-8T1	8-port multichannel T1, integrated CSU/DSUs	—	Yes
PA-MC-8E1/120	8-port multichannel E1, G.703 120-ohm interface	—	Yes
PA-MC-8TE1+	8-port multichannel T1/E1 8PRI	—	Yes
PA-MC-STM-1MM	1-port multichannel STM-1 multimode	—	Yes
PA-MC-STM-1SMI	1-port multichannel STM-1 single mode	—	Yes
PA-4B-U	4-port BRI, U Interface	—	No
PA-8B-S/T	8-port BRI, S/T Interface	—	No

Table 2 Supported Port Adapters for the Cisco 7304 (continued)

Cisco Product Number[1]	Adapter Description	In	7304 Routers
Service Adapters			
SA-ENCRYPT=	Encryption Service Adapter	—	No
SA-ISA	Integrated Services Adapter for IPSec or MPPE encryption	—	No
Shared Port Adapters (SPAs)			
SPA-4FE-7304	4-port 10/100 Fast Ethernet SPA	—	Yes
SPA-2GE-7304	2-port 10/100/1000 Gigabit Ethernet SPA	—	Yes
SPA-2XOC3-POS	2-port OC-3c/STM-1 POS SPA	—	Yes
SPA-4XOC3-POS	4-port OC-3c/STM-1 POS SPA	—	Yes
SPA-1OC12-POS	1-port OC-12c/STM-4 POS SPA	—	Yes
SPA-2XT3/E3	2-port T3/E3 Serial SPA	—	Yes
SPA-4XT3/E3	4-port T3/E3 Serial SPA	—	Yes
SONET Port Adapters			
PA-POS-OC3MM	1-port Packet over SONET OC3c/STM1 multimode	—	Yes
PA-POS-OC3SMI	1-port Packet over SONET OC3c/STM1 single mode (IR)	—	Yes
PA-POS-OC3SML	1-port Packet over SONET OC3c/STM1 single mode (LR)	—	Yes
PA-POS-2OC3	2-port OC-3/STM-1 POS with APS	(18)	Yes
T1/E1 Port Adapters			
PA-4T+	4-port Serial, Enhanced	—	Yes
PA-8T-V35	8-port Serial, V.35	—	Yes
PA-8T-X21	8-port Serial, X.21	—	Yes
PA-8T-232	8-port Serial, 232	—	Yes
T3/E3 Port Adapters			
PA-T3	1-port T3 Serial, T3 DSUs	—	Yes
PA-T3+	1-port T3 Serial, Enhanced	—	Yes
PA-2T3	2-port T3 Serial, T3 DSUs	—	Yes
PA-2T3+	2-port T3 Serial, Enhanced	—	Yes
PA-E3	1-port E3 Serial, E3 DSUs	—	Yes
PA-2E3	2-port E3 Serial, E3 DSUs	—	Yes
Token Ring Port Adapters			
PA-4R-DTR	4-port Dedicated Token Ring, 4/16Mbps, HDX/FDX	—	No
Voice Port Adapters			
PA-MCX-2TE1=	2-port MIX-enabled multichannel T1/E1, CSU/DSU	—	No
PA-MCX-4TE1=	4-port MIX-enabled multichannel T1/E1, CSU/DSU	—	No

Table 2 Supported Port Adapters for the Cisco 7304 (continued)

Cisco Product Number[1]	Adapter Description	In	7304 Routers
PA-MCX-8TE1-M=	8-port multichannel T1/E1, Signaling System 7 over IP (SS7oIP)	—	No
PA-MCX-8TE1=	8-port MIX-enabled multichannel T1/E1, CSU/DSU	—	No
PA-VXA-1TE1-24+	1-port T1/E1 Digital Voice, 24 Channels	—	No
PA-VXA-1TE1-30+	1-port T1/E1 Digital Voice, 30 Channels	—	No
PA-VXB-2TE1+	2-port T1/E1 moderate capacity, Enhanced	—	No
PA-VXC-2TE1+	2-port T1/E1 high capacity, Enhanced	—	No

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

For more information about the Cisco 7304 router port adapters, see the Cisco documents at the following location:

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

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

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

Supported Line Cards for the Cisco 7304

Table 3 lists the line cards that are supported for the Cisco 7304 router in Cisco IOS Release 12.2SB.

The number in the "In" column indicates the Cisco IOS 12.2SB release in which the line card was introduced. For example, (27) would mean that a line card was introduced in Cisco IOS Release 12.2(27)SBC. If a cell in this column contains an em dash (—), support for the line card was inherited from Cisco IOS Release 12.2, from Cisco IOS Release 12.2(25)S3, or from another release and was included in the initial base release of Cisco IOS Release 12.2SB.

Table 3 Supported Line Cards for the Cisco 7304

Common Abbreviation	Cisco Product Number[1]	Line Card Description	In
ATM Line Cards			
2-Port OC-3 ATM	7300-2OC3ATM-MM	2-port OC-3 ATM line card, multimode	—
	7300-2OC3ATM-SMI	2-port OC-3 ATM line card, single-mode, intermediate reach	—
	7300-2OC3ATM-SML	2-port OC-3 ATM line card, single-mode, long reach[2]	—
1-Port OC-12 ATM	7300-1OC12ATM	1-port OC-12 ATM line card (requires SPF modules)	—
Clear Channel E3 and T3 Line Cards			
6-Port E3	7300-6E3	Clear Channel 6-port E3 line card	—
6-Port T3	7300-6T3	Clear Channel 6-port T3 line card	—

Table 3 Supported Line Cards for the Cisco 7304 (continued)

Common Abbreviation	Cisco Product Number[1]	Line Card Description	In
Packet over SONET (POS) Line Cards			
2-Port OC-3 POS	7300-2OC3POS-MM	2-port OC-3 POS line card, multimode	—
	7300-2OC3POS-SMI	2-port OC-3 POS line card, single-mode, intermediate reach	—
	7300-2OC3POS-SML	2-port OC-3 POS line card, single-mode, long reach[2]	—
4-Port OC-3 POS	7300-4OC3POS-MM	4-port OC-3 POS line card, multimode[2]	—
	7300-4OC3POS-SMI	4-port OC-3 POS line card, single-mode, intermediate reach	—
	7300-4OC3POS-SML	4-port OC-3 POS line card, single-mode, long reach[2]	—
1-Port OC-12 POS	7300-1OC12POS-MM	1-port OC-12 POS line card, multimode[2]	—
	7300-1OC12POS-SMI	1-port OC-12 POS line card, single-mode, intermediate reach	—
	7300-1OC12POS-SML	1-port OC-12 POS line card, single-mode, long reach[2]	—
2-Port OC-12 POS	7300-2OC12POS-MM	2-port OC-12 POS line card, multimode[2]	—
	7300-2OC12POS-SMI	2-port OC-12 POS line card, single-mode, intermediate reach	—
	7300-2OC12POS-SML	2-port OC-12 POS line card, single-mode, long reach[2]	—
1-Port OC-48 POS	7300-1OC48POS-SMS	1-port OC-48 POS line card, single-mode, short reach	—
	7300-1OC48POS-SMI	1-port OC-48 POS line card, single-mode, intermediate reach	—
	7300-1OC48POS-SML	1-port OC-48 POS line card, single-mode, long reach[2]	—

1. For a spare product number, append an equal sign (=) to the product number. For End-of-Sale (EoS) and End-of-Life (EoL) information about line cards, see the Cisco product bulletins at the following location: http://www.cisco.com/en/US/products/hw/routers/ps133/prod_eol_notices_list.html
2. This product has reached End of Sales (EoS) but is still supported.

For more information about the Cisco 7304 router line cards, see the Cisco documents at the following location:

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

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) 7300 Software (c7300-p-mz), Version 12.2(27)SBC, 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* document:

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

For information about upgrading the Cisco 7304 router, see the following document:

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

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

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

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

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

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

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

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

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

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

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 13

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(27)SBC5

There are no new FPGA images for Cisco IOS Release 12.2(27)SBC5. All Cisco IOS Release 12.2(27)SBC5 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(27)SBC3.

Bundled FPGAs for Cisco IOS Release 12.2(27)SBC4

There are no new FPGA images for Cisco IOS Release 12.2(27)SBC4. All Cisco IOS Release 12.2(27)SBC4 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(27)SBC3.

Bundled FPGAs for Cisco IOS Release 12.2(27)SBC3

All Cisco IOS Release 12.2(27)SBC3 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 4.

Table 4 Bundled FPGA Versions for Cisco IOS Release 12.2(27)SBC3

FPGA Image	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
6E3 line card FPGA	0.21	2.00	12
6T3 line card FPGA	0.21	2.00	12
MSC-100 FPGA	0.27	0.10	22
NPE-G100 FPGA	2.05	0.30	12
NSE-100 Motherboard FPGA	1.14	2.00 or 4.00	15
	1.14	5.00	15
NSE-100 Daughterboard FPGA	1.14	0.00	6
	1.14	5.00	6
OC-3 ATM line card FPGA	0.19	2.00	8
OC-12 ATM line card FPGA	0.19	2.00	8
OC-3 POS line card FPGA	0.22	2.00	8
OC-12 POS line card FPGA	0.20	1.00	12
OC-48 POS line card FPGA	0.16	2.00	5
PACC line card FPGA	1.40	1.01	8

Bundled FPGAs for Cisco IOS Release 12.2(27)SBC2

All Cisco IOS Release 12.2(27)SBC2 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(27)SBC2

FPGA Image	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
6E3 line card FPGA	0.21	2.00	12
6T3 line card FPGA	0.21	2.00	12

Table 5 Bundled FPGA Versions for Cisco IOS Release 12.2(27)SBC2 (continued)

FPGA Image	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
MSC-100 FPGA	0.27	0.10	22
NPE-G100 FPGA	2.05	0.30	12
NSE-100 Motherboard FPGA	1.07	2.00 or 4.00	15
	1.08	5.00	15
NSE-100 Daughterboard FPGA	1.07	0.00	6
	1.08	5.00	6
OC-3 ATM line card FPGA	0.19	2.00	8
OC-12 ATM line card FPGA	0.19	2.00	8
OC-3 POS line card FPGA	0.22	2.00	8
OC-12 POS line card FPGA	0.20	1.00	12
OC-48 POS line card FPGA	0.16	2.00	5
PACC line card FPGA	1.40	1.01	8

Bundled FPGAs for Cisco IOS Release 12.2(27)SBC1

There are no new FPGA images for Cisco IOS Release 12.2(27)SBC1. All Cisco IOS Release 12.2(27)SBC1 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(27)SBC.

Bundled FPGAs for Cisco IOS Release 12.2(27)SBC

All Cisco IOS Release 12.2(27)SBC software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 6.

Table 6 Bundled FPGA Versions for Cisco IOS Release 12.2(27)SBC

FPGA Image	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
6E3 line card FPGA	0.21	2.00	12
6T3 line card FPGA	0.21	2.00	12
MSC-100 FPGA	0.27	0.10	22
NPE-G100 FPGA	2.05	0.30	12
NSE-100 Motherboard FPGA	1.07	2.00 or 4.00	15
	1.08	5.00	15
NSE-100 Daughterboard FPGA	1.07	0.00	6
	1.08	5.00	6
OC-3 ATM line card FPGA	0.19	2.00	8
OC-12 ATM line card FPGA	0.19	2.00	8
OC-3 POS line card FPGA	0.22	2.00	8
OC-12 POS line card FPGA	0.20	1.00	12

Table 6 Bundled FPGA Versions for Cisco IOS Release 12.2(27)SBC (continued)

FPGA Image	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
OC-48 POS line card FPGA	0.16	2.00	5
PACC line card FPGA	1.30	1.01	8

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(27)SBC5

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(27)SBC5 is the c7304-fpd-pkg.122-27.SBC5.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(27)SBC.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(27)SBC4

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(27)SBC4 is the c7304-fpd-pkg.122-27.SBC4.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(27)SBC.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(27)SBC3

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(27)SBC3 is the c7304-fpd-pkg.122-27.SBC3.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(27)SBC.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(27)SBC2

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(27)SBC2 is the c7304-fpd-pkg.122-27.SBC2.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(27)SBC.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(27)SBC1

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(27)SBC1 is the c7304-fpd-pkg.122-27.SBC1.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(27)SBC.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(27)SBC

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(27)SBC is the c7304-fpd-pkg.122-27.SBC.pkg file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image from the Software Center on Cisco.com.

Table 7 Release 12.2(27)SBC FPD Image Package Contents

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

Feature Support

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

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

The feature set tables have been removed from the Cisco IOS Release 12.2SB release notes to improve the usability of the release notes documentation. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 3 Click **Continue**.

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

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

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

New and Changed Information

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

Note A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL: http://tools.cisco.com/RPF/register/register.do.

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

There are no new hardware features in Cisco IOS Release 12.2(27)SBC.

New Hardware Features Inherited from Cisco IOS Release 12.2S

This section describes the new hardware features that were introduced in Cisco IOS Release 12.2S and that Release 12.2(27)SBC inherits from Release 12.2S. 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.

Line Cards

For information about all supported Cisco 7304 router line cards, see Table 3 on page 8 and the Cisco documents at the following location:

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

Cisco IOS Release 12.2(27)SBC inherited support from Cisco IOS Release 12.2S for the following line cards for the Cisco 7304.

1 Port OC-12 ATM Line Card (7300-1OC12ATM)

This release supports the 1-port OC-12 ATM line card (7300-1OC12ATM) for the Cisco 7304 router. For detailed information about this feature, see the Cisco documents at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/linecard/ol_6876/index.htm

Modular Services Card 100

The Modular Services Card 100 (MSC-100) enables support for Cisco shared port adapters (SPAs) on the Cisco 7304. The MSC-100 is a jacket card that is designed to accept two supported half-height SPAs in one line card slot of the Cisco 7304 chassis. For additional information on the MSC-100, see the following documents:

- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Hardware Installation Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspahw/index.htm
- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Installation Guide*

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

Cisco 7304 Port Adapters

The Cisco 7304 supports Cisco 7000 series port adapters (that is, regular non-SPA port adapters) in conjunction with the 7300-CC-PA carrier card. For information about the supported port adapters, see Table 2 on page 5 and see the Cisco documents at the following location:

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

Cisco 7304 Shared Port Adapters

The Cisco 7304 supports shared port adapters (SPAs) in conjunction with the Modular Services Card 100 (7304-MSC-100). For information about the supported port adapters, see Table 2 on page 5 and see the Cisco documents at the following location:

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

Cisco IOS Release 12.2(27)SBC inherited support from Cisco IOS Release 12.2S for the following SPAs, for the Cisco 7304.

1-Port OC-12c/STM-4 POS SPA Shared Port Adapter (SPA-1OC12-POS)

This release supports the 1-port OC-12c/STM-4 POS SPA (SPA-1OC12-POS) shared port adapter for the Cisco 7304 router. For detailed information about this feature, see the following Cisco documents:

- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Hardware Installation Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspahw/index.htm
- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Installation Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspasw/index.htm

2-Port and 4-Port OC-3 POS SPA Shared Port Adapter (SPA-2XOC3-POS and SPA-4XOC3-POS)

This release supports the 2-port and 4-port OC-3 POS shared port adapters (SPA-2XOC3-POS and SPA-4XOC3-POS) for the Cisco 7304 router. For detailed information about this feature, see the following Cisco documents:

- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Hardware Installation Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspahw/index.htm
- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Installation Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspasw/index.htm

2-Port and 4-Port T3/E3 Serial SPA Shared Port Adapter (SPA-2XT3/E3 and SPA-4XT3/E3)

This release supports the 2-port and 4-port T3/E3 serial SPA shared port adapters (SPA-2XT3/E3 and SPA-4XT3/E3) for the Cisco 7304 router. For detailed information about this feature, see the following Cisco documents:

- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Hardware Installation Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspahw/index.htm
- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Installation Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspasw/index.htm

4-Port 10/100 Fast Ethernet Shared Port Adapter

The 4-port 10/100 Fast Ethernet shared port adapter (7304-4FE-SPA) provides four 10/100 Fast Ethernet ports for the Cisco 7304. SPAs are half-height interface line cards that provide additional physical interfaces to the Cisco 7304 when inserted into Modular Services Cards (MSCs), assuming that the SPA is supported by the MSC. MSCs are jacket cards in which multiple SPAs can be inserted. An MSC fits into a line card slot.

For additional information on the 4-port 10/100 Fast Ethernet shared port adapter for the Cisco 7304, see the following documents:

- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Hardware Installation Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspahw/index.htm
- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Installation Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/73mscspa/mscspasw/index.htm

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

This section describes new and changed features in Cisco IOS Release 12.2(27)SBC. Some features may be new to Cisco IOS Release 12.2SB but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.2(27)SBC. 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 lists the features that are new in Cisco IOS Release 12.2SB 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 8 New 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 Command and Debug Command Enhancements	Yes	Yes	No
IP SLAs LSP Health Monitor	Yes	Yes	No
MPLS-VPN eiBGP Multi-path Loadbalancing Enhancements	Yes	Yes	Yes
MPLS VPN VRF-Select for PXF	Yes	Not applicable[1]	Yes
Multiple Action Policer for PXF	Yes	Not applicable[1]	Yes
Three-level Hierarchical Policy Support in PXF	Yes	Not applicable[1]	Yes
Turbo Access Control List Scalability Enhancements	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.

Frame Relay Show Command and Debug Command Enhancements

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

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

IP SLAs LSP Health Monitor

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

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

MPLS-VPN eiBGP Multi-path Loadbalancing Enhancements

In this Cisco IOS release, the MPLS-VPN eiBGP Multi-path 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 VRF-Select for PXF

VRF-Select for PXF was available on the Cisco 7304 router until Cisco IOS Release 12.2(20)S. This feature restores support for VRF-Select in the PXF processing path.

For information about MPLS VPN VRF-Select, see the following Cisco document:

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

Multiple Action Policer for PXF

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

Three-level Hierarchical Policy Support in PXF

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

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 requires 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 much larger ACL tables.

This is a functional enhancement that introduces no new configuration.

Warm Reload

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

New Software Features Inherited from Cisco IOS Release 12.2S

This section describes the new software features that were introduced in Cisco IOS Release 12.2S and that Release 12.2(27)SBC inherits from Release 12.2S. 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.

Access Control Lists

Cisco IOS Release 12.2(27)SBC supports the following access control list (ACL) features.

ACL IP Options Selective Drop

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/sel_drop.htm

ACL—Named ACL Support for Noncontiguous Ports on an Access Control Entry

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

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

ACL Performance Enhancement

An IP access control list (ACL) is a Cisco IOS software feature that allows an administrator to configure a network to permit and deny packets based on a set of ACL entries, thus improving security and control within a network. These lists contain entries that are searched sequentially for matches among certain fields in Layer 3 and Layer 4 packet headers.

In older Cisco IOS software releases, ACL entries were sequentially configured and stored. This implementation caused the first match in a search to be the first ACL entry in a given list, not the entry that provided the best match. Although this implementation was straightforward and logical, it did not scale well with the number of ACL entries in an ACL.

Release 12.2(27)SBC implements ACLs using hierarchical radix tries (sometimes called multilevel tries, backtracking tries, or tries-of-tries) to improve matching performance. Individual tries are made for the source prefix and the destination prefix, with additional ACL entry information such as TCP ports, TCP flags, and time ranges being held at the nodes. Cisco IOS software performs a best match lookup for the given set of prefixes. This new implementation is an internal improvement that supports all existing functionality, and the sequential searching properties that cause ACLs to check the entries from start to end and stop searching for a match as soon as one is found are still valid.

The benefits of this implementation of ACLs using hierarchical radix tries are as follows:

- Memory usage is made more efficient.
- Less system resources are required to maintain the tries information.
- Performance of ACL matching is improved for larger access lists.

ACL TCP Flags Filtering

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

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

Any Transport over MPLS for PXF

The Any Transport over MPLS for PXF feature that was previously introduced in Cisco IOS Release 12.2S is also available in Cisco IOS Release 12.2SBC starting in Cisco IOS Release 12.2(27)SBC.

Any Transport over MPLS (AToM) transports Layer 2 packets over a Multiprotocol Label Switching (MPLS) backbone. AToM enables service providers to connect customer sites with existing data link layer (Layer 2) networks, by using a single, integrated, packet-based network infrastructure— a Cisco MPLS network. Instead of separate networks with network management environments, service providers can deliver Layer 2 connections over an MPLS backbone. AToM provides a common framework to encapsulate and transport supported Layer 2 traffic types over an MPLS network core.

The AToM for PXF features introduces AToM in the PXF-processing path for the Cisco 7304 router.

IP and Ethernet interworkings are supported in PXF as part of this feature.

The following AToM transport modes are now supported on line card, port adapter, shared port adapter, and the native Gigabit Ethernet interface on the Cisco 7304 processor:

- ATM AAL5 over MPLS
- Ethernet Port over MPLS
- Frame Relay over MPLS

- HDLC over MPLS
- PPP over MPLS
- VLAN over MPLS

The following modes are supported on the PA-A3-OC3 only:

- ATM Single Cell Relay over MPLS
- ATM single cell relay: VC mode
- ATM single cell relay: VP mode
- ATM single cell relay: Port mode
- ATM packed cell relay: VP and VC modes

For general information on AToM (non-PXF and across platforms), see the *Any Transport over ATM* document:

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

For additional information on this feature, see the *Cisco 7304 Troubleshooting and Configuration Notes* document:

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

ARP Optimization

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/arpoptim.htm

ATM

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

ATM Conditional Debug Support

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 PVC Trap Enhancements for Segment and End AIS/RDI Failures

When an ATM permanent virtual circuit (PVC) cannot be used to transmit data because of a connectivity failure, it may be placed in a down state. To detect a connectivity failure, various types of Operation, Administration, and Maintenance (OAM) cells can be used. The operator can inform the network management system (NMS) about OAM failures using ATM PVC trap notifications. Depending on the PVC trap notification that is enabled, the PVC state can be kept up or can brought down. The various ATM PVC trap notifications supported for different types of PVC connectivity failure detection mechanisms are as follows:

- ATM PVC down trap
- ATM PVC F5 loopback failure trap
- ATM PVC F5 segment continuity check (CC) failure trap

- ATM PVC F5 end-to-end CC failure trap
- ATM PVC F5 alarm indication signal/remote defect indication (AIS/RDI) failure trap

When connectivity is restored and the PVC is in a down state, it is changed to an up state and data transfer is allowed to occur over the PVC. This restoration of connectivity can be detected using OAM cells, and the following recovery trap notifications can be used to inform the NMS:

- ATM PVC up trap
- ATM PVC F5 loopback recovery trap
- ATM PVC F5 segment CC recovery trap
- ATM PVC F5 end-to-end CC recovery trap
- ATM PVC F5 AIS/RDI recovery trap

If the traps in these lists were sent for each PVC failure and recovery, they would generate much traffic for the NMS. To reduce this traffic, at most one trap of each type could be generated in each notification interval. However, because there can be multiple PVCs, each of which can have multiple failures and recoveries, the trap may contain multiple PVCs. To reduce the size of the trap packet, successive PVCs that have the same failures or recoveries are expressed by means of ranges.

In the F5 AIS/RDI failure and recovery traps listed above, separate segment and end AIS/RDI traps are not implemented. The ATM PVC Trap Enhancements for Segment and End AIS/RDI Failures feature introduced in Cisco IOS Release 12.2(25)S allows the generation of separate ATM F5 segment and end AIS/RDI failure and recovery trap notifications. This enhancement also adds the ifDescr object to the traps.

See the *ATM OAM Support for F5 Continuity Check* document for information about enabling ATM OAM F5 support:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/24soamcc.htm

BGP

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

BGP CLI Troubleshooting Commands

For detailed information about this feature (which is also known as the BGP Standard Usage of CLI Troubleshooting Commands feature), see the *Implementing Multiprotocol BGP for IPv6* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_bgpv6.htm

BGP Configuration Using Peer Templates

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

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

BGP Convergence Optimization

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

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

BGP Cost Community

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

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

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

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

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

BGP Dynamic Update Peer-Groups

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

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

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

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

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

BGP MIB Support Enhancements

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

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

BGP Restart Session After Max-Prefix Limit

For detailed information about this feature (which is also known as the BGP Restart Neighbor Session After max-prefix Limit Reached feature), see the following Cisco document:

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

BGP Route-Map Continue

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

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

BGP Route-Map Policy List Support

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

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

BGP Support for Dual AS Configuration for Network AS Migrations

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

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

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

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

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

BGP Support for Named Extended Community Lists

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

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

BGP Support for Sequenced Entries in Extended Community Lists

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

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

BGP Support for TTL Security Check

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

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

Cisco IOS Login Enhancements

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_login.htm

CLNS Support for GRE Tunneling of IPv4 and IPv6 Packets in CLNS Networks

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/gtclnsv6.htm

Configuration Change Notification and Logging

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/gtconlog.htm

Configuration Generation Performance Enhancement

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/gtinvgen.htm

Configuration Replace and Configuration Rollback

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

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

Contextual Configuration Diff Utility

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

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

Control Plane Policing (CPP)

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/gtrtlimt.htm

Enhanced Management of the Cisco 7304 Router, Phase 1

The Enhanced Management of the Cisco 7304 Router, Phase 1 feature enables you to:

- Manage and monitor Cisco 7304 resources through a Simple Network Management Protocol (SNMP)-based network management system (NMS).
- Use **set** and **get** SNMP commands to access information in Cisco 7304 router MIBs.
- Reduce the amount of time and system resources required to perform functions like inventory management and bulk data transfers.

Other benefits include the following:

- A standards-based technology (that is, SNMP) for monitoring faults and performance on the router.
- Support for all SNMP versions (SNMPv1, SNMPv2c, and SNMPv3).
- Notification of faults, alarms, and conditions that might affect services.
- The ability to aggregate fault and alarm information for multiple entities.
- A way to access router information other than through the command-line interface (CLI).

Supported Cisco 7304 Modules

The following Cisco 7304 network processing engines, line cards, and port adapters are supported:

- Network Services Engine 100 (NSE-100)
- Network Processing Engine G-100 (NPE-G100)
- 1-port OC-12 POS and 2-port OC-12 POS line cards (7300-1OC12POS-MM, 7300-1OC12POS-SMI, 7300-1OC12POS-SML, 7300-2OC12POS-MM, 7300-2OC12POS-SMI, 7300-2OC12POS-SML)
- 1-port OC-48 POS line card (7300-1OC48POS-SMS, 7300-1OC48POS-SMI, 7300-1OC48POS-SML)
- 2-port OC-3 ATM line card (7300-2OC3ATM-MM, 7300-2OC3ATM-SMI, 7300-2OC3ATM-SML)
- 2-port OC-3 POS and 4-port OC-3 POS line cards (7300-2OC3POS-MM, 7300-2OC3POS-SMI, 7300-2OC3POS-SML, 7300-4OC3POS-MM, 7300-4OC3POS-SMI, 7300-4OC3POS-SML)
- Clear Channel 6-port E3 line card (7300-6E3)
- Clear Channel 6-port T3 (DS3) line card (7300-6T3)
- Port Adapter Carrier Card (7300-CC-PA)
- 1-port ATM Enhanced E3 port adapter (PA-A3-E3)

- 1-port ATM Enhanced DS3 port adapter (PA-A3-T3)
- 2-port Fast Ethernet 100BASE-FX port adapter (PA-2FE-FX)
- 2-port Fast Ethernet 100BASE-FX port adapter (PA-2FE-TX)

Cisco 7304 MIB Enhancements

In Cisco IOS Release 12.2S, the Cisco 7304 supports the following MIBs:

- CISCO-ENTITY-ALARM-MIB—Foundation Fault Management
- CISCO-ENTITY-ASSET-MIB—Inventory and Asset Management
- CISCO-ENTITY-FRU-CONTROL-MIB—Foundation Fault Management
- CISCO-ENTITY-PFE-MIB—Performance Management
- CISCO-ENTITY-SENSOR-MIB—Foundation Fault Management
- CISCO-ENTITY-VENDORTYPE-OID-MIB—Inventory and Asset Management
- CISCO-ENTITY-EXT-MIB—Inventory and Asset Management
- ENTITY-MIB (RFC 2037)—Inventory and Asset Management
- NOTIFICATION-LOG-MIB (RFC 3014)—Core fault management

Further Information

For further information about the Enhanced Management of the Cisco 7304 Router, Phase 1 feature, see the *Cisco 7304 Router MIB Specifications Guide*:

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

Extended ACL Support for IGMP to Support SSM in IPv4

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/gtmcxacl.htm

FHRP

Cisco IOS Release 12.2(27)SBC supports the following First-Hop Redundancy Protocol (FHRP) features.

FHRP - Enhanced Object Tracking of IP SLAs Operations

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

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

FHRP - SSO Aware HSRP

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/fshsrpss.htm

GLBP MD5 Authentication

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/gtglbpau.htm

Integrated IS-IS Global Default Metric

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

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

Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

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

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

IP SLAs MPLS VPN Aware

The IP SLAs MPLS VPN Aware feature is supported on the Network Services Engine 100 (NSE-100) and the Network Processing Engine G-100 (NPE-G100) on the Cisco 7304 router. The feature is not supported in the Parallel Express Forwarding (PXF) processing path on the Cisco 7304 router. For detailed information about this feature, see the following Cisco document:

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

IP SLAs Multi-Operation Scheduler

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

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

IPv6

Cisco IOS Release 12.2(27)SBC supports the following IP version 6 (IPv6) and IPv6-related features.

Distributed MFIB for Multicast v6

For information about this feature, see the "Distributed MFIB" section in the *Implementing IPv6 Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm#wp1208669

IPv6: Anycast Address

For information about this feature, see the "IPv6 Address Type: Anycast" section in the *Implementing Basic Connectivity for IPv6* document:

https://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con_ps6922_TSD_Products_Configuration_Guide_Chapter.html

IPv6 Multicast

For detailed information about this feature, see the *Implementing IPv6 Multicast* document:

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

The *Cisco IOS IPv6 Configuration Library* is available at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm

IPv6 Multicast: Address Family Support for Multiprotocol BGP

For information about this feature, see the "Multiprotocol BGP for the IPv6 Multicast Address Family" section in the *Implementing IPv6 Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm#wp1208447

IPv6 Multicast: Multicast Listener Discovery (MLD) Protocol

For detailed information about this feature, see the "Information About IPv6 Multicast" section in the *Implementing IPv6 Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm#wp1289312

IPv6 Multicast: PIM Source-Specific Multicast (PIM-SSM)

For detailed information about this feature, see the "Information About IPv6 Multicast" section in the *Implementing IPv6 Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm#wp1289312

IPv6 Multicast: PIM Sparse Mode (PIM-SM)

For detailed information about this feature, see the "Information About IPv6 Multicast" section in the *Implementing IPv6 Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm#wp1289312

IPv6 Multicast: Scope Boundaries

For detailed information about this feature, see the "Information About IPv6 Multicast" section in the *Implementing IPv6 Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm#wp1289312

IPv6 Routing: IS-IS Multitopology Support for IPv6

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_isis6.htm

IPv6 Routing: OSPF for IPv6 (OSPFv3)

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_ospf3.htm

IS-IS

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

IS-IS Caching of Redistributed Routes

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

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

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

For detailed information about this feature (which is also known as the IS-IS Incremental SPF feature), see the following Cisco document:

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

IS-IS Limit on Number of Redistributed Routes

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

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

IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements

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/fsisiadv.htm

IS-IS Support for a Redistribution Limit of Maximum Prefixes Imported

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

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

IS-IS Support for IP Route Tags

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/gtisitag.htm

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

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

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

Layer 2 Local Switching

The following Layer 2 Local Switching features are supported:

- Layer 2 Local Switching - ATM to ATM
- Layer 2 Local Switching - ATM to Ethernet
- Layer 2 Local switching - ATM-FR

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

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

Layer 2 Tunnel Protocol Version 3

The Layer 2 Tunnel Protocol Version 3 (L2TPv3) feature and the following L2TPv3-related features are supported on both the Cisco 7304 NPE-G100 and the Cisco 7304 NSE-100:

- ATM AAL5 OAM Emulation over L2TPv3
- ATM Port Mode Cell Relay over L2TPv3
- ATM Single Cell Relay VC Mode over L2TPv3
- ATM VP Mode Single Cell Relay over L2TPv3
- L2TPv3 Control Message Hashing
- L2TPv3 Control Message Rate Limiting
- L2TPv3 Layer 2 Fragmentation
- Layer 2 VPN (L2VPN): Syslog, SNMP Trap, and show Command Enhancements for AToM and L2TPv3

Support for the following L2TPv3-related features was added on the Cisco 7304 NPE-G100 only:

- L2TPv3 Distributed Sequencing
- Protocol Demultiplexing for L2TPv3

For detailed information about these features, 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 Tunneling Protocol v3 for PXF on the Cisco 7304 NSE-100

The Layer 2 Tunneling Protocol v3 for PXF on the Cisco 7304 NSE-100 feature that was previously introduced in Cisco IOS Release 12.2S is also available in Cisco IOS Release 12.2SBC starting in Cisco IOS Release 12.2(27)SBC.

L2TPv3 is an Internet Engineering Task Force (IETF) l2tpext working group draft that provides several enhancements to L2TP for the capability to tunnel any Layer 2 payload over L2TP. Specifically, L2TPv3 defines the L2TP protocol for tunneling Layer 2 payloads over an IP core network using Layer 2 Virtual Private Networks (VPNs).

L2TP has two fundamental parts:

- A control plane responsible for setting up the connection
- A data plane responsible for tunneling Layer 2 frames

L2TPv3 signaling is responsible for negotiating control plane parameters, session IDs, and cookies; for performing authentication; and for exchanging configuration parameters. L2TPv3 is also used to reliably deliver hello messages and circuit status messages. These messages are critical to support circuit interworking, such as the Local Management Interface (LMI), and to monitor the remote circuit status.

This feature introduces L2TPv3 in the PXF processing path for Cisco 7304 routers using an NSE-100 (this feature is already available for the NPE-G100). Specifically, the following is supported for L2TPv3 in the PXF processing path:

- L2 Media
  - Ethernet Port mode
  - Ethernet 802.1q VLAN
  - PPP
  - HDLC
  - Frame Relay
  - AAL5/OAM
  - VP Single Cell relay
  - VC Single Cell relay
- Interworking Types
  - Ethernet (bridged)
  - IP (routed)
- Rewrite Options
  - VLAN ID rewrite
  - VLAN Header rewrite
  - Frame Relay DLCI switching
- L2TPv3 Options
  - 0,4,8 byte cookies
  - TTL set in tunnel header
  - IP ToS set, or reflect from inner IP header
  - DF bit set
  - Path MTU discovery

- QoS
  - There is no classification support when the interface has xconnect.
  - Input QoS on the L2 circuit is limited to set and police configured under the default class. The service policy must have the following format:

```
policymap p1
   class class-default
     set qos-group .. [AND/OR]
     police ..
```

  - Output QoS on the L2 circuit is limited to police configured under the default class.
- Local Switching
  - Support for VLAN, Ethernet port, AAL5, HDLC and PPP local switching.
- MIB Support
  - Limited to Cisco Enterprise VPDN MIB. PW-MIB support is not available in this release.

For additional information on this feature, see the *Cisco 7304 Troubleshooting and Configuration Notes* document:

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

Loadsharing IP Packets over More Than Six Parallel Paths

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/fs_mpg6.htm

Memory Threshold Notifications

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/fs_memnt.htm

MPLS

Cisco IOS Release 12.2(27)SBC supports the following Multiprotocol Label Switching (MPLS) features.

MPLS - Interfaces MIB Enhancements

For detailed information about this feature (which is also known as the MPLS Enhancements to Interfaces MIB feature), see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsintmb4.htm

MPLS - LDP MIB Version 08 Upgrade

For detailed information about this feature, including the MPLS LDP - MIB Notifications feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fsldp8_3.htm

MPLS Traffic Engineering Forwarding Adjacency

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

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 VPN Support for EIGRP Between Provider Edge and Customer Edge

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/fteipece.htm

MPLS VPN—VRF Selection Based on Source IP Address

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

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

MSDP Compliance with IETF RFC 3618

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

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

Multicast and Multicast VPN for PXF

Multicast and Multicast VPN support for PXF that was previously introduced in Cisco IOS Release 12.2S is also available in Cisco IOS Release 12.2SBC release starting in Cisco IOS Release 12.2(27)SBC.

The Multicast and Multicast VPN (mVPN) for PXF feature introduces support for the following packets in the PXF processing path:

- Basic Multicast Packets
- Basic Multicast Packets using VRF (VRF-lite configuration)
- Multicast packets using VRF and MPLS VPN

No new configuration has been introduced as a result of the introduction of this feature. This feature simply forwards the previously mentioned packets using the PXF-switching path, assuming the configurations were previously configured.

For some sample configurations, see the following documents:

- The *Multicast Quick-Start Configuration Guide*

  http://www.cisco.com/warp/customer/105/48.html

- The "Configuration Examples for Multicast VPN—IP Multicast Support for MPLS VPNs" section in the *Multicast VPN—IP Multicast Support for MPLS VPNs* document

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs_mvpn.htm#1041814

For additional information on this feature, see the *Cisco 7304 Troubleshooting and Configuration Notes* document:

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

NetFlow

Cisco IOS Release 12.2(27)SBC supports the following NetFlow features.

NetFlow Export Version 9 Support

For detailed information about this feature (which is also known as the NetFlow v9 Export Format feature), see the following Cisco document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/nfexpfv9.html

NetFlow Input Filters

For detailed information about this feature (which is also known as the NetFlow Input Filters and Multi-Sampling Rates feature), see the following Cisco document:

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

NetFlow MIB

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/nflowmib.htm

NetFlow MIB and Top Talkers

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/nflowtt.htm

NetFlow Multicast Support

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/nfmultic.htm

OSPF

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

OSPF Area Transit Capability

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

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

OSPF Forwarding Address Suppression in Translated Type-5 LSAs

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

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

OSPF Inbound Filtering Using Route Maps with a Distribute List

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

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

OSPF Incremental Shortest Path First (i-SPF) Support

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

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

OSPF Link-Local Signaling Per Interface Basis

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

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

OSPF Link State Database Overload Protection

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

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

OSPF MIB Support of RFC 1850 and Latest Extensions

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

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

OSPF Support for a Redistribution Limit of Maximum Prefixes Imported

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

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

OSPF Support for Fast Hellos

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

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

OSPF Support for Forwarding Adjacencies over MPLS Traffic Engineered Tunnels

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

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

OSPF Support for Link State Advertisement (LSA) Throttling

For detailed information about this feature (which is also known as the OSPF Link-State Advertisement [LSA] Throttling feature), see the following Cisco document:

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

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

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

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

PXF

Cisco IOS Release 12.2(27)SBC supports the following Parallel Express Forwarding (PXF)-based features.

For additional information on these features and other PXF features, including restrictions, see the "PXF Features" section in the *Cisco 7304 Troubleshooting and Configuration Notes* document:

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

Frame Relay Discard Eligibility Bit Marking (PXF Based)

The ability to mark Frame Relay Discard Eligibility (DE) bits via the **set fr-de** command is now available in the Parallel Express Forwarding (PXF) processing path on the Cisco 7304 router.

The DE bit in the address field of a Frame Relay frame is used as a method for prioritizing the discarding of frames in congested Frame Relay networks. The Frame Relay DE bit has only two settings, 0 or 1. If congestion occurs in a Frame Relay network, frames with the DE bit set to 1 are discarded before frames with the DE bit set to 0. Therefore, important traffic should have the DE bit set to 0, and less important traffic should be forwarded with the DE bit set to 1.

The default DE bit setting is 0. The Class-Based Packet Marking feature allows users to change the DE bit setting to 1 for various traffic, giving users the option of keeping the default value of 0 or changing the value to 1. Users can therefore use Frame Relay DE bit marking to prioritize frames in a Frame Relay network.

For general, non-PXF specific information on this feature, see the *Class-Based Marking* document:

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

Generic Routing Encapsulation Tunnel IP Source and Destination VRF Membership (PXF Based)

The Generic Routing Encapsulation Tunnel IP Source and Destination VRF Membership feature enables users to specify the Virtual Private Network (VPN) routing/forwarding (VRF) membership of a generic routing encapsulation (GRE) tunnel IP source and destination in the Parallel Express Forwarding (PXF) processing path for the Cisco 7304 router. Before the introduction of this feature, the VRF tunnel interface required the global route to the tunnel destination to remain up. This feature removes this restriction.

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/fsgrevrf.htm

For additional information on this and other PXF features, see the "PXF Features" section in the *Cisco 7304 Troubleshooting and Configuration Notes* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm#65935

Hierarchical Aggregate Ingress Policing (PXF Based)

Hierarchical Aggregate Ingress Policing support is now available in the Parallel Express Forwarding (PXF) processing path on the Cisco 7304 router.

Hierarchical Aggregate Ingress Policing enables users to first police the aggregate default traffic and then police (via marking) the traffic that belongs to each nested traffic class.

In a Hierarchical Aggregate Ingress Policing configuration, the child policy map can have up to 23 user-defined classes, and the service policy that contains the child policy can be configured only on the default traffic class.

Interface Queueing for Subinterfaces (PXF Based)

The Interface Queueing for Subinterfaces feature is now available in the Parallel Express Forwarding (PXF) processing path for the Cisco 7304 router.

The Port Level Queueing for Subinterfaces feature allows port-level quality of service (QoS) configurations to be applied to 802.1q subinterfaces and data-link connection identifiers (DLCIs). QoS features can still be applied specifically to 802.1q subinterfaces and DLCIs, and the QoS configurations on the 802.1q subinterfaces and DLCIs will always take precedence over the port-level QoS configurations when the 802.1q subinterfaces or DLCI configurations conflict with the port-level QoS configurations.

MQC Hierarchical Service-Policy Map Infrastructure (PXF Based)

The MQC Hierarchical Service-Policy Map Infrastructure feature introduces hierarchical service policies that do not require a default class at the parent level in the Parallel Express Forwarding (PXF) processing path on the Cisco 7304 router. A user can now define multiple class queues with multiple classes of traffic feeding into each class queue.

For additional information on this and other PXF features, see the "PXF Features" section in the *Cisco 7304 Troubleshooting and Configuration Notes* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm#65935

MQC Match and Set QoS Group (PXF Based)

Quality of Service (QoS) group matching and setting are now available in the Parallel Express Forwarding (PXF) processing path on the Cisco 7304 router.

Marking a packet with a local QoS group value allows users to identify a group ID with a packet. The group ID can be used to classify packets into QoS groups based on prefix, autonomous system, and community string. This QoS group marking can be used only to classify traffic within a single router and cannot, therefore, be used to mark packets leaving the router. For this reason, QoS group values cannot be applied on output traffic policies (which are attached to interfaces that are configured with the **service-policy output** command).

The QoS group value is usually used for one of the two following reasons:

- To leverage a large range of traffic classes. The QoS group value has 100 different individual packet markings, as opposed to IP DSCP and IP Precedence, which have 64 and 8 values, respectively.
- If changing the IP Precedence or IP differentiated services code point (DSCP) value of the packet is undesirable.

For general, non-PXF specific information on this feature, see the *Class-Based Marking* document:

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

NetFlow Export of BGP Next Hop Information (PXF Based)

The NetFlow Export of BGP Next Hop Information feature is now available in the Parallel Express Forwarding (PXF) processing path for the Cisco 7304 router.

The BGP Next Hop Information feature provides additional flexibility when designing and migrating networks. The BGP Next Hop Propagation feature allows a route reflector to modify the next hop attribute for a reflected route and allows Border Gateway Protocol (BGP) to send an update to an external BGP (eBGP) multihop peer with the next hop attribute unchanged.

For additional information on this and other PXF features, see the "PXF Features" section in the *Cisco 7304 Troubleshooting and Configuration Notes* document:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm#65935

For general, non-PXF specific information about the NetFlow Export of BGP Next Hop Information feature, see the *NetFlow BGP Next Hop Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/nfbgpnxt.htm

Port Mode Cell Relay Support for PA-A3-T3, PA-A3-E3, and PA-A3-OC3 PAs

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

Random Sampled NetFlow

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/nfstatsa.htm

Route Processor Redundancy Plus (RPR+)

The Route Processor Redundancy Plus (RPR+) and Stateful Switchover (SSO) redundancy modes, along with Route Processor Redundancy (RPR), Fast Software Upgrade (FSU), and online insertion and removal (OIR) of Route Processors (RPs), comprise the Cisco 7304 Route Processor High Availability feature.

A benefit of operating in RPR+ or SSO mode is that the standby RP boots up completely and switches over in a short period of time, usually 4 to 5 seconds in the case of RPR+ and in under 1 second in the case of SSO. The fast switchover is achieved in part because line cards are not reset across the switchover. In addition, the running configuration and the startup configuration are synchronized from the active RP to the standby RP.

For more information on the Route Processor Redundancy Plus (RPR+) feature on the Cisco 7304 router, see the *Cisco 7300 Series High Availability NSE Redundancy* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121ex/121ex10/12e_rpr.htm

Router Security Audit Logs

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/gtaudlog.htm

Secure Shell Version 2 Support

For detailed information about this feature, including the Secure Shell SSH Version 2 Client Support feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_ssh2.htm

SNMPv3 Community MIB Support

The SNMPv3 Community MIB Support feature implements support for the SNMP Community MIB (SNMP-COMMUNITY-MIB) module, defined in RFC 2576, in Cisco IOS software.

RFC 2576, “Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework,” defines the requirements for interoperability between SNMPv1, SNMPv2c, and SNMPv3. The SNMP Community MIB module defines objects to help support these requirements.

The SNMPv1/v2c Message Processing Model and Security Model require mappings between parameters used in SNMPv1 and SNMPv2c messages and the version-independent parameters used in the Simple Network Management Protocol (SNMP) architecture. The SNMP Community MIB contains objects for mapping between these community strings and version-independent SNMP message parameters.

The mapped parameters consist of the SNMPv1/v2c community name and the SNMP securityName and contextEngineID/contextName pair. This MIB provides mappings in both directions; that is, a community name may be mapped to a securityName, contextEngineID, and contextName, or the

combination of securityName, contextEngineID, and contextName may be mapped to a community name. This MIB also augments the snmpTargetAddrTable with a transport address mask value and a maximum message size value.

For implementation details, see the SNMP-COMMUNITY-MIB.my file, available through Cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Source Specific Multicast (SSM) Mapping

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/gtssmma.htm

Stateful Switchover and Nonstop Forwarding

Cisco IOS Release 12.2(27)SBC supports the following Stateful Switchover (SSO) and Nonstop Forwarding (NSF) features.

EIGRP NonStop Forwarding Awareness

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_ensf.htm

Nonstop Forwarding (NSF) with Stateful Switchover (SSO)

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

- Nonstop Forwarding (NSF):

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

- Stateful Switchover (SSO):

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

Stateful Switchover (SSO) for ATM

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

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

Stateful Switchover (SSO) for Frame Relay

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

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

Stateful Switchover (SSO) for HDLC

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

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

Stateful Switchover (SSO) for Multilink PPP (MLP)

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

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

Stateful Switchover (SSO) for PPP

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

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

Unique Device Identifier (UDI) Retrieval

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

VRF Aware Multicast Error Messages

Multicast error messages that are associated with a particular multicast VPN customer in an MPLS VPN environment can be tracked.

MIBs

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

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

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

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

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

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

Limitations and Restrictions

The following sections contain information about limitations and restriction in Cisco IOS Release 12.2SB that can apply to the Cisco 7304 router.

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

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

SNMP Version 1 BGP4-MIB Limitations

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

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2SB that can apply to the Cisco 7304 router.

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml

Field Notices and Bulletins

For general information about the types of documents listed in this section, see the following document:

http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/index.shtml

- Field Notices—We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account with Cisco.com, you can find field notices at http://www.cisco.com/kobayashi/support/tac/fn_index.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/public/support/tac/fn_index.html.Product Bulletins—If you have an account with Cisco.com, you can find product bulletins at

http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find product bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.

- *What's New for IOS—What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in to Cisco.com and selecting **Support**: **Software Downloads**: **Cisco IOS Software**: **What's New for IOS**.

Important Notes for Cisco IOS Release 12.2(27)SBC

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

MPLS MTU Command Change

The behavior of the **mpls mtu** command has changed in Cisco IOS Release 12.2(27)SBC 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

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(27)SBC5

Cisco IOS Release 12.2(27)SBC5 is a rebuild release for Cisco IOS Release 12.2(27)SBC. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBC5 but may be open in previous Cisco IOS releases.

Miscellaneous

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsd79827

  Symptoms: The **service-policy input** or **service-policy output** command may not take affect on ATM VCs and the following error message may be generated

  ```
  CBWFQ: Not supported on subinterfaces
  ```

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(27)SBC2.

  Workaround: Re-apply the command and save the configuration.

- CSCse03796

  Symptoms: When you insert a redundant power supply, no ENVMON traps are generated.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with dual power supplies. When one of the power supplies is shut down and then re-inserted, log messages are generated but no ENVMON traps are generated.

  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.

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(27)SBC4

Cisco IOS Release 12.2(27)SBC4 is a rebuild release for Cisco IOS Release 12.2(27)SBC. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBC4 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeg62206

  Symptoms: High CPU utilization may occur during the TPLUS process on a platform.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(6c) and that is configured for TACACS. The symptom may also occur in other releases.

  Workaround: There is no workaround.

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

- CSCej43682

  Symptoms: Packet loss may occur on a Cisco 7304 when packets are switched in the CEF path into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S or a later release. The symptom could also occur in Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCek27783

  Symptoms: A ping from a Cisco 7304 to a DNS server may fail until a first High Availability (HA) switchover occurs.

  Conditions: This symptom is observed on Cisco 7304 that has NPE-G100 Network Processing Engines (NPEs) that function in Stateful Switchover (SSO) HA mode and that run the c7300-js-mz Cisco IOS software image. For the symptom to occur, traffic must be sent via the interfaces of the standby RP.

  Workaround: Ensure that no traffic is sent to the interfaces of the standby NPE.

- 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.

- 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.

- 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.

- CSCsd14442

  Symptoms: A VRF-aware GRE tunnel does not function properly when you disable the PXF engine; packets are not punted properly by the PXF engine.

Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that functions as a PE router.

Workaround: There is no workaround.

- 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: Do not apply a virtual template to an ATM interface.

- CSCsd25815

  Symptoms: When the **bandwidth** and **bandwidth remaining percent** commands are configured in the same service policy, the service policy does not function as expected because the bandwidth that is configured in the class does not receive the guaranteed bandwidth.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 processor.

  Workaround: There is no workaround.

  Further Problem Description: The **bandwidth** and **bandwidth remaining percent** commands are not allowed in the same service policy, that is, a mixed bandwidth configuration is not allowed in the same policy map.

- 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.

- CSCsd68445

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

  1. Symptom 1: You may not be able to apply a QoS policy map with class-based shaping that is configured in the default class on a dot1q subinterface, and the following error messages may be generated:

     Configuring this shaping class will impact guarantees in other classes under this policy-map

     Condition 1: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(27)SBC2 when a hierarchical QoS policy is configured in the following way and when the shape rate is higher than the CIR rate:

     policy-map child-qos class *user-defined-class* **priority police cir** *cir-rate* **bc** *Bc* **be** *Be* **conform-action transmit exceed-action drop**

     policy-map parent-qos class class-default shape average *shape-rate* **service-policy child-qos**

     Workaround 1: There is no workaround.

  2. Symptom 2: You may not be able to apply a QoS policy map with class-based shaping that is configured in the default class on a dot1q subinterface, and the following error messages may be generated:

     Configuring this shaping class will impact guarantees in other classes under this policy-map

     Condition 2: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(27)SBC2 when a single policy map with class-based shaping is configured in the following way:

     policy-map shaping-qos class class-default shape average *shape-rate*

     Workaround 2: Perform the following steps:

     1) Configure a new class map that has the same characteristics as the original class default as in the example below, in which the new class map is called “my-class-default”:

     class-map match-all my-class-default match any

     2) Configure the new policy map by using the just created class-default equivalent class (“my-class-default”) as following example, in which the new policy map is called “my-policy-map”:

     policy-map my-policy-map class my-class-default shape average *shape-rate*

     3) Apply the service policy (“my-class-default”) to the dot1q subinterface.

- 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.

Wide-Area Networking

- CSCeg82698

  Symptoms: PPTP tunnels do not come up.

  Conditions: This symptom is observed when VPDN is configured.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(27)SBC3

Cisco IOS Release 12.2(27)SBC3 is a rebuild release for Cisco IOS Release 12.2(27)SBC. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBC3 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCsc29478

  Symptoms: Interfaces of a serial port adapter fail and do not come into service, preventing you from establishing links or tunnels via these interfaces.

  Conditions: This symptom is observed on a Cisco 7500 series that runs an interim release for Cisco IOS Release 12.0(32)S. However, the symptom is not platform-specific and release-specific.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCei45669

  Symptoms: An OSPF router may update and originate a new version of an LSA when it should flush the LSA.

  Conditions: This symptom is observed on the originating router when it receives a self-originated MaxAge LSA before it can flush this LSA from its database. This symptom may occur under a rare condition when a neighboring router calculates that is has a newer copy of the LSA from the originating router and bounces the MaxAge LSA to the originating router.

  Workaround: Enter the **clear ip ospf process** command.

Miscellaneous

- CSCeg19184

  Symptoms: An I/O memory leak and intermittent packet loss may occur on a Cisco 7304 that is configured with an NSE-100.

  Conditions: This symptom is observed only on interfaces that are configured for MLP.

  Workaround: There is no workaround.

- CSCek05730

  Symptoms: A Cisco router may crash unexpectedly because of a bus error and/or display some spurious memory accesses.

Conditions: This symptom is observed when an interface that is configured for some form of fancy queueing (that is, anything besides FIFO queueing) actively forwards traffic.

Workaround: Disable fancy queueing on the Ethernet interface.

- CSCsb94859

  Symptoms: AToM VCs do not come up after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that is configured with AToM VCs when you perform a soft SSO switchover by entering the **redundancy force-switchover** command, preventing the AToM VCs from coming up on the standby RP and the AToM circuit from being established.

  Workaround: First, configure an incorrect MTU value on the AToM VCs. Then, change the MTU to the correct value. Doing so brings up the AToM VCs and establishes the AToM circuit.

- CSCsc24788

  Symptoms: Scaling to 4000 Ethernet VLANs fails, and the following error message may be generated:

  ```
  ws_dot1q_encap_vlan_table: failed to get a tif number.
  ```

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and occurs when the router is configured with more than 2000 VLANs.

  Workaround: There is no workaround.

- CSCsc65787

  Symptoms: A router may modify the interface MTU of an interface during the initialization process. In turn, this situation may modify layer 3 protocol MTUs (such as IP MTUs), preventing OSPF, IS-IS, or other L3 protocols from coming up.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image of Release 12.2SB that includes the fix for caveat CSCsa73817 when the MPLS MTU is larger than the interface MTU.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa73817.

  Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Configure the interface MTU to be equal to or larger than the MPLS MTU and configure the IP MTU to the desired value.

- 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.

- CSCsc96947

  Symptoms: A Cisco 7304 that has an NSE-100 and that is configured for AToM may lose connectivity.

  Conditions: This symptom is observed when a network event such as an interface flap or LDP update occurs while the AToM circuit is being established, preventing the PXF engine from being updated with the new MPLS label and causing the previous label to be used to forward the packet.

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

- CSCsc97627

  Symptoms: When you enter the **mpls l2transport route** command on an Ethernet interface that has a VLAN configuration, an unrecognized command error message may be generated.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NSE-1.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs because the NSE has not been added to the AToM validation list, preventing the **mpls l2transport route** command from being accepted.

- CSCsd11646

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

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

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

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

- CSCsd13069

  Symptoms: Packets that are sent from one CE router to another CE router via a PE router are dropped in an EoMPLS configuration.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100, that functions as a PE router in the backbone of an MPLS network, and that is configured for EoMPLS.

  Workaround: There is no workaround. Note that the symptom does not occur when the PXF engine is disabled.

- CSCsd14538

  Symptoms: In a configuration with a GRE tunnel and VPN VRFs, when you ping between CE routers, the PE router in between crashes.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that functions as a PE router. The symptom occurs after you have reloaded the Cisco 7304 with VPN VRFs.

  This symptom may be more likely to occur when a serial interface connects the PE router (which terminates the GRE tunnel) to the MPLS core. After GRE encapsulation has occurred, packets should be punted from the PXF engine because the tunnel adjacency is not complete. However, the PXF engine fails to punt the packets.

  Possible Workaround: Replace the serial interface with an interface of a different type.

- CSCsd26878

  Symptoms: A Cisco 7304 may crash, and the following error messages are generated in the crashinfo file:

  ```
  %Error: TMCINT
  PXF[0] Exception: mac_xid=0x10000, cpu_xid=0x0 IHB Exception:
  ihb_x_type=0x8 ihb_x_mask=0x0
  PXF[1] Exception: mac_xid=0x10000, cpu_xid=0x0 IHB Exception:
  ihb_x_type=0x8 ihb_x_mask=0x0

  PXF to RP IPC Queue: 0/128/0/0 (size/max/received/drops) Fail to get new buffer for
  PXF2RP IPC processing: 0 Fail to send RP-to-PXF IPC: 0
  ```

  Conditions: This symptom is observed on a Cisco 7304 that has dual NSE-100 processors that are configured with 512 MB SDRAM and 256 MB flash memory, and that run in redundancy mode.

  Workaround: There is no workaround.

- CSCsd32567

  Symptoms: A Cisco 7304 may reload unexpectedly when a port adapter carrier card (7300-CC-PA) is de-activated.

  Conditions: This symptom is observed when one of the following events occurs and is more likely to occur with high traffic rates:

  - You enter the **hw-module slot** *slot-number* **stop** command for the slot in which the 7300-CC-PA is installed.
  - The FPGA image for the 7300-CC-PA or the ROM monitor on the 7300-CC-PA are upgraded. At the end of the FPGA or ROM monitor upgrade the line card is de- activated and re-activated.
  - An event that leads to an unexpected reload occurs on the 7300-CC-PA, requiring the 7300-CC-PA to be de-activated and re-activated.

  Workaround: There is no workaround. Reduce the traffic through the line card and through the router to diminish the chances of the symptom occurring.

  Further Problem Description: The symptom could also occur with a 6-port E3 (7300-6E3) or 6-port T3 (7300-6T3) line card. However, the fix for this caveat addresses the 7300-CC-PA, 7300-6E3, and 7300-6T3 line cards.

Resolved Caveats—Cisco IOS Release 12.2(27)SBC2

Cisco IOS Release 12.2(27)SBC2 is a rebuild release for Cisco IOS Release 12.2(27)SBC. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBC2 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCej20751

  Symptoms: A Cisco router may not process IP packets on an Ethernet interface, and the output of the **show ip cef switching stat** command may display non-zero counts for “Bad IP packet length”.

  Conditions: This symptom is observed on a Cisco router that is configured for IP CEF or dCEF and occurs after some dot1q subinterfaces are deleted from the Ethernet interface.

  Workaround: After the dot1q subinterfaces are deleted, create a Native VLAN subinterface, assign an IP address to it, and send some IP traffic to this IP address. After you have done so, you may delete the Native VLAN subinterface.

IP Routing Protocols

- CSCsa98059

  Symptoms: Suboptimal routing occurs in an OSPF configuration or a routing loop occurs between two border routers that redistribute BGP into OSPF.

  Conditions: These symptoms are observed when at least two border routers are connected via eBGP to another autonomous system, receive the same prefix over these connections, and redistribute the prefix into OSPF. Under certain conditions, for example when the eBGP session from the preferred BGP exit point to the eBGP peer flaps, the second router in the local autonomous system becomes the preferred path and redistributes the eBGP route into OSPF. When the eBGP session with the first router comes back up, the LSA should be flushed but this does not occur. This situation may create routing problems on other OSPF routers or, when BGP has a higher administrative distance than OSPF, routing loops between both border routers.

  Workaround: There is no workaround.

Miscellaneous

- CSCed21063

  Symptoms: On a headend of an MPLS TE tunnel, a tag may be changed to an implicit null label when a RESV message is received with a different label than the one that was previously programmed. On the midpoint of the MPLS TE tunnel, the label is deprogrammed altogether for several seconds (15 to 30 seconds), causing a label mismatch to occur between the headend and the midpoint and packets to be lost.

  Conditions: This symptom is observed when a non-Cisco P router changes the label on a TE tunnel without issuing a tear message. This situation causes a Cisco router to receive a RESV message with a different label than the one that was previously programmed and causes the Cisco router to program an implicit null label for the IP address that is associated with the tunnel.

  Workaround: To restore proper traffic flowing, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected tunnel interface.

- CSCed48156

  Symptoms: A Cisco 7500 series router may generate SYS-3-CPUHOG error messages and may drop OSPF and BGP adjacencies.

  Condition: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.1(10)E6 after a script has removed and added two ACLs. The symptom is not platform-specific and may also occur in other releases.

  Workaround: There is no workaround.

- CSCeg03885

  This caveat consists of two symptoms, two conditions, and two workarounds, and only refers to routers that are configured with MPLS TE tunnels:

  1. Symptom 1: Momentary packet loss may occur during tunnel reoptimization, usually several times between the creation of a new tunnel and the cleanup of the old tunnel. Sometimes, longer packet loss may occur during tunnel reoptimization.

     Condition 1: This symptom is observed on any MPLS TE tunnel when the reoptimized label switched path (LSP) traverses a midpoint or headend router that runs Cisco IOS Release 12.0(25)S4.

Workaround 1: There is no workaround.

2. Symptom 2: Permanent bad labels may be present after MPLS TE tunnel reoptimization.

   Condition 2: This symptom is observed on a router that runs a Cisco IOS image that does not include the fix for CSCed21063 and that functions in a network in which some routers run Cisco IOS Release 12.0(25)S4. With the exception of release 12.0(25)S4 itself, Cisco IOS software releases that are listed in the "First Fixed-in Version" field at the following location are not affected:
   http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed21063.

   Workaround 2: There is no workaround. To recover from the symptoms, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected TE tunnel interface.

- CSCei82285

  Symptoms: A software-forced reload may occur on a Cisco 7304 that functions as a PE router.

  Conditions: This symptom is observed when the Cisco 7304 receives a UDP packet and when the following conditions are present:

  – The UDP packet is switched via MPLS from an Ethernet ingress interface that is configured for dot1q.

  – The UDP packet has an aggregate label for the egress interface.

  This situation is typically found in an MPLS VPN environment for an interface of a CE router that faces a PE router. The symptom occurs because the aggregate label instructs the PE router to perform a FIB lookup to resolve the forwarding, but the PE router does not perform this action.

  Workaround: There is no workaround.

- CSCej51891

  Symptoms: The framing configuration on the interface of a T3/E3 serial SPA is rejected and defaults to C-bit when a Cisco 7304 boots.

  Condition: This symptom is observed when the interface of the T3/E3 serial SPA is configured for M13 framing.

  Workaround: When the router has booted, re-enter the **framing m13** interface configuration command on the affected interface.

- CSCej65100

  Symptoms: A Cisco 7304 may crash when interfaces flap and the following error message is generated:

  ```
  Error:TMCINT router crashed
  ```

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2S or Release 12.2SB.

  Workaround: There is no workaround.

- 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.

- CSCsb88605

  Symptoms: Some interfaces on which channel groups are configured may flap continuously and keepalives may become lost. The interfaces flap whether they process a high volume of traffic or no traffic at all and appear to be stuck.

  Conditions: This symptom is observed on a Cisco 7304 that has a channelized port adapter that is configured for channel groups. The symptom may also occur on other Cisco 7x00 routers that are configured with channelized port adapters and is more likely to occur with a large number of channel groups.

  Workaround: There is no workaround.

- CSCsb92588

  Symptoms: A Cisco 7304 port adapter carrier card (7300-CC-PA) may reload.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 7300-CC-PA when a heavy volume of egress traffic is sent. The symptom occurs only in the following Cisco IOS releases:

  - Release 12.2(20)S9
  - Release 12.2(25)S5
  - Release 12.2(25)S6
  - Release 12.2(25)S7
  - Release 12.2(27)SBC
  - Release 12.2(27)SBC1

  Workaround: There is no workaround.

- CSCsc35918

  Symptoms: When packets are dropped from the PXF engine, the ICMP error message generation process may fail to send "Destination Unreachable" messages to the source.

Conditions: The symptom is observed on a Cisco 7304 that functions as a PE router in an MPLS VPN environment when the core-facing interface is an Ethernet port adapter or SPA.

Workaround: There is no workaround.

- CSCsc44237

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

  1. Symptom 1: A switch or router that is configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

     The output of the **show processes memory** command shows that the "ATM PA Helper" process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

     Condition 1: This symptom is observed on a Cisco switch or router that runs a Cisco IOS software image that contains the fixes for caveats CSCeh04646 and CSCeb30831. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh04646 and http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb30831.

     Cisco IOS software releases that are not listed in the "First Fixed-in Version" fields at these locations are not affected.

     Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

  2. Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory.

     The output of the **show processes memory** command shows that the "PIM process" does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

     Condition 2: This symptom observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCef50104.

     A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef50104. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

     Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf** *vrf-name* command is configured, enter the **ip vrf forwarding** *vrf-name* command on at least one interface that has PIM enabled.

- CSCsc62499

  Symptoms: A router crashes when you apply a service policy with a WRED configuration.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100 when traffic is being send.

  Workaround: There is no workaround.

- CSCsc93774

  Symptoms: A Cisco 7304 may crash when you enter the **debug platform ipc packets** privileged EXEC command.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for high availability (HA).

Workaround: Do not enter the **debug platform ipc packets** privileged EXEC command.

- CSCsc98645

  Symptoms: When you configure a three-level policy map with traffic policing and apply it on an Ethernet subinterface, the router rejects the configuration with the following error message:

  ```
  Policing in both parent and child policy-maps is only supported if parent class is class-default
  ```

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(27)SBC1.

  Workaround: Remove traffic policing (and therefore the priority) from the policy map. If this is not an option, there is no workaround.

Wide-Area Networking

- CSCsc66592

  Symptoms: When a user session is not subject to renegotiation, an LNS sends PPP keepalives with a magic number that is different from the one negotiated between the client and the LAC, preventing the client from answering the keepalive requests of the LNS.

  Conditions: This symptom is observed on a Cisco router that functions as an LNS when a user session is not subject to renegotiation. The symptom does not occur when renegotiation is triggered on the LNS.

  Workaround: Disable keepalives on the virtual-template interface that is used to clone the configuration for the user sessions.

  Alternate Workaround: Configure renegotiation.

Resolved Caveats—Cisco IOS Release 12.2(27)SBC1

Cisco IOS Release 12.2(27)SBC1 is a rebuild release for Cisco IOS Release 12.2(27)SBC. The caveats in this section are resolved in Cisco IOS Release 12.2(27)SBC1 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCej05426

  Symptoms: When the standby RP functions in SSO mode and you enter the **no rtr reaction-configuration** *operation-number* command, the standby RP is forced into RPR mode and the active RP cannot enter the configuration mode. The standby RP remains in the initialization mode. You must reload both the active RP and the standby RP to enable them to return into SSO mode.

  Conditions: This symptom is observed on a Cisco 7304 when a probe is created automatically via the IP SLA “rtr mpls-lsp-monitor” commands and when you remove, reschedule, or reconfigure the probe via the **no rtr** *operation-number*, **no rtr reaction-configuration** *operation-number*, or **no rtr schedule** *operation-number* command.

  Workaround: Do not use the CLI to make changes to the probe. Rather, make changes to the probe via the IP SLA “rtr mpls-lsp-monitor” commands.

IP Routing Protocols

- CSCei13040

  Symptoms: When an OSPF neighbor comes back up after a very fast (sub-second) interface flap, OSPF routes that are learned via the interface that flapped may not be re-installed in the RIB.

  Conditions: This symptom is observed when the following two events occur:

  - The interface flaps very quickly.
  - The neighbor comes back up before the LSA generation timer expires.

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

  Alternate Workaround: Enter the **clear ip route *** EXEC command.

- CSCsc07467

  Symptoms: An OSPF route is lost after an interface flaps.

  Conditions: This symptom is observed rarely when all of the following conditions are present:

  - There is a very brief (shorter than 500 ms) interface flap on a point-to-point interface such as a POS interface.
  - The flap is not noticed by the neighbor, so the neighbors interface remains up.
  - The OSPF adjacency goes down and comes back up very quickly (the total time is shorter than 500 ms).
  - OSPF runs an SPF during this period and, based on the transient adjacency information, removes routes via this adjacency.
  - The OSPF LSA generation is delayed because of LSA throttling. When the LSA throttle timer expires and the LSA is built, the LSA appears unchanged.

  Workaround: Increase the carrier-delay time for the interface to about 1 second or longer.

  Alternate Workaround: Use an LSA build time shorter than the time that it takes for an adjacency to come up completely.

ISO CLNS

- CSCei36669

  Symptoms: A CPUHOG and traceback occur when a malicious IS-IS LSP packet is received.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S.

  Workaround: There is no workaround.

Miscellaneous

- CSCed92374

  Symptoms: ALIGN-3-SPURIOUS and/or ALIGN-3-TRACE tracebacks may be generated on a router when you set the default for a range of ports.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S.

  Possible Workaround: Set the default ports one at the time.

- CSCei36831

  Symptoms: A Cisco 7304 that functions as an mVPN PE router may reload while processing large ping packets.

  Conditions: This symptom is observed when the router runs an mVPN script and when a remote CE router pings a multicast group and when packets require fragmentation.

  Workaround: There is no workaround.

- CSCej22671

  Symptoms: When shaping and bandwidth are configured with Low Latency Queuing (LLQ), the bandwidth and shaping class of traffic do not receive the guaranteed bandwidth.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100.

  Workaround: There is no workaround.

- CSCej54824

  Symptoms: AToM connectivity is lost when an MPLS core side interface is configured as an Ethernet VLAN.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that has PXF enabled.

  Workaround: There is no workaround.

- CSCin95594

  Symptoms: Weighted Random Early Detection (WRED) does not function for user-defined classes in a policy that is attached to a PVC on an interface of a PA-A3-8T1IMA port adapter.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2(27)SBC when a service policy is configured with random-detect for user-defined classes.

  Workaround: Increase the value of the VC hold queue size via the **vc-hold-queue** interface configuration command, for example, to 512, which is the default hold queue size for WFQ.

- CSCsb09972

  Symptoms: A Cisco 7304 that is configured with a GRE tunnel may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(20)S8. The symptom may also occur in other releases of Release 12.2S or in releases that are based on Release 12.2S.

  Workaround: There is no workaround.

- CSCsb43489

  Symptoms: When PPP encapsulation is configured on a Cisco 7304, excessive traffic loss may occur after an SSO switchover.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(27)SBC.

  Workaround: There is no workaround.

- CSCsb62668

  Symptoms: A VRF-aware GRE tunnel may not function on a Cisco 7304.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 or NPE-G100 and that runs Cisco IOS Release 12.2(25)S6 or Release 12.2(27)SBC.

Traffic from the tunnel source to the destination does not go through properly and a ping between the tunnel address of a Cisco 7304 that functions as a CE router and the tunnel address of a Cisco 7304 that functions as a PE router does not work properly when the routers run Release 12.2(25)S6. This configuration works fine when the routers run Release 12.2(27)SBC.

When both routers function as CE routers and run either Release 12.2(25)S6 or Release 12.2(27)SBC, there is no proper connectivity.

Workaround: There is no workaround.

- CSCsb64724

  Symptoms: You cannot unconfigure and reconfigure a VC.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 2-port OC-3 ATM line card.

  Workaround: There is no workaround.

- CSCsb73181

  Symptoms: A standby RP crashes and reloads when you apply an ATM QoS configuration.

  Conditions: This symptom is observed on a Cisco 7304 that has two RPs and ATM line cards when an HA switchover occurs and when a QoS configuration is applied or changed.

  Workaround: There is no workaround.

- CSCsb84788

  Symptoms: A Cisco 7304 may crash when a (tmc0/1) PXF crash occurs. The crash summary shows the following information:

```
tmc0 Crash Summary
  0040 0300 XHXType  :80000000 Global Halt
  0040 0308 MACXID   :00010000 IHB Exception
  0040 0004 IHBXType :00000008 watchdog timer expired
  0040 0120 RPXType  :00000000
tmc1 Crash Summary
  0040 0300 XHXType  :80000000 Global Halt
  0040 0308 MACXID   :00010000 IHB Exception
  0040 0004 IHBXType :00000008 watchdog timer expired
  0040 0120 RPXType  :00000000
```

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(25)S5 when NetFlow is enabled.

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

- CSCsc11636

  Symptoms: A router requires a very long time to boot (more than 5 minutes, potentially hours). Also, changes to the QoS configuration may require long times.

  Conditions: This symptom is observed when the QoS configuration has a complex arrangement of many policies that reference many access control entries (ACEs) through a number of class maps. The time required is, roughly, proportional to the number of combinations of interfaces, policies, classes, and ACEs. For example, if each of 200 interfaces has a QoS policy, each policy uses five class maps, each class map references two ACLs, and each ACL has 30 entries, there are 60,000 combinations.

Workaround: Either reduce the number of combinations of interfaces, policies, class maps, and ACEs, or load the configuration in two stages. The first stage (from NVRAM) should contain the interface and ACL definitions, and the second stage (from another file) should contain the classes and policies.

- CSCsc16611

  Symptoms: A Cisco 7304 crashes at the "fib_path_list_get_first_path" function.

  Conditions: This symptom is observed on a Cisco 7304 when a link flap occurs on a directly connected OSPF router.

  Workaround: Disable NetFlow. If this no an option, there is no workaround.

Open Caveats—Cisco IOS Release 12.2(27)SBC

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(27)SBC. All the caveats listed in this section are open in Cisco IOS Release 12.2(27)SBC. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCei54507

  Symptoms: When a packet of disconnect (PoD) is issued on a PPP over ISDN link to disconnect a call, the call is not disconnected and a stop record is not generated.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs only for PoD types of disconnect and does not occur for normal types of disconnect.

- CSCej05426

  Symptoms: When the standby RP functions in SSO mode and you enter the **no rtr reaction-configuration** *operation-number* command, the standby RP is forced into RPR mode and the active RP cannot enter the configuration mode. The standby RP remains in the initialization mode. You must reload both the active RP and the standby RP to enable them to return into SSO mode.

  Conditions: This symptom is observed on a Cisco 7304 when a probe is created automatically via the IP SLA "rtr mpls-lsp-monitor" commands and when you remove, reschedule, or reconfigure the probe via the **no rtr** *operation-number*, **no rtr reaction-configuration** *operation-number*, or **no rtr schedule** *operation-number* command.

  Workaround: Do not use the CLI to make changes to the probe. Rather, make changes to the probe via the IP SLA "rtr mpls-lsp-monitor" commands.

IP Routing Protocols

- CSCei68145

  Symptoms: The **auto-summary** command does not function properly for a BGP IPv4 multicast address family.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC.

Workaround: There is no workaround.

- CSCej04971

  Symptoms: An EIGRP neighbor bounces when a loopback interface is created.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC when the state of a newly created loopback interface changes to "up" before the **no shutdown** command is entered. The state of a newly created loopback interface should not change to "up" until after the **no shutdown** command is entered.

  Workaround: There is no workaround.

- CSCsa83949

  Symptoms: Networks that are advertised by BGP do not show in the BGP table, which can be seen in the output of the **show ip bgp** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC.

  Workaround: There is no workaround.

- CSCsb14692

  Symptoms: The packet loss in a traffic flow from a CE router to a PE router is larger than what you would expect during an SSO switchover.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC and that functions in SSO mode.

  Workaround: There is no workaround.

Miscellaneous

- CSCei35197

  Symptoms: A router that boots may generate a "%SYS-3-NULLIDB" error message.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC and that is configured for IS-IS.

  Workaround: There is no workaround.

- CSCei36831

  Symptoms: A Cisco 7304 that functions as an mVPN PE router may reload while processing large ping packets.

  Conditions: This symptom is observed when the router runs an mVPN script and when a remote CE router pings a multicast group and when packets require fragmentation.

  Workaround: There is no workaround.

- CSCei43532

  Symptoms: Policing does not mark packets correctly for an interface that is configured for Frame Relay over L2VPN.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCei43849

  Symptoms: A cell-based policy map cannot be attached to an interface that is configured for L2VPN.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

Workaround: There is no workaround.

- CSCei44050

  Symptoms: The standby NSE-100 of a CiSco 7304 may crash when you change the configuration of the active NSE-100.

  Conditions: This symptom is observed on a Cisco 7304 that has two NSE-100 processors that run in SSO mode, that functions as a PE router in an MPLS VPN network, and that is configured with multiple VPNs.

  Workaround: There is no workaround.

- CSCej00340

  Symptoms: A Cisco 7304 crashes when you configure an SVC, unconfigure the SVC, configure a VC, and unconfigure the VC.

  Conditions: This symptom is observed on a Cisco 7304 when you perform the following actions:

  1. Configure an SVC, ping another interface, and unconfigure the SVC.
  2. Configure a VC, and ping another interface.
  3. Unconfigure the VC by entering the following commands:

     no ip routing

     no ip address *ip-address mask*

     no atm pvc *vcd vpi vci* **aal5snap inarp** *minutes*

  At this point, the router crashes.

  Workaround: Do not unconfigure a VC by using the method that is indicated in the Conditions above.

- CSCej01256

  Symptoms: A QoS set action duplicates the packet counts on a CE router that has an interface that is configured for Gigabit Ethernet over L2TPv3.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC and that functions as a CE router.

  Workaround: There is no workaround.

- CSCej03044

  Symptoms: CBWFQ does not match the input packet rate on an ATM interface, causing the input rate to be lower than what you would expect.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC.

  Workaround: There is no workaround.

- CSCin95594

  Symptoms: Weighted Random Early Detection (WRED) does not function for user-defined classes in a policy that is attached to a PVC on an interface of a PA-A3-8T1IMA port adapter.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2(27)SBC when a service policy is configured with random-detect for user-defined classes.

  Workaround: Increase the value of the VC hold queue size via the **vc-hold-queue** interface configuration command, for example, to 512, which is the default hold queue size for WFQ.

- CSCsb40799

  Symptoms: A Cisco 7304 that functions as a provider edge (PE) router may reload unexpectedly while sending traffic to a static VRF that redistributes ("leaks") a route to a global address.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(27)SBC and that functions in an MPLS VPN configuration.

  Workaround: Enter the **no ip pxf** global configuration command.

- CSCsb43489

  Symptoms: When PPP encapsulation is configured on a Cisco 7304, excessive traffic loss may occur after an SSO switchover.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(27)SBC.

  Workaround: There is no workaround.

- CSCsb62668

  Symptoms: A VRF-aware GRE tunnel may not function on a Cisco 7304.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 or NPE-G100 and that runs Cisco IOS Release 12.2(25)S6 or Release 12.2(27)SBC.

  Traffic from the tunnel source to the destination does not go through properly and a ping between the tunnel address of a Cisco 7304 that functions as a CE router and the tunnel address of a Cisco 7304 that functions as a PE router does not work properly when the routers run Release 12.2(25)S6. This configuration works fine when the routers run Release 12.2(27)SBC.

  When both routers function as CE routers and run either Release 12.2(25)S6 or Release 12.2(27)SBC, there is no proper connectivity.

  Workaround: There is no workaround.

- CSCsb73181

  Symptoms: A standby RP crashes and reloads when you apply an ATM QoS configuration.

  Conditions: This symptom is observed on a Cisco 7304 that has two RPs and ATM line cards when an HA switchover occurs and when a QoS configuration is applied or changed.

  Workaround: There is no workaround.

- CSCsb77990

  Symptoms: The PXF engine of a Cisco 7304 crashes when EoMPLS is configured.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that functions as a PE router.

  Workaround: There is no workaround.

- CSCsc95166

  Symptoms: When you boot a Cisco router with its native Gigabit Ethernet (GE) interface shut down, the controller status shows the GBIC as "gbic not present". Note that this situation is of a cosmetic nature: the native GE interface and the GBIC work fine.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1 and on a Cisco 7304 that is configured with an NPE-G100 and occurs only when the native GE interface is configured with a GBIC and is shut down when you boot the router.

  Workaround: Ensure that the native GE interface is not shut down when you boot the router. Doing so prevents the symptom from occurring.

If the symptom has occurred, enter the **no shutdown** interface configuration command on the native GE interface to enable the GBIC to be recognized.

Resolved Caveats—Cisco IOS Release 12.2(27)SBC

The caveat that is listed in this section is resolved in Cisco IOS Release 12.2(27)SBC.

Basic System Services

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

Troubleshooting

Troubleshooting information that is specific to the Cisco 7304 is available at the following location:

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

This location provides access to the following documents:

- *Cisco 7304 Router Troubleshooting*
- *Cisco 7304 Router Troubleshooting and Configuration Notes*
- *System Error Messages for the Cisco 7304 Router*
- *Bandwidth Information for Cisco 7304 Routers*

The following documents and locations provide general 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 69
- Platform-Specific Documents, page 71
- Feature Modules, page 71
- Cisco Feature Navigator, page 72
- Cisco IOS Software Documentation Set, page 72

Release-Specific Documents

This section provides information about release-specific documents.

Cisco IOS Release 12.2SB

The following documents are specific to Cisco IOS Release 12.2SB and can be found at:

- Cisco IOS Release 12.2(27)SBC

  http://www.cisco.com/en/US/docs/ios/12_2sb/release/notes/122sbrln.html
  - New feature documentation (feature modules for new features in Cisco IOS Release 12.2(27)SBC)

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 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**

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2SB and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature modules for Cisco IOS Release 12.2SB are available at the following locations:

- Release 12.2(27)SBC

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

Cisco Feature Navigator

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

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

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

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

http://www.cisco.com/register

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

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command reference publications, and several other supporting documents.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

- Configuration guides on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Reference Guides**: **Configuration Guides**

- Command references on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Configure**: **Command References**

- Configuration guides and command references on http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Cisco IOS Release 12.2 Configuration Guides and Command References**

Cisco IOS Release 12.2 Documentation Set Contents

Table 9 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**

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

Modules	Major Topics
• *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
• *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

Modules	Major Topics
• *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
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • *New Features in Release 12.2 T* • *Release Notes* (Release note and caveat documentation for 12.2-based releases and various platforms)	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco.com. From Cisco.com, click the following path: **Support: Software Downloads: Network Management Software: Cisco Network Management Toolkit: Cisco MIBs**.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

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

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

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

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

Original SSLeay License:

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

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

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

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

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

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

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

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

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

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

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

Obtaining Documentation, 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 69.