Cross-Platform Release Notes for Cisco IOS Release 12.2S

September 24, 2008

Cisco IOS Release 12.2(30)S1

OL-2586-09 Rev. Q1

These release notes support Cisco IOS Release 12.2S up to and including Cisco IOS Release 12.2(30)S1. 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(30)S and its rebuilds support only the Cisco ONS 15530 and Cisco ONS 15540 platforms. These releases do not introduce new hardware or software features but integrate resolved caveats.

Cisco IOS Release 12.2S is based on Cisco IOS Release 12.2 and is tailored for service provider and large-scale enterprise networks. Cisco IOS Release 12.2S includes features that were initially supported in Cisco IOS Release 12.2. Additionally, Cisco IOS Release 12.2S integrates features from Cisco IOS Release 12.0S, Release 12.0ST, and Release 12.1E.

For a list of the software caveats that apply to Cisco IOS Release 12.2S, see the "Caveats" section on page 140 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

© 2003–2010 Cisco Systems, Inc. All rights reserved.

Contents

- Introduction, page 2
- System Requirements, page 5
- New and Changed Information, page 32
- MIBs, page 136
- Limitations and Restrictions, page 136
- Important Notes, page 136
- Caveats, page 140
- Troubleshooting, page 536
- Related Documentation, page 537
- Notices, page 544
- Obtaining Documentation and Submitting a Service Request, page 546

Introduction

Cisco IOS Release 12.2(14)S was the first general availability release of this software. Many of the features and the hardware 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 Cisco IOS Release 12.2S, see the "New and Changed Information" section on page 32 and the "Caveats" section on page 140.

Early Deployment Releases

These release notes describe the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 routers, Cisco 7400 series routers, Cisco 7500 series routers, Cisco ONS 15530 platform, and Cisco ONS 15540 platform for Cisco IOS Release 12.2S, which is an early deployment (ED) release based on Cisco IOS Release 12.2. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features. Table 1 shows the Cisco IOS Release 12.2S early deployment releases for the above-mentioned platforms.

Table 1 Early Deployment Releases for the Cisco 7200 Series, Cisco 7301, Cisco 7304, Cisco 7400 Series, Cisco 7500 Series, Cisco ONS 15530, and Cisco ONS 15540

Cisco IOS ED Release	Type of ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(30)S1	Rebuild	No new software features.	No new hardware features.	11/17/05
12.2(30)S	Maintenance[1]	No new software features.	No new hardware features.	07/29/05
12.2(25)S15	Rebuild	No new software features.	No new hardware features.	12/06/07
12.2(25)S14	Rebuild	No new software features.	No new hardware features.	08/28/07
12.2(25)S13	Rebuild	No new software features.	No new hardware features.	06/25/07
12.2(25)S12	Rebuild	No new software features.	No new hardware features.	02/09/07

Table 1 Early Deployment Releases for the Cisco 7200 Series, Cisco 7301, Cisco 7304, Cisco 7400 Series, Cisco 7500 Series, Cisco ONS 15530, and Cisco ONS 15540 (continued)

Cisco IOS ED Release	Type of ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(25)S11	Rebuild	No new software features.	No new hardware features.	10/20/06
12.2(25)S10	Rebuild	No new software features.	No new hardware features.	07/10/06
12.2(25)S9	Rebuild	No new software features.	No new hardware features.	03/30/06
12.2(25)S8	Rebuild	No new software features.	No new hardware features.	01/10/06
12.2(25)S7	Rebuild	No new software features.	No new hardware features.	10/31/05
12.2(25)S6	Rebuild	No new software features.	No new hardware features.	10/24/05
12.2(25)S5	Rebuild	No new software features.	No new hardware features.	06/23/05
12.2(25)S4	Rebuild	No new software features.	No new hardware features.	04/13/05
12.2(25)S3	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(25)S3" section on page 34.	See the "New Hardware Features in Cisco IOS Release 12.2(25)S3" section on page 33.	03/07/05
12.2(25)S2	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(25)S2" section on page 34.	No new hardware features.	12/30/04
12.2(25)S1	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(25)S1" section on page 37.	No new hardware features.	10/14/04
12.2(25)S	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(25)S" section on page 38.	See the "New Hardware Features in Cisco IOS Release 12.2(25)S" section on page 38.	08/16/04
12.2(22)S2	Rebuild	No new software features.	No new hardware features.	08/26/04
12.2(22)S1	Rebuild	No new software features.	No new hardware features.	06/24/04
12.2(22)S	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(22)S" section on page 57.	See the "New Hardware Features in Cisco IOS Release 12.2(22)S" section on page 56.	03/18/04
12.2(20)S14	Rebuild	No new software features.	No new hardware features.	08/03/07
12.2(20)S13	Rebuild	No new software features.	No new hardware features.	03/27/07
12.2(20)S12	Rebuild	No new software features.	No new hardware features.	06/30/06
12.2(20)S11	Rebuild	No new software features.	No new hardware features.	04/27/06
12.2(20)S10	Rebuild	No new software features.	No new hardware features.	12/29/05
12.2(20)S9	Rebuild	No new software features.	No new hardware features.	09/19/05
12.2(20)S8	Rebuild	No new software features.	No new hardware features.	05/13/05
12.2(20)S7	Rebuild	No new software features.	No new hardware features.	03/04/05
12.2(20)S6	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(20)S6" section on page 58.	No new hardware features.	11/01/04
12.2(20)S5	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(20)S5" section on page 59.	No new hardware features.	08/11/04

Table 1 Early Deployment Releases for the Cisco 7200 Series, Cisco 7301, Cisco 7304, Cisco 7400 Series, Cisco 7500 Series, Cisco ONS 15530, and Cisco ONS 15540 (continued)

Cisco IOS ED Release	Type of ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(20)S4	Rebuild	No new software features.	No new hardware features.	06/28/04
12.2(20)S3	Rebuild	See the "New Software Features in Cisco IOS Release 12.2(20)S3" section on page 60.	See the "New Hardware Features in Cisco IOS Release 12.2(20)S3" section on page 60.	05/21/04
12.2(20)S2	Rebuild	No new software features.	See the "New Hardware Features in Cisco IOS Release 12.2(20)S2" section on page 61.	03/16/04
12.2(20)S1	Rebuild	No new software features.	No new hardware features.	01/21/04
12.2(20)S	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(20)S" section on page 63.	No new hardware features.	10/29/03
12.2(18)S13	Rebuild	No new software features.	No new hardware features.	08/01/07
12.2(18)S12	Rebuild	No new software features.	No new hardware features.	06/22/06
12.2(18)S11	Rebuild	No new software features.	No new hardware features.	02/09/06
12.2(18)S10	Rebuild	No new software features.	No new hardware features.	09/29/05
12.2(18)S9	Rebuild	No new software features.	No new hardware features.	04/19/05
12.2(18)S8	Rebuild	No new software features.	No new hardware features.	02/24/05
12.2(18)S7	Rebuild	No new software features.	No new hardware features.	12/09/04
12.2(18)S6	Rebuild	No new software features.	No new hardware features.	09/10/04
12.2(18)S5	Rebuild	No new software features.	No new hardware features.	05/24/04
12.2(18)S4	Rebuild	No new software features.	No new hardware features.	03/22/04
12.2(18)S3	Rebuild	No new software features.	No new hardware features.	01/26/04
12.2(18)S2	Rebuild	No new software features.	No new hardware features.	12/05/03
12.2(18)S1	Rebuild	No new software features.	No new hardware features.	10/09/03
12.2(18)S	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(18)S" section on page 69.	See the "New Hardware Features in Cisco IOS Release 12.2(18)S" section on page 68.	08/21/03
12.2(14)S19	Rebuild	No new software features.	No new hardware features.	07/26/07
12.2(14)S18	Rebuild	No new software features.	No new hardware features.	05/29/07
12.2(14)S17	Rebuild	No new software features.	No new hardware features.	05/18/06
12.2(14)S16	Rebuild	No new software features.	No new hardware features.	01/30/06
12.2(14)S15	Rebuild	No new software features.	No new hardware features.	09/20/05
12.2(14)S14	Rebuild	No new software features.	No new hardware features.	04/13/05
12.2(14)S13	Rebuild	No new software features.	No new hardware features.	02/17/05
12.2(14)S12	Rebuild	No new software features.	No new hardware features.	11/16/04
12.2(14)S10	Rebuild	No new software features.	No new hardware features.	08/09/04
12.2(14)S9	Rebuild	No new software features.	No new hardware features.	05/17/04

Table 1 Early Deployment Releases for the Cisco 7200 Series, Cisco 7301, Cisco 7304, Cisco 7400 Series, Cisco 7500 Series, Cisco ONS 15530, and Cisco ONS 15540 (continued)

Cisco IOS ED Release	Type of ED Release	Additional Software Features	Additional Hardware Features	Availability
12.2(14)S7	Rebuild	No new software features.	No new hardware features.	03/08/04
12.2(14)S5	Rebuild	No new software features.	No new hardware features.	09/29/03
12.2(14)S3	Rebuild	No new software features.	No new hardware features.	07/10/03
12.2(14)S2	Rebuild	No new software features.	No new hardware features.	06/03/03
12.2(14)S1	Rebuild	No new software features.	No new hardware features.	04/10/03
12.2(14)S	Maintenance	See the "New Software Features in Cisco IOS Release 12.2(14)S" section on page 89.	See the "New Hardware Features in Cisco IOS Release 12.2(14)S" section on page 84.	01/30/03

1. Cisco IOS Release 12.0(30)S is the last maintenance release of Release 12.2S.

System Requirements

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

- Memory Recommendations, page 5
- Supported Hardware, page 6
- Determining the Software Version, page 12
- Upgrading to a New Software Release, page 13
- Microcode Software, page 13
- Feature Support, page 30

Memory Recommendations

The memory recommendation tables have been removed from the Cisco IOS Release 12.2S 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 and Catalyst OS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

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

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

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

http://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 12.2S, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Search by 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 and port adapters that are supported in Cisco IOS Release 12.2S.

Supported Platforms

Cisco IOS Release 12.2S supports the following platforms:

- Cisco 7200 series routers (including the Cisco 7202, Cisco 7204, Cisco 7204VXR, Cisco 7206, and Cisco 7206VXR routers)
- Cisco 7301 router
- Cisco 7304 routers (including the 7304-NSE-100 and Cisco 7304-NPE-G100 routers)
- Cisco 7400 series routers (including the Cisco 7401 ASR-BB and Cisco 7401 ASR-CP routers)
- Cisco 7500 series routers (including the Cisco 7505, Cisco 7507, and Cisco 7513 routers)
- Cisco ONS 15530 DWDM Multiservice Aggregation Platform
- Cisco ONS 15540 Extended Services Platform (ESP) (including the Cisco ONS 15540 ESP and Cisco ONS 15540 ESPx platforms)

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 32.

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

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

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

Table 2 Supported Platforms for Cisco IOS Release 12.2S

Cisco IOS Release	Cisco 7200 Series	Cisco 7301 Router	Cisco 7304 Routers	Cisco 7400 Series	Cisco 7500 Series	Cisco ONS 15530	Cisco ONS 15540
12.2(30)S1	No	No	No	No	No	Yes	Yes
12.2(30)S	No	No	No	No	No	Yes	Yes
12.2(25)S15	Yes	Yes	Yes	No	Yes	No	No
12.2(25)S14	Yes	Yes	Yes	No	Yes	No	No
12.2(25)S13	Yes	Yes	Yes	No	Yes	No	No
12.2(25)S12	Yes	Yes	Yes	No	Yes	No	No
12.2(25)S11	Yes	Yes	Yes	No	Yes	No	No
12.2(25)S10	Yes	Yes	Yes	No	Yes	No	No
12.2(25)S9	Yes	Yes	Yes	No	Yes	No	No
12.2(25)S8	Yes	Yes	Yes	No	Yes	No	No
12.2(25)S7	Yes	Yes	Yes	No	Yes	Yes	Yes
12.2(25)S6	Yes	Yes	Yes	No	Yes	Yes	Yes
12.2(25)S5	Yes	Yes	Yes	No	Yes	Yes	Yes
12.2(25)S4	Yes	Yes	Yes	No	Yes	Yes	Yes
12.2(25)S3	Yes	Yes	Yes	No	Yes	Yes	Yes
12.2(25)S2	Yes	Yes	Yes	No	Yes	Yes	Yes
12.2(25)S1	Yes	Yes	No	No	Yes	Yes	Yes
12.2(25)S	Yes	Yes	No	No	Yes	Yes	Yes
12.2(22)S2	No	No	No	No	No	Yes	Yes
12.2(22)S1	No	No	No	No	No	Yes	Yes
12.2(22)S	No	No	No	No	No	Yes	Yes
12.2(20)S14	No	No	Yes	No	No	No	No
12.2(20)S13	No	No	Yes	No	No	No	No
12.2(20)S12	No	No	Yes	No	No	No	No
12.2(20)S11	No	No	Yes	No	No	No	No
12.2(20)S10	No	No	Yes	No	No	No	No
12.2(20)S9	No	No	Yes	No	No	No	No
12.2(20)S8	No	No	Yes	No	No	No	No

Table 2 Supported Platforms for Cisco IOS Release 12.2S (continued)

Cisco IOS Release	Cisco 7200 Series	Cisco 7301 Router	Cisco 7304 Routers	Cisco 7400 Series	Cisco 7500 Series	Cisco ONS 15530	Cisco ONS 15540
12.2(20)S7	No	No	Yes	No	No	No	No
12.2(20)S6	No	No	Yes	No	No	No	No
12.2(20)S5	No	No	Yes	No	No	No	No
12.2(20)S4	No	No	Yes	No	No	No	No
12.2(20)S3	No	No	Yes	No	No	No	No
12.2(20)S2	No	No	Yes	No	No	No	No
12.2(20)S1	No	No	Yes	No	No	No	No
12.2(20)S	No	No	Yes	No	No	No	No
12.2(18)S13	Yes	Yes	No	No	Yes	No	No
12.2(18)S12	Yes	Yes	No	No	Yes	No	No
12.2(18)S11	Yes	Yes	No	No	Yes	No	No
12.2(18)S10	Yes	Yes	No	No	Yes	No	No
12.2(18)S9	Yes	Yes	No	No	Yes	No	No
12.2(18)S8	Yes	Yes	No	No	Yes	No	No
12.2(18)S7	Yes	Yes	No	No	Yes	No	No
12.2(18)S6	Yes	Yes	No	No	Yes	No	No
12.2(18)S5	Yes	Yes	No	No	Yes	No	No
12.2(18)S4	Yes	Yes	No	No	Yes	No	No
12.2(18)S3	Yes	Yes	No	No	Yes	No	No
12.2(18)S2	Yes	Yes	No	No	Yes	No	No
12.2(18)S1	Yes	Yes	No	No	Yes	No	No
12.2(18)S	Yes	Yes	Yes	No	Yes	No	No
12.2(14)S19	Yes	No	No	No	Yes	No	No
12.2(14)S18	Yes	No	No	No	Yes	No	No
12.2(14)S17	Yes	No	No	No	Yes	No	No
12.2(14)S16	Yes	No	No	No	Yes	No	No
12.2(14)S15	Yes	No	No	Yes	Yes	No	No
12.2(14)S14	Yes	No	No	Yes	Yes	No	No
12.2(14)S13	Yes	No	No	Yes	Yes	No	No
12.2(14)S12	Yes	No	No	Yes	Yes	No	No
12.2(14)S10	Yes	No	No	Yes	Yes	No	No
12.2(14)S9	Yes	No	No	Yes	Yes	No	No
12.2(14)S7	Yes	No	No	Yes	Yes	No	No
12.2(14)S5	Yes	No	No	Yes	Yes	No	No
12.2(14)S3	Yes	No	No	Yes	Yes	No	No

Table 2 Supported Platforms for Cisco IOS Release 12.2S (continued)

Cisco IOS Release	Cisco 7200 Series	Cisco 7301 Router	Cisco 7304 Routers	Cisco 7400 Series	Cisco 7500 Series	Cisco ONS 15530	Cisco ONS 15540
12.2(14)S2	Yes	No	No	Yes	Yes	No	No
12.2(14)S1	Yes	No	No	Yes	Yes	No	No
12.2(14)S	Yes	No	No	Yes	Yes	No	No

Supported Port Adapters

Table 3 lists the port adapters that are supported for the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 router, Cisco 7400 series routers, and Cisco 7500 series routers in Cisco IOS Release 12.2S up to and including Cisco IOS Release 12.2(30)S1 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 12.2S release in which the port adapter was introduced. For example, (14) means that a port adapter was introduced in Cisco IOS Release 12.2(14)S. If a cell in this column contains an em dash (—), support for the port adapter was inherited from Cisco IOS Release 12.2 or from another release and was included in the initial base release of Cisco IOS Release 12.2S.

Table 3 Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, Cisco 7304, Cisco 7400 Series, and Cisco 7500 Series

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7304 Router	7400 Series	7500 Series
ATM Port Adapters							
PA-A1-OC3SM	1-port ATM OC3 single mode (IR)	—	No	No	No	No	Yes
PA-A1-OC3MM	1-port ATM OC3 multimode	—	No	No	No	No	Yes
PA-A2-4T1C-OC3SM=	ATM CES, 4 T1 CES ports, 1 OC3 ATM SM port	—	Yes	No	No	No	No
PA-A2-4T1C-T3ATM=	ATM CES, 4 T1 CES ports, 1 T3 ATM port	—	Yes	No	No	No	No
PA-A2-4E1XC-OC3SM=	CES OC3, 4 E1 ports, 120 ohms	—	Yes	No	No	No	No
PA-A2-4E1XC-E3ATM=	CES E3/E1, 120 ohms	—	Yes	No	No	No	No
PA-A3-OC3MM	1-port ATM Enhanced OC3c/STM1 multimode	—	Yes	Yes	Yes	Yes	Yes
PA-A3-OC3SMI	1-port ATM Enhanced OC3c/STM1 single mode (IR)	—	Yes	Yes	Yes	Yes	Yes
PA-A3-OC3SML	1-port ATM Enhanced OC3c/STM1 single mode (LR)	—	Yes	Yes	Yes	Yes	Yes
PA-A3-OC12MM	1-port ATM Enhanced OC12/STM4 multimode	—	No	No	No	No	Yes
PA-A3-OC12SMI	1-port ATM Enhanced OC12/STM4 single mode (IR)	—	No	No	No	No	Yes
PA-A3-E3	1-port ATM Enhanced E3	—	Yes	Yes	Yes	Yes	Yes

Table 3 Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, Cisco 7304, Cisco 7400 Series, and Cisco 7500 Series (continued)

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7304 Router	7400 Series	7500 Series
PA-A3-T3	1-port ATM Enhanced DS3	—	Yes	Yes	Yes	Yes	Yes
PA-A3-8E1IMA	8-port ATM Inverse Mux E1, 120 ohms	—	Yes	Yes	Yes	Yes	Yes
PA-A3-8T1IMA	8-port ATM Inverse Mux T1	—	Yes	Yes	Yes	Yes	Yes
Channel Port Adapters							
PA-4C-E=	1-port Enhanced ESCON Channel	—	Yes	No	No	No	No
Dynamic Packet Transport (DPT) Port Adapters							
PA-SRP-OC12MM=	DPT-OC12 multimode (Cisco 7200 series only)	—	Yes	No	No	No	No
PA-SRP-OC12SMI=	DPT-OC12 single mode (IR) (Cisco 7200 series only)	—	Yes	No	No	No	No
PA-SRP-OC12SML=	DPT-OC12 single mode (LR) (Cisco 7200 series only)	—	Yes	No	No	No	No
PA-SRP-OC12SMX=	DPT-OC12 single mode extended reach (Cisco 7200 series only)	—	Yes	No	No	No	No
SRPIP-OC12MM=	DPT-OC12 multimode (Cisco 7500 series only)	—	No	No	No	No	Yes
SRPIP-OC12SMI=	DPT-OC12 single mode (IR) (Cisco 7500 series only)	—	No	No	No	No	Yes
SRPIP-OC12SML=	DPT-OC12 single mode (LR) (Cisco 7500 series only)	—	No	No	No	No	Yes
SRPIP-OC12SMX=	DPT-OC12 single mode extended reach (Cisco 7500 series only)	—	No	No	No	No	Yes
Ethernet/Fast Ethernet/Gigabit Ethernet Port Adapters							
PA-4E	4-port Ethernet 10BASE-T	—	Yes	Yes	Yes	Yes	Yes
PA-4E1G/75	4-port E1 G.703 Serial, 75 ohms/unbalanced	—	Yes	Yes	Yes	Yes	Yes
PA-4E1G/120	4-port E1 G.703 Serial, 120 ohms/balanced	—	Yes	Yes	Yes	Yes	Yes
PA-5EFL	5-port Ethernet 10BASE-FL	—	Yes	Yes	No	Yes	Yes
PA-8E	8-port Ethernet 10BASE-T	—	Yes	Yes	Yes	Yes	Yes
PA-FE-FX	1-port Fast Ethernet 100BASE-FX	—	Yes	Yes	Yes	Yes	Yes
PA-FE-TX	1-port Fast Ethernet 100BASE-TX	—	Yes	Yes	Yes	Yes	Yes
PA-2FE-FX	2-port Fast Ethernet 100BASE-FX	—	Yes	Yes	Yes	Yes	Yes
PA-2FE-TX	2-port Fast Ethernet 100BASE-TX	—	Yes	Yes	Yes	Yes	Yes
PA-GE	1-port Gigabit Ethernet	—	Yes	No	Yes	Yes	No
FDDI Port Adapters							
PA-F/FD-MM	1-port FDDI Full Duplex multimode	—	Yes[2]	No	No	No	Yes
PA-F/FD-SM	1-port FDDI Full Duplex single mode	—	Yes[2]	No	No	No	Yes

Table 3 Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, Cisco 7304, Cisco 7400 Series, and Cisco 7500 Series (continued)

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7304 Router	7400 Series	7500 Series
High-Speed Serial Port Adapters							
PA-H	1-port High-Speed Serial Interface (HSSI)	—	Yes	Yes	Yes	Yes	Yes
PA-2H	2-port High-Speed Serial Interface (HSSI)	—	Yes	Yes	Yes	Yes	Yes
Multichannel Serial Port Adapters							
PA-MC-T3	1-port multichannel T3	—	Yes	Yes	Yes	Yes	Yes
PA-MC-E3	1-port multichannel E3	—	Yes	Yes	Yes	Yes	Yes
PA-MC-2T3+	2-port multichannel T3	—	Yes	Yes	Yes	Yes	Yes
PA-MC-2T1	2-port multichannel T1, integrated CSU/DSUs	—	Yes	Yes	Yes	Yes	Yes
PA-MC-2E1/120	2-port multichannel E1, G.703 120-ohm interface	—	Yes	Yes	Yes	Yes	Yes
PA-MC-4T1	4-port multichannel T1, integrated CSU/DSUs	—	Yes	Yes	Yes	Yes	Yes
PA-MC-8T1	8-port multichannel T1, integrated CSU/DSUs	—	Yes	Yes	Yes	Yes	Yes
PA-MC-8E1/120	8-port multichannel E1, G.703 120-ohm interface	—	Yes	No	Yes	Yes	Yes
PA-MC-8TE1+	8-port multichannel T1/E1 8PRI	(14)	Yes	Yes	Yes	Yes	Yes
PA-MC-STM-1MM	1-port multichannel STM-1 multimode	(14)	Yes	Yes	Yes	Yes	Yes
PA-MC-STM-1SMI	1-port multichannel STM-1 single mode	(14)	Yes	Yes	Yes	Yes	Yes
PA-4B-U	4-port BRI, U Interface	—	Yes	Yes	No	Yes	No
PA-8B-S/T	8-port BRI, S/T Interface	—	Yes	Yes	No	Yes	No
Service Adapters							
SA-ENCRYPT=	Encryption Service Adapter	—	No	No	No	No	Yes
SA-ISA	Integrated Services Adapter for IPSec or MPPE encryption	(14)	Yes	No	No	No	No
Shared Port Adapters (SPAs)							
SPA-4FE-7304	4-port 10/100 Fast Ethernet SPA	(20)S2	No	No	Yes	No	No
SPA-2GE-7304	2-port 10/100/1000 Gigabit Ethernet SPA	(20)S2	No	No	Yes	No	No
SPA-2XOC3-POS	2-port OC-3c/STM-1 POS SPA	(25)S3	No	No	Yes	No	No
SPA-4XOC3-POS	4-port OC-3c/STM-1 POS SPA	(25)S3	No	No	Yes	No	No
SPA-1OC12-POS	1-port OC-12c/STM-4 POS SPA	(25)S3	No	No	Yes	No	No
SPA-2XT3/E3	2-port T3/E3 Serial SPA	(25)S3	No	No	Yes	No	No
SPA-4XT3/E3	4-port T3/E3 Serial SPA	(25)S3	No	No	Yes	No	No
SONET Port Adapters							
PA-POS-OC3MM	1-port Packet over SONET OC3c/STM1 multimode	—	Yes	Yes	Yes	Yes	Yes

Table 3 Supported Port Adapters for the Cisco 7200 Series, Cisco 7301, Cisco 7304, Cisco 7400 Series, and Cisco 7500 Series (continued)

Cisco Product Number[1]	Adapter Description	In	7200 Series	7301 Router	7304 Router	7400 Series	7500 Series
PA-POS-OC3SMI	1-port Packet over SONET OC3c/STM1 single mode (IR)	—	Yes	Yes	Yes	Yes	Yes
PA-POS-OC3SML	1-port Packet over SONET OC3c/STM1 single mode (LR)	—	Yes	Yes	Yes	Yes	Yes
PA-POS-2OC3	2-port OC-3/STM-1 POS with APS	(18)	Yes	Yes	Yes	Yes	Yes
T1/E1 Port Adapters							
PA-4T+	4-port Serial, Enhanced	—	Yes	Yes	Yes	Yes	Yes
PA-8T-V35	8-port Serial, V.35	—	Yes	Yes	Yes	Yes	Yes
PA-8T-X21	8-port Serial, X.21	—	Yes	Yes	Yes	Yes	Yes
PA-8T-232	8-port Serial, 232	—	Yes	Yes	Yes	Yes	Yes
T3/E3 Port Adapters							
PA-T3	1-port T3 Serial, T3 DSUs	—	Yes	Yes	Yes	Yes	Yes
PA-T3+	1-port T3 Serial, Enhanced	—	Yes	Yes	Yes	Yes	Yes
PA-2T3	2-port T3 Serial, T3 DSUs	—	Yes	Yes	Yes	Yes	Yes
PA-2T3+	2-port T3 Serial, Enhanced	—	Yes	Yes	Yes	Yes	Yes
PA-E3	1-port E3 Serial, E3 DSUs	—	Yes	Yes	Yes	Yes	Yes
PA-2E3	2-port E3 Serial, E3 DSUs	—	Yes	Yes	Yes	Yes	Yes
Token Ring Port Adapters							
PA-4R-DTR	4-port Dedicated Token Ring, 4/16Mbps, HDX/FDX	—	Yes	No	No	No	Yes

1. For a spare product number, append an equal sign (=) to the product number. If a product number is listed as a spare product, only a spare product is available. For End-of-Sale (EOS) and End-of-Life (EOL) information about port adapters, refer to the Cisco product bulletins at the following locations:
   Cisco 7200 series: http://www.cisco.com/en/US/products/hw/routers/ps341/prod_eol_notices_list.html
   Cisco 7300 series: http://www.cisco.com/en/US/products/hw/routers/ps352/prod_eol_notices_list.html
   Cisco 7400 series: http://www.cisco.com/en/US/products/hw/routers/ps354/prod_eol_notices_list.html
   Cisco 7500 series: http://www.cisco.com/en/US/products/hw/routers/ps359/prod_eol_notices_list.html
2. The FDDI port adapters are supported on non-VXR routers.

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

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

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) 7500 Software (rsp-jsv-mz), Version 12.2(25)S, EARLY DEPLOYMENT RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

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

For information about upgrading to a new software release, see the appropriate platform-specific document:

- Cisco 7200 series, Cisco 7301, Cisco 7304, Cisco 7400 series, and Cisco 7500 series:

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

- Cisco ONS 15530 DWDM Multiservice Aggregation Platform:

  http://www.cisco.com/en/US/products/hw/optical/ps2011/ps4002/index.html

- Cisco ONS 15540 ESP Extended Services Platform:

  http://www.cisco.com/en/US/products/hw/optical/ps2011/ps2014/index.html

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

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

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

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

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

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

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

Microcode Software

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

- Bundled FPGAs for the Cisco 7304, page 13
- Shared Port Adapter FPD Image Packages for the Cisco 7304, page 23

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 at the following location:

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(25)S15

There are no new FPGA images for Cisco IOS Release 12.2(25)S15. All Cisco IOS Release 12.2(25)S15 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S9.

Bundled FPGAs for Cisco IOS Release 12.2(25)S14

There are no new FPGA images for Cisco IOS Release 12.2(25)S14. All Cisco IOS Release 12.2(25)S14 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S9.

Bundled FPGAs for Cisco IOS Release 12.2(25)S13

There are no new FPGA images for Cisco IOS Release 12.2(25)S13. All Cisco IOS Release 12.2(25)S13 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S9.

Bundled FPGAs for Cisco IOS Release 12.2(25)S12

There are no new FPGA images for Cisco IOS Release 12.2(25)S12. All Cisco IOS Release 12.2(25)S12 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S9.

Bundled FPGAs for Cisco IOS Release 12.2(25)S11

There are no new FPGA images for Cisco IOS Release 12.2(25)S11. All Cisco IOS Release 12.2(25)S11 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S9.

Bundled FPGAs for Cisco IOS Release 12.2(25)S10

There are no new FPGA images for Cisco IOS Release 12.2(25)S10. All Cisco IOS Release 12.2(25)S10 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S9.

Bundled FPGAs for Cisco IOS Release 12.2(25)S9

All Cisco IOS Release 12.2(25)S9 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(25)S9 Sorted by Hardware Type

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

Bundled FPGAs for Cisco IOS Release 12.2(25)S8

All Cisco IOS Release 12.2(25)S8 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(25)S8 Sorted by Hardware Type

FPGA Image	Hardware Type	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
NSE-100 Motherboard FPGA	0x0001	1.07	2.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.07	4.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.08	5.00	15
NSE-100 Daughterboard FPGA	0x0002	1.07	0.00	6
NSE-100 Daughterboard FPGA	0x0002	1.08	5.00	6
OC-48 POS line card FPGA	0x0003	0.16	2.00	5
OC-3 POS line card FPGA	0x0004	0.22	2.00	8
6E3 line card FPGA	0x0005	0.21	2.00	12
6T3 line card FPGA	0x0005	0.21	2.00	12
OC-12 POS line card FPGA	0x0006	0.20	1.00	12
OC-3 ATM line card FPGA	0x0007	0.19	2.00	8

Table 5 Bundled FPGA Versions for Cisco IOS Release 12.2(25)S8 Sorted by Hardware Type

FPGA Image	Hardware Type	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
OC-12 ATM line card FPGA	0x0007	0.19	2.00	8
CC-PA line card FPGA	0x0008	1.40	1.01	8
NPE-G100 FPGA (PS)	0x000A	2.05	0.30	12
NPE-G100 FPGA (ES)	0x000A	2.05	0.20	12
MSC-100 FPGA	0x000D	0.27	0.10	22

Bundled FPGAs for Cisco IOS Release 12.2(25)S7

There are no new FPGA images for Cisco IOS Release 12.2(25)S7. All Cisco IOS Release 12.2(25)S7 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S3.

Bundled FPGAs for Cisco IOS Release 12.2(25)S6

There are no new FPGA images for Cisco IOS Release 12.2(25)S6. All Cisco IOS Release 12.2(25)S6 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S3.

Bundled FPGAs for Cisco IOS Release 12.2(25)S5

There are no new FPGA images for Cisco IOS Release 12.2(25)S5. All Cisco IOS Release 12.2(25)S5 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S3.

Bundled FPGAs for Cisco IOS Release 12.2(25)S4

There are no new FPGA images for Cisco IOS Release 12.2(25)S4. All Cisco IOS Release 12.2(25)S4 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(25)S3.

Bundled FPGAs for Cisco IOS Release 12.2(25)S3

All Cisco IOS Release 12.2(25)S3 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(25)S3

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

Table 6 Bundled FPGA Versions for Cisco IOS Release 12.2(25)S3 (continued)

FPGA Image	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
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
CC-PA line card FPGA	1.30	1.01	8

Bundled FPGAs for Cisco IOS Release 12.2(25)S2

All Cisco IOS Release 12.2(25)S2 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 7.

Table 7 Bundled FPGA Versions for Cisco IOS Release 12.2(25)S2

FPGA Image	Hardware Version	FPGA Version Bundled	Approx. Upgrade Time in Minutes
6E3 line card FPGA	—	0.21	12
6T3 line card FPGA	—	0.21	12
NPE-G100 FPGA	—	2.05	12
OC-12 POS line card FPGA	—	0.20	12
OC-3 ATM line card FPGA	—	0.18	8
OC-3 POS line card FPGA	—	0.22	8
OC-48 POS line card FPGA	—	0.16	5
NSE-100 Daughterboard FPGA	3.0 or lower	1.07	6
	5.0 or higher	1.08	6
NSE-100 Motherboard FPGA	3.0 or lower	1.07	15
	5.0 or higher	1.08	15
CC-PA line card FPGA	—	1.30	8
MSC-100 FPGA	—	0.24	22

Bundled FPGAs for Cisco IOS Release 12.2(20)S14

There are no new FPGA images for Cisco IOS Release 12.2(20)S14. All Cisco IOS Release 12.2(20)S14 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(20)S11.

Bundled FPGAs for Cisco IOS Release 12.2(20)S13

There are no new FPGA images for Cisco IOS Release 12.2(20)S13. All Cisco IOS Release 12.2(20)S13 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(20)S11.

Bundled FPGAs for Cisco IOS Release 12.2(20)S12

There are no new FPGA images for Cisco IOS Release 12.2(20)S12. All Cisco IOS Release 12.2(20)S12 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(20)S11.

Bundled FPGAs for Cisco IOS Release 12.2(20)S11

All Cisco IOS Release 12.2(20)S11 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 8.

Table 8 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S11

FPGA Image	Hardware Type	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
6E3 line card FPGA	0x0005	0.21	2.00	12
6T3 line card FPGA	0x0005	0.21	2.00	12
NPE-G100 FPGA (PS)	0x000A	2.05	0.30	12
NPE-G100 FPGA (ES)	0x000A	2.05	0.20	12
OC-12 POS line card FPGA	0x0006	0.20	1.00	12
OC-3 ATM line card FPGA	0x0007	0.19	2.00	8
OC-3 POS line card FPGA	0x0004	0.22	2.00	8
OC-48 POS line card FPGA	0x0003	0.15	2.00	5
NSE-100 Daughterboard FPGA	0x0002	1.07	0.00	6
NSE-100 Daughterboard FPGA	0x0002	1.08	5.00	6
NSE-100 Motherboard FPGA	0x0001	1.10	2.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.13	4.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.14	5.00	15
CC-PA line card FPGA	0x0008	1.40	1.01	8
MSC-100 FPGA	0x000D	0.27	0.10	22

Bundled FPGAs for Cisco IOS Release 12.2(20)S10

All Cisco IOS Release 12.2(20)S10 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 9.

Table 9 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S10

FPGA Image	Hardware Type	FPGA Version Bundled	Minimum Required Hardware Version	Approx. Upgrade Time in Minutes
6E3 line card FPGA	0x0005	0.21	2.00	12
6T3 line card FPGA	0x0005	0.21	2.00	12
NPE-G100 FPGA (PS)	0x000A	2.05	0.30	12
NPE-G100 FPGA (ES)	0x000A	2.05	0.20	12
OC-12 POS line card FPGA	0x0006	0.20	1.00	12
OC-3 ATM line card FPGA	0x0007	0.19	2.00	8
OC-3 POS line card FPGA	0x0004	0.22	2.00	8
OC-48 POS line card FPGA	0x0003	0.15	2.00	5
NSE-100 Daughterboard FPGA	0x0002	1.07	0.00	6
NSE-100 Daughterboard FPGA	0x0002	1.08	5.00	6
NSE-100 Motherboard FPGA	0x0001	1.07	2.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.07	4.00	15
NSE-100-CR Motherboard FPGA	0x0001	1.08	5.00	15
CC-PA line card FPGA	0x0008	1.40	1.01	8
MSC-100 FPGA	0x000D	0.27	0.10	22

Bundled FPGAs for Cisco IOS Release 12.2(20)S9

There are no new FPGA images for Cisco IOS Release 12.2(20)S9. All Cisco IOS Release 12.2(20)S9 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(20)S8.

Bundled FPGAs for Cisco IOS Release 12.2(20)S8

All Cisco IOS Release 12.2(20)S8 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 10.

Table 10 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S8

FPGA Image	FPGA Version Bundled	Approx. Upgrade Time in Minutes
6E3 line card FPGA	0.21	12
6T3 line card FPGA	0.21	12
NPE-G100 FPGA	2.05	12
OC-12 POS line card FPGA	0.20	12
OC-3 ATM line card FPGA	0.19	8
OC-3 POS line card FPGA	0.22	8
OC-48 POS line card FPGA	0.15	5
NSE-100 Daughterboard FPGA	1.08	6

Table 10 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S8 (continued)

FPGA Image	FPGA Version Bundled	Approx. Upgrade Time in Minutes
NSE-100 Motherboard FPGA	1.08	15
CC-PA line card FPGA	1.30	8
MSC-100 FPGA	0.27	22

Bundled FPGAs for Cisco IOS Release 12.2(20)S7

All Cisco IOS Release 12.2(20)S7 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 11.

Table 11 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S7

FPGA Image	FPGA Version Bundled	Approx. Upgrade Time in Minutes
6E3 line card FPGA	0.21	12
6T3 line card FPGA	0.21	12
NPE-G100 FPGA	2.05	12
OC-12 POS line card FPGA	0.20	12
OC-3 ATM line card FPGA	0.19	8
OC-3 POS line card FPGA	0.22	8
OC-48 POS line card FPGA	0.15	5
NSE-100 Daughterboard FPGA	1.08	6
NSE-100 Motherboard FPGA	1.08	15
CC-PA line card FPGA	1.30	8
MSC-100 FPGA	0.24	22

Bundled FPGAs for Cisco IOS Release 12.2(20)S6

All Cisco IOS Release 12.2(20)S6 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 12.

Table 12 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S6

FPGA Image	FPGA Version Bundled	Approx. Upgrade Time in Minutes
6E3 line card FPGA	0.21	12
6T3 line card FPGA	0.21	12
NPE-G100 FPGA	2.05	12
OC-12 POS line card FPGA	0.20	12
OC-3 ATM line card FPGA	0.18	8
OC-3 POS line card FPGA	0.22	8

Table 12 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S6 (continued)

FPGA Image	FPGA Version Bundled	Approx. Upgrade Time in Minutes
OC-48 POS line card FPGA	0.15	5
NSE-100 Daughterboard FPGA	1.08	6
NSE-100 Motherboard FPGA	1.08	15
CC-PA line card FPGA	1.30	8
MSC-100 FPGA	0.24	22

Bundled FPGAs for Cisco IOS Release 12.2(20)S5

All Cisco IOS Release 12.2(20)S5 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 13.

Table 13 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S5

FPGA Image	FPGA Version Bundled
6E3 line card FPGA	0.20
6T3 line card FPGA	0.20
NPE-G100 FPGA	2.05
OC-12 POS line card FPGA	0.20
OC-3 ATM line card FPGA	0.18
OC-3 POS line card FPGA	0.22
OC-48 POS line card FPGA	0.15
NSE-100 Daughterboard FPGA	1.08
NSE-100 Motherboard FPGA	1.08
CC-PA line card FPGA	1.30
MSC-100 FPGA	0.24

Bundled FPGAs for Cisco IOS Release 12.2(20)S4

There are no new FPGA images for Cisco IOS Release 12.2(20)S4. All Cisco IOS Release 12.2(20)S4 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(20)S3.

Bundled FPGAs for Cisco IOS Release 12.2(20)S3

All Cisco IOS Release 12.2(20)S3 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 14.

Table 14 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S3

FPGA Image	FPGA Version Bundled
6E3 line card FPGA	0.20
6T3 line card FPGA	0.20

Table 14 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S3 (continued)

FPGA Image	FPGA Version Bundled
NPE-G100 FPGA	2.04
OC-12 POS line card FPGA	0.18
OC-3 ATM line card FPGA	0.18
OC-3 POS line card FPGA	0.20
OC-48 POS line card FPGA	0.15
NSE-100 Daughterboard FPGA	1.07
NSE-100 Motherboard FPGA	1.07
CC-PA line card FPGA	1.20
MSC-100 FPGA	0.23

Bundled FPGAs for Cisco IOS Release 12.2(20)S2

All Cisco IOS Release 12.2(20)S2 software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 15.

Table 15 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S2

FPGA Image	FPGA Version Bundled
6E3 line card FPGA	0.20
6T3 line card FPGA	0.20
NPE-G100 FPGA	2.04
OC-12 POS line card FPGA	0.18
OC-3 ATM line card FPGA	0.18
OC-3 POS line card FPGA	0.20
OC-48 POS line card FPGA	0.15
NSE-100 Daughterboard FPGA	1.07
NSE-100 Motherboard FPGA	1.07
CC-PA line card FPGA	1.11
MSC-100 FPGA	0.23

Bundled FPGAs for Cisco IOS Release 12.2(20)S1

There are no new FPGA images for Cisco IOS Release 12.2(20)S1. All Cisco IOS Release 12.2(20)S1 software images for the Cisco 7304 support the bundled FPGAs that were released in Release 12.2(20)S.

Bundled FPGAs for Cisco IOS Release 12.2(20)S

All Cisco IOS Release 12.2(20)S software images for the Cisco 7304 support the bundled FPGAs that are listed in Table 16.

Table 16 Bundled FPGA Versions for Cisco IOS Release 12.2(20)S

FPGA Image	FPGA Version Bundled
6T3 line card FPGA	0.16
NPE-G100 FPGA	2.03
OC-12 POS line card FPGA	0.18
OC-3 ATM line card FPGA	0.18
OC-3 POS line card FPGA	0.20
OC-48 POS line card FPGA	0.15
NSE-100 Daughterboard FPGA	1.07
NSE-100 Motherboard FPGA	1.07
CC-PA line card FPGA	1.10

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(25)S15

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S15 is the c7304-fpd.122-25.S15.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S14

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S14 is the c7304-fpd.122-25.S14.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S13

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S13 is the c7304-fpd.122-25.S13.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S12

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S12 is the c7304-fpd.122-25.S12.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S11

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S11 is the c7304-fpd.122-25.S11.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S10

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S10 is the c7304-fpd.122-25.S10.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S9

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S9 is the c7304-fpd.122-25.S9.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S8

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S8 is the c7304-fpd.122-25.S8.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S7

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S7 is the c7304-fpd.122-25.S7.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S6

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S6 is the c7304-fpd.122-25.S6.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S5

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S5 is the c7304-fpd.122-25.S5.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S4

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S4 is the c7304-fpd.122-25.S4.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(25)S3.

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S3

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S3 is the c7304-fpd.122-25.S3.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 17 Release 12.2(25)S3 FPD Image Package Contents

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

Table 17 Release 12.2(25)S3 FPD Image Package Contents (continued)

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(25)S2

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(25)S2 is the c7304-fpd.122-25.S2.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 18 Release 12.2(25)S2 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S14

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S14 is the c7304-fpd-pkg.122-20.S14 file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image in the Software Center on Cisco.com.

Table 19 Release 12.2(20)S14 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S13

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S13 is the c7304-fpd-pkg.122-20.S13 file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image in the Software Center on Cisco.com.

Table 20 Release 12.2(20)S13 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S12

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S12 is the c7304-fpd-pkg.122-20.S12 file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image in the Software Center on Cisco.com.

Table 21 Release 12.2(20)S12 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S11

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S11 is the c7304-fpd-pkg.122-20.S11 file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image in the Software Center on Cisco.com.

Table 22 Release 12.2(20)S11 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S10

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S10 is the c7304-fpd-pkg.122-20.S10 file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image in the Software Center on Cisco.com.

Table 23 Release 12.2(20)S10 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S9

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S9 is the c7304-fpd-pkg.122-20.S9 file. This SPA FPD image package file is accessible from the page where you downloaded your specific Cisco IOS image in the Software Center on Cisco.com.

Table 24 Release 12.2(20)S9 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S8

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S8 is the spa-fpd-122-20.S8.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 25 Release 12.2(20)S8 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S7

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S7 is the spa-fpd-122-20.S7.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 26 Release 12.2(20)S7 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S6

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S6 is the spa-fpd-122-20.S6.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 27 Release 12.2(20)S6 FPD Image Package Contents

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

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S5

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S5 is the spa-fpd-122-20.S5.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 28 Release 12.2(20)S5 FPD Image Package Contents

Supported SPAs	FPD ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
7304-4FE-SPA	1	I/O FPGA	4.17	0.0
7304-2GE-SPA	1	I/O FPGA	4.17	0.0

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S4

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S4 is the spa-fpd-122-20.S4.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 29 Release 12.2(20)S4 FPD Image Package Contents

Supported SPAs	FPD ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
7304-4FE-SPA	1	I/O FPGA	4.17	0.0
7304-2GE-SPA	1	I/O FPGA	4.17	0.0

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S3

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S3 is the spa-fpd-122-20.S3.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 30 Release 12.2(20)S3 FPD Image Package Contents

Supported SPAs	FPD ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
7304-4FE-SPA	1	I/O FPGA	4.17	0.0
7304-2GE-SPA	1	I/O FPGA	4.17	0.0

Shared Port Adapter FPD Image Package for Cisco IOS Release 12.2(20)S2

The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(20)S2 is the spa-fpd-122-20.S2.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 31 Release 12.2(20)S2 FPD Image Package Contents

Supported SPAs	FPD ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
7304-4FE-SPA	1	I/O FPGA	4.17	0.0
7304-2GE-SPA	1	I/O FPGA	4.17	0.0

Cisco IOS Release 12.2(20)S2 is the first Cisco IOS Release to support SPAs. Therefore, Cisco IOS Release 12.2(20)S2 is the first Cisco IOS Release to support FPD image packages.

Feature Support

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

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

Note The feature set tables have been removed from the Cisco IOS Release 12.2S 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 and Catalyst OS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

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

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

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

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

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

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

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

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

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

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

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

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

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

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 12.2S, go to the Cisco Feature Navigator home page and perform the following steps.

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

Step 2 In the "Find the features in a specific Cisco IOS release, using one of the following methods:" area, choose **12.2S** 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 12.2S and contains the following subsections:

- New Hardware Features in Cisco IOS Release 12.2(30)S, page 32
- New Software Features in Cisco IOS Release 12.2(30)S, page 33
- New Hardware Features in Cisco IOS Release 12.2(25)S3, page 33
- New Software Features in Cisco IOS Release 12.2(25)S3, page 34
- New Hardware Features in Cisco IOS Release 12.2(25)S2, page 34
- New Software Features in Cisco IOS Release 12.2(25)S2, page 34
- New Hardware Features in Cisco IOS Release 12.2(25)S1, page 37
- New Software Features in Cisco IOS Release 12.2(25)S1, page 37
- New Hardware Features in Cisco IOS Release 12.2(25)S, page 38
- New Software Features in Cisco IOS Release 12.2(25)S, page 38
- New Hardware Features in Cisco IOS Release 12.2(22)S, page 56
- New Software Features in Cisco IOS Release 12.2(22)S, page 57
- New Hardware Features in Cisco IOS Release 12.2(20)S5, page 59
- New Software Features in Cisco IOS Release 12.2(20)S5, page 59
- New Hardware Features in Cisco IOS Release 12.2(20)S3, page 60
- New Software Features in Cisco IOS Release 12.2(20)S3, page 60
- New Hardware Features in Cisco IOS Release 12.2(20)S2, page 61
- New Software Features in Cisco IOS Release 12.2(20)S2, page 63
- New Hardware Features in Cisco IOS Release 12.2(20)S, page 63
- New Software Features in Cisco IOS Release 12.2(20)S, page 63
- New Hardware Features in Cisco IOS Release 12.2(18)S, page 68
- New Software Features in Cisco IOS Release 12.2(18)S, page 69
- New Hardware Features in Cisco IOS Release 12.2(14)S, page 84
- New Software Features in Cisco IOS Release 12.2(14)S, page 89

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

New Hardware Features in Cisco IOS Release 12.2(30)S

There are no new hardware features in Cisco IOS Release 12.2(30)S.

New Software Features in Cisco IOS Release 12.2(30)S

There are no new software features in Cisco IOS Release 12.2(30)S.

New Hardware Features in Cisco IOS Release 12.2(25)S3

This section describes new and changed features in Cisco IOS Release 12.2(25)S3. Some features may be new to Cisco IOS Release 12.2S 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(25)S3. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

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

This release introduces 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

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

This release introduces the 1-port OC-12c/STM-4 POS SPA (SPA-1OC12-POS) shared port adapter (SPA) 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 introduces 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 introduces 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

New Software Features in Cisco IOS Release 12.2(25)S3

This section describes new and changed features in Cisco IOS Release 12.2(25)S3. Some features may be new to Cisco IOS Release 12.2S 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(25)S3. 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.

MPLS VPN: SSO/NSF Support

This feature was introduced in Cisco IOS Release 12.2(25)S. Release 12.2(25)S3 adds support for the Cisco 7304 routers. For detailed information about this feature, see the following Cisco document:

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

New Hardware Features in Cisco IOS Release 12.2(25)S2

There are no new hardware features in Cisco IOS Release 12.2(25)S2.

New Software Features in Cisco IOS Release 12.2(25)S2

This section describes new and changed features in Cisco IOS Release 12.2(25)S2. Some features may be new to Cisco IOS Release 12.2S 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(25)S2. 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.

Any Transport over MPLS for PXF

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 over MPLS (Port and VLAN modes)
- Frame Relay over MPLS
- HDLC over MPLS
- PPP 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 at the following location:

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

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

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

Layer 2 Tunneling Protocol v3 for PXF on the Cisco 7304 NSE-100

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 at the following location:

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

Multicast and Multicast VPN for PXF

The Multicast and Multicast VPN (mVPN) for PXF feature introduces support for the following packets in the PXF processing path on the Cisco 7304 Router in Cisco IOS Release 12.2(25)S2:

- 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* at the following location:

  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 at the following location:

  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 at the following location:

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

New Hardware Features in Cisco IOS Release 12.2(25)S1

There are no new hardware features in Cisco IOS Release 12.2(25)S1.

New Software Features in Cisco IOS Release 12.2(25)S1

This section describes new and changed features in Cisco IOS Release 12.2(25)S1. Some features may be new to Cisco IOS Release 12.2S 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(25)S1. 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.

Multiple Trunk

Cisco IOS Release 12.2(25)S1 adds support for multiple trunk connections that enable more than one network topology to connect to a single Cisco ONS 15540 chassis.

PPP/MLP MRRU Negotiation Configuration

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

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

New Hardware Features in Cisco IOS Release 12.2(25)S

This section describes new and changed features in Cisco IOS Release 12.2(25)S. Some features may be new to Cisco IOS Release 12.2S 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(25)S. 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.

Route Switch Processor 16

The Route Switch Processor 16 (RSP16) is available in new system deployments and as an upgrade to existing systems that are based on the RSP8, RSP4+, or RSP2. The RSP16 is compatible with existing Versatile Interface Processors (VIPs), including the new Cisco VIP6-80, and with port adapters that are supported with existing VIPs.

The RSP16 fully supports Cisco 7500 series high-availability features, including Single Line Card Reload (SLCR), Route Processor Redundancy (RPR), RPR Plus (RPR+), Fast Software Upgrade (FSU), Nonstop Forwarding (NSF), and Stateful Switchover (SSO). This support allows the Cisco 7500 series routers to demonstrate some of the highest uptime in the industry. FSU allows customers to upgrade their existing RSP2, RSP4+, and RSP8 to RSP16 with minimal downtime.

The RSP16 is an ideal platform for enterprise and service provider networks that require additional performance and processing power to support service-enabled edge and core applications.

For information about installation and configuration of the RSP16, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/rte_swit/13963r16.htm

New Software Features in Cisco IOS Release 12.2(25)S

This section describes new and changed features in Cisco IOS Release 12.2(25)S. Some features may be new to Cisco IOS Release 12.2S 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(25)S. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

1-Gbps ISC Links Peer Mode

The 1-Gbps ISC links peer mode is now supported on the Cisco ONS 15530 transponder line cards and Cisco ONS 15540 2.5-Gbps transponder modules.

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/ios123/123newft/123t/123t_7/gtaclace.htm

ACL Support for Filtering IP Options

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/gtipofil.htm

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/ios123/123newft/123t/123t_4/gtaclflg.htm

Any Transport over MPLS

The following Any Transport over Multiprotocol Label Switching (AToM) features are introduced for the Cisco 7500 series in Cisco IOS Release 12.2(25)S:

- Any Transport over MPLS (AToM): Ethernet over MPLS: Port Mode (EoMPLS)
- Any Transport over MPLS (AToM): Distributed Mode for Frame Relay, PPP, and HDLC over MPLS
- Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: Packed Cell Relay
- Any Transport over MPLS (AToM): Single Cell Relay - VC Mode (CRoMPLS)
- Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: VP Mode
- Any Transport over MPLS: (AToM): ATM OAM Emulation
- Any Transport over MPLS (AToM) SCR VC Mode for PA-A3-T1/E1-IMA
- Any Transport over MPLS (AToM) SCR VP Mode and Port Mode for PA-A3-T1/E1-IMA

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

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

Any Transport over MPLS (AToM) Graceful Restart

For detailed information about this feature, see the *Any Transport over MPLS High Availability - Stateful Switchover (SSO) and Non-Stop Forwarding (NSF)* document:

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

Any Transport over MPLS High Availability - Stateful Switchover (SSO) and Non-Stop Forwarding (NSF)

For detailed information about this feature, see the *Any Transport over MPLS High Availability - Stateful Switchover (SSO) and Non-Stop Forwarding (NSF)* document:

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

AToM Port Mode Cell Relay Support for PA-A3-8T1 IMA PA and PA-A3-8E1 IMA PA

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

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

ATM Conditional Debug 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/120s28/12satmdb.htm

ATM OAM Ping

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

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

ATM Port Mode Packed Cell Relay over AToM

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

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

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* feature module 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 Features

The following BGP features are supported as of Cisco IOS Release 12.2(25)S:

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

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

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

BGP MIB Support Enhancements

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

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

BGP Policy Accounting Output Interface Accounting

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/gtbgppax.htm

BGP Support for Dual AS Configuration for Network AS Migrations

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

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

BGP Support for 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/ios122s/122snwft/release/122s25/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/ios122s/122snwft/release/122s25/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/ios122s/122snwft/release/122s25/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/ios122s/122snwft/release/122s25/fs_btsh.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

Cisco IOS Scripting with Tcl

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

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

CLNS Support for GRE Tunneling of IPv4 and IPv6

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

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-tunnel.html#wp1055474

CNS Agents

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fs_cns.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 - Time Based

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

CPU Threshold Notification

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_cput.htm

Embedded Event Manager 2.0

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fs_eem2.htm

Embedded Syslog Manager (ESM)

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

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

Enhanced Object Tracking

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/fthsrptk.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 - Enhanced Object Tracking of Service Assurance Agent (SAA) Operations

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/gtfhrp.htm

FHRP - HSRP - 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

First Hop Redundancy Protocols

The following First Hop Redundancy Protocols (FHRPs) are supported in Cisco IOS Release 12.2(25)S:

- HSRP 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/gthsrpau.htm

- Hot Standby Router Protocol Version 2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gthsrpv2.htm

- VRRP Object Tracking

  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/gtvrrptk.htm

Frame Relay Conditional Debug 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/120s28/12sfrcdb.htm

Frame Relay FRF.1.2 Annex A Support

The Frame Relay FRF.1.2 Annex A Support feature is also known as Local Management Interface (LMI) segmentation and supports an enhancement to the Frame Relay LMI protocol where LMI full status messages are segmented because MTU constraints or large numbers of permanent virtual circuits (PVCs). This feature is useful when the MTU size cannot be increased but is insufficient to accommodate the large number of PVCs on the link. During Frame Relay internetworking with other Layer 2 protocols, the MTUs on each interface must match. In software without the Frame Relay FRF.1.2 Annex A Support feature, users cannot change the MTU size on the Frame Relay side and place all the PVC data into one LMI packet. With the Frame Relay FRF.1.2 Annex A Support functionality, this problem is solved.

The FRF.1.2 Annex A standard adds a new message type “Full status continued” to an LMI packet. When a DCE determines that it cannot fit all PVCs into one packet (enforced by the MTU size), the message type is set to “Full status continued.” The DTE responds to “Full status continued” messages sent to this packet immediately instead of waiting for the T391 timer to expire. The DCE sends the remaining PVCs in one or more “Full status continued” messages until all the remaining PVCs can fit into one message. At this point, a normal “Full status” message is sent.

If the DTE receives a “Full status” or “Full status continued” STATUS message in response to a “Full status continued” STATUS ENQUIRY message, this exchange indicates a lower-valued data-link connection identifier (DLCI) than the previous “Full status continued” STATUS message and is considered to be an error event and PVC information elements (IEs) will not be processed. The next time the T391 timer expires, the “Full status” STATUS ENQUIRY procedure is reinitiated.

This feature follows the FRF1.2 implement agreement [1] and allows the Cisco IOS software to be compliant with the FRF1.2 standard. The implementation is platform-independent and applies to all platforms running Cisco IOS software that support Frame Relay. This feature interoperates only with existing Cisco IOS software releases where all PVCs can be reported in one packet. A router running the new functionality must be able to interoperate with routers running existing Cisco IOS software releases and with routers that support the new functionality using the continuation status request and reply frames. Only LMI types Q.933A and ANSI support the FRF.1.2 Annex A standard.

You can track “Full status continued” packets using the **debug frame-relay lmi** privileged EXEC command. An extra field, 04, has been added to the display output. The following example indicates where in the report to look for this field (text in **bold** for purpose of example):

```
17:42:39: Serial1(out): StEnq, myseq 126, yourseen 125, DTE up
17:42:39: datagramstart = 0x40058DA4, datagramsize = 13
17:42:39: FR encap = 0x00010308
```

```
17:42:39: 00 75 51 01 04 53 02 7E 7D
```

The string segment “active/inactive” in the **show interface** commands indicates whether the FRF.1.2 Annex A standard is triggered. The report indicates active when routers receive the “Full status continued” message; otherwise, the report indicates inactive.

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

IPMROUTE-STD-MIB

This feature introduces support for the IPMROUTE-STD-MIB in Cisco IOS Release 12.2(25)S. The IPMROUTE-STD-MIB, as defined in RFC 2932, is a module for management of IP multicast routing in a manner independent of the specific multicast routing protocol in use. Support for this MIB replaces the draft form of the IPMROUTE-MIB.

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

- ipMRouteEntryCount
- ipMRouteHCOctets
- ipMRouteInterfaceHCInMcastOctets
- ipMRouteInterfaceHCOutMcastOctets

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

IP Traffic Export

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_rawip.htm

IPv6 Anycast Address

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

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html#wp1052470

IPv6 Multicast Features

The following IPv6 Multicast and IPv6 Multicast-related features are supported as of Cisco IOS Release 12.2(25)S:

- IPv6 Bidirectional PIM
- IPv6 Multicast: Address Family Support for Multiprotocol BGP
- IPv6 Multicast: Bootstrap Router (BSR)
- IPv6 Multicast: Explicit Tracking of Receivers
- IPv6 Multicast: MLD Access Group
- IPv6 Multicast: PIM Accept Register
- IPv6 Multicast: PIM Embedded RP Support
- IPv6 Multicast: Routable Address Hello Option
- IPv6 Multicast: RPF Flooding of Bootstrap Router (BSR) Packets
- IPv6 Multicast: Static Multicast Routing (mroute) for IPv6

For information about the IPv6 Multicast: PIM Embedded RP Support feature and the IPv6 Multicast: Static Multicast Routing (mroute) for IPv6 feature, see the following section in the *Implementing IPv6 Multicast* document:

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

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

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

For information about all other IPv6 Multicast and IPv6 Multicast-related features mentioned above, see the following section in the *Implementing IPv6 Multicast* document:

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

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 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

L2TPv3: Layer 2 Tunneling Protocol Version 3

Cisco IOS Release 12.2(25)S introduces support for the Layer 2 Tunneling Protocol version 3 (L2TPv3) feature, including the following L2TPv3-related features:

- ATM AAL5 OAM Emulation over L2TPv3
- ATM Single Cell Relay VC Mode over L2TPv3
- ATM VP Mode Single Cell Relay over L2TPv3
- L2TPv3 Distributed Sequencing
- L2TPv3 Layer 2 Fragmentation

  For information about the L2TPv3 Layer 2 Fragmentation feature, see the "IP Packet Fragmentation" section in the *Layer 2 Tunnel Protocol Version 3* document (see below).
- L2TPv3 Support for PA-A3-8T1IMA PA and PA-A3-8E1IMA Port Adapters

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/120s29/l2tpv29s.htm

L2VPN Interworking

Cisco IOS Release 12.2(25)S introduces support for the L2VPN Interworking feature, including the following features:

- L2VPN Interworking: Ethernet to VLAN
- L2VPN Interworking: Ethernet VLAN to ATM AAL5
- L2VPN Interworking: Ethernet VLAN to Frame Relay
- L2VPN Interworking: Frame Relay to ATM AAL5
- L2VPN Interworking: Frame Relay to PPP

For detailed information about these features, see the *L2VPN Interworking* document:

https://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_l2vpn_intrntwkg_ps6922_TSD_Products_Configuration_Guide_Chapter.html

Layer 2 Local Switching Features

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/en/US/docs/ios/12_0s/feature/guide/fslocal.html

Loadsharing IP Packets over More Than Six Parallel Paths

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

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

Memory Leak Detector

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

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

Memory Pool - SNMP Notification Support

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/gtmemnot.htm

MPLS LDP Inbound Label Binding Filtering

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsinbd4.htm

MPLS LDP: SSO/NSF Support and Graceful Restart

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

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

MPLS LDP MIB: SSO/NSF Support

For further information about this feature, see the "MPLS LDP MIB: SSO/NSF Support" section in the *MPLS High Availability: Overview* document:

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

MPLS VPN MIB: SSO/NSF Support

For detailed information about this feature, see the "MPLS VPN MIB: SSO/NSF Support" section in the *MPLS High Availability: Overview* document:

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

MPLS VPN - Route Target Rewrite

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/fsrtrw4.htm

MPLS VPN: SSO/NSF Support

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

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

MPLS VPN VRF Selection Using Policy Based Routing

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fs_pbrsv.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 Fast Switching Performance Improvement

The Multicast Fast Switching Performance Improvement feature provides improvement of up to 100 percent of the existing multicast path packet throughput. This feature targets software forwarding-based platforms for IPv4 multicast only.

Multilink Frame Relay over L2TPv3/AToM

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/fsmfrl2.htm

NAT—dCEF Support

The NAT—dCEF Support feature enhances the overall performance of Route Switch Processors (RSPs) on a Cisco 7500 series by enabling line cards to perform address translation. Without this feature, any distributed Cisco Express Forwarding (dCEF) switched packet that needs address translation must be switched by the Route Switch Controller (RSC), which increases load and reduces system performance and throughput.

Line cards are able to maintain a subset of the RSC's NAT table. This enables the line cards to switch packets and perform express forwarding within and between port adapters. Because embedded address translation cannot occur at the line card level, packets that require payload translation are punted to the next higher level switching mechanism in the RSC.

NAT—Performance Enhancement—CEF Switching Support

The NAT—Performance Enhancement—CEF Switching Support feature enhances router performance by optimizing packet processing. Through Cisco Express Forwarding (CEF), decisions to translate, punt, drop, or forward a packet are made with a single lookup. To improve performance, packets that do not require translation and fragmented packets are not punted to the process level. Those packets that have special flags, such as TCP syn/fin/reset, are processed in the CEF path itself. Any action that is CPU-intensive is performed by a background process or by process-level NAT code.

NAT—Performance Enhancement—Translation Table Optimization

The NAT Translation Table Optimization Performance enhancement provides greater structure for storing translation table entries and an optimized look up in the table for associating table entries to IP connections.

NAT—Performance & Scalability Enhancement—Timer Wheel

The NAT—Performance & Scalability Enhancement—Timer Wheel feature reduces CPU utilization in cases where routers must manage large numbers of Network Address Translation (NAT) entries and it eliminates the performance bottleneck caused by the previous timer tree model. By using a more efficient data structure and a priority queue to sort the timer and eliminate the sorting operation during a timer insertion, the process of inserting and removing a timer is faster, improving the scalability of a router that is running NAT.

NAT—Rate Limiting NAT Translation

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_natrl.htm

NAT—Translation of External IP Addresses Only

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

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

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

This release adds MIB support to NetFlow. NetFlow cache information, current NetFlow configuration, and statistics can now be monitored using the Simple Network Management Protocol (SNMP).

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

For more information about CISCO-NETFLOW-MIB, the MIB objects for the functionality described above, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

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

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

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 Adjacency

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 Link-Local Signaling Per Interface Basis

For detailed information about this feature (which may also be 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

This release updates the OSPF MIB support to the latest RFC 1850 and adds the latest draft extensions. For more information regarding the definitions of the draft extensions, see the CISCO-OSPF-MIB.my and CISCO-OSPF-TRAP-MIB.my files that are available through the Cisco MIB FTP site at the following URL:

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

For routers that are running Cisco IOS Release 12.0(26)S and later releases, the OSPF MIB and CISCO OSPF MIB will be supported only for the first OSPF process (except for MIB objects that are related to virtual links and sham links). SNMP traps will be generated for OSPF events that are related to any of the OSPF processes. There is no workaround for this situation.

The CISCO-OSPF-MIB.my is a read-only MIB.

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 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

PBR Support for Multiple Tracking Options

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/gtpbrtrk.htm

Periodic MIB Data Collection and Transfer Mechanism

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/gdatacol.htm

PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss

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/gtautorp.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 following Cisco document:

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

Rate Limiting NAT Translation

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_natrl.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

RTP Header Compression over Satellite Links

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

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

Secure Copy

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

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

Secure SNMP Views

The User Security Model (USM), View-Based Access Control Model (VACM), and Community MIBs (SNMP-USM-MIB, SNMP-VACM-MIB, and SNMP-COMMUNITY-MIB) contain information that can potentially be used to gain access to a router using Simple Network Management Protocol (SNMP). Therefore, the USM, VACM, and Community MIBs are excluded from the default SNMP access view so as not to allow remote access unless it is specifically configured. However, when an SNMP view is created with any parent object identifier (OID) of these MIBs included (for example “internet included”), these MIBs also are included in the view. To increase security, the Secure SNMP Views feature excludes these MIBs from SNMP access views even when parent OIDs are included in the view.

In releases earlier than this release, when you configure SNMP views with parent OIDs that include the USM, VACM, or Community MIBs, you must explicitly exclude them. For example, the following configuration can be used to exclude security-sensitive MIBs from the SNMP view that is named “test”:

```
! - include all MIBs under the parent tree "internet" snmp-server view test internet
included
! -- exclude snmpUsmMIB snmp-server view test 1.3.6.1.6.3.15 excluded
! -- exclude snmpVacmMIB snmp-server view test 1.3.6.1.6.3.16 excluded
! -- exclude snmpCommunityMIB snmp-server view test 1.3.6.1.6.3.18 excluded
```

As of Cisco IOS Release 12.0(26)S, 12.2(25)S, and 12.2(2)T, the USM, VACM, and Community MIBs are excluded from any parent OIDs in a configured view by default. If you wish to include these MIBs in a view, you must now explicitly include them.

Service Assurance Agent (SAA) Multiple Operation Scheduling

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

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

Silent Operation Mode

For detailed information about this feature, see the *Control Plane Policing* document:

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

SNMP Support over VPNs—Context Based Access Control

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/gtsnmpvp.htm

Stateful Switchover (SSO) Support for QoS

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

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

Stateful Switchover Support for Multilink Frame Relay

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

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

Suppress BGP Advertisement for Inactive Routes

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

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

VC Single Cell Relay Support for PA-A3-OC12 over AToM/L2TPv3

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

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

VP/VC Mode Packed Cell Relay Support for PA-A3-8T1 IMA PA and PA-A3-8E1 IMA PA

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

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

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.

New Hardware Features in Cisco IOS Release 12.2(22)S

This section describes new and changed features in Cisco IOS Release 12.2(22)S. Some features may be new to Cisco IOS Release 12.2S 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(22)S. 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.

ONS 15530 Platform

The Cisco ONS 15530 is a dense wavelength-division multiplexing (DWDM) multiservice aggregation platform that maximizes the carrying capacity of fiber by performing service aggregation of protocols such as Enterprise System Connection (ESCON), Fibre Channel, Fiber Connectivity (FICON), and Gigabit Ethernet. With the Cisco ONS 15530, users can take advantage of the availability of dark fiber to build a common infrastructure that supports data, storage area networking (SAN), and time-division multiplexing (TDM) traffic.

The Cisco ONS 15530 is available in two configurations, Network Equipment Building Systems (NEBS) and European Telecommunications Standards Institute (ETSI). Both configurations have two vertically stacked half-height slots specifically for the optical add/drop multiplexers (OADM) modules and ten vertically oriented slots that hold the CPU switch modules, line cards, and transponder line cards.

For further information about the Cisco ONS 15530 hardware, see the documents at the following Cisco location:

http://www.cisco.com/univercd/cc/td/doc/product/mels/15530/12_2_s/index.htm

ONS 15540 Platform

The Cisco ONS 15540 Extended Services Platform (ESP) is an optical transport platform that employs dense wavelength-division multiplexing (DWDM) technology. With the Cisco ONS 15540 ESP, users can take advantage of the availability of dark fiber to build a common infrastructure that supports data, storage area networking (SAN), and time-division multiplexing (TDM) traffic.

ONS 15540 ESP

The Cisco ONS 15540 ESP uses a 12-slot modular vertical chassis for optical mux/demux modules, transponder modules, and processor cards. The system has an optical backplane for carrying signals between the transponder modules and the mux/demux modules.

For further information about the Cisco ONS 15540 hardware, see the documents at the following Cisco location:

http://www.cisco.com/univercd/cc/td/doc/product/mels/15540/12_2_s/index.htm

ONS 15540 ESPx

The Cisco ONS 15540 ESPx is similar to the Cisco ONS 15504 ESP but uses an enhanced chassis with front fiber-optic cable access for optical interconnections between transponders and optical mux/demux modules. The system has an electrical backplane for system control.

For further information about the Cisco ONS 15540x hardware, see the documents at the following Cisco location:

http://www.cisco.com/univercd/cc/td/doc/product/mels/15540x/12_2_s/index.htm

Regex Engine Performance Enhancement

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s_22/fs_rexpe.hm

New Software Features in Cisco IOS Release 12.2(22)S

This section describes new and changed features in Cisco IOS Release 12.2(22)S. Some features may be new to Cisco IOS Release 12.2S 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(22)S. 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.

ONS 15530 and ONS 15540 Cisco IOS Software Features

The Cisco IOS software features that are supported for the Cisco ONS 15530 and Cisco ONS 15540 include the following ones:

- 10GbE Support over Optical Transport
- Client Service Aggregation over 10Gbps
- ESCON Service Aggregation
- Fibre Channel/FICON/Gigabit Ethernet Service Aggregation
- Optical Client Based Line Card Protection
- Optical High Availability Software
- Optical Multiplexing and Demultiplexing
- Optical Splitter Protection
- Optical Supervisory Channel Protocol
- Optical Switch Fabric Based Line Card Protection
- Optical Trunk Fiber Protection

- Optical Y-Cable Line Card Protection
- Protocol Monitoring of Storage and Data Protocols
- Variable Optical Attenuation

For more information about these and other features, see the *Cisco ONS 15530 and Cisco ONS 15540: Cisco IOS Software Configuration Library* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s_22/fs_ons.htm

New Hardware Features in Cisco IOS Release 12.2(20)S6

There are no new hardware features in Cisco IOS Release 12.2(20)S6.

New Software Features in Cisco IOS Release 12.2(20)S6

This section describes new and changed features in Cisco IOS Release 12.2(20)S6. Some features may be new to Cisco IOS Release 12.2S 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(20)S6. 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.

Cisco 7304 FPGA Upgrade Enhancements

In Cisco IOS Release 12.2(20)S6, some major enhancements were made to the Cisco 7304 FPGA upgrade process. The following enhancements were made:

- The **no upgrade fpga** command was introduced and became the default setting. Starting in this Cisco IOS Release, FPGA is not upgraded automatically when an FPGA version mismatch is detected and the user is not prompted to upgrade the FPGA when the default settings are maintained.
- The **no upgrade fpga prompt** command behavior was changed. The **no upgrade fpga prompt** configuration no longer automatically begins an FPGA upgrade when an FPGA mismatch is detected.
- The prompt asking users if they would like to reload the line card to complete the FPGA upgrade process after entering the **upgrade fpga all** command was added. As a result of this enhancement, FPGA upgrades can be completed up to the stage where a hardware reload is required to finish the upgrade, but the hardware can be reloaded at a later time to complete the FPGA upgrade.
- The **show c7300** command was modified to show more FPGA information.
- The **show upgrade fppa progress** command was introduced.
- The **upgrade fpga force** command was introduced.

For additional information on the Cisco 7304 FPGA upgrade process, 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

Cisco 7304 Shared Port Adapter Field Programmable Device show Command Updates

In this Cisco IOS Release, the **show upgrade** commands that are used to monitor SPA FPD behavior on the Cisco 7304 router (**show upgrade file**, **show upgrade package default**, **show upgrade progress**, and **show upgrade table**) have been changed to add the **fpd** keyword. The output previously generated with the aforementioned commands can now be generated by entering the appropriate **show upgrade fpd** command (**show upgrade fpd file**, **show upgrade fpd package default**, **show upgrade fpd progress**, and **show upgrade fpd table**).

For additional information on these commands and FPD in general, see the *Cisco 7304 Router 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

New Hardware Features in Cisco IOS Release 12.2(20)S5

There are no new hardware features in Cisco IOS Release 12.2(20)S5.

New Software Features in Cisco IOS Release 12.2(20)S5

This section describes new and changed features in Cisco IOS Release 12.2(20)S5. Some features may be new to Cisco IOS Release 12.2S 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(20)S5. 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.

PXF Logical Interface Options on the Cisco 7304 Router Using an NSE-100

On the Cisco 7304 router using an NSE-100, the PXF processing path is enhanced in Cisco IOS Release 12.2(20)S5 to support up to 63 classes per QoS policy (previous IOS releases supported up to 23 classes per QoS policy).

The **pxf max-logical-interfaces** command is introduced as part of this feature. This command allows you to choose the number of PXF logical interfaces that you want to support on the router. There is a direct trade off between the number of supported PXF logical interfaces on the router and the number of supported QoS traffic classes per policy in PXF. You can configure the **pxf max-logical-interfaces** command by using either the **4k** or **16k** options. If the router is configured to support 4,096 PXF logical interfaces (with the **pxf max-logical-interfaces 4k** command), up to 63 QoS classes per policy can be supported in PXF. If the router is configured to support 16,384 logical interfaces (which is the default setting, or which can be restored by entering the **pxf max-logical-interfaces 16k** command), up to 23 QoS classes per policy can be supported in PXF.

The **show max-logical-interfaces** command is also introduced to show the selected number of PXF logical interfaces that is configured in both the running and startup configurations.

For additional information on this feature, see the *PXF Logical Interface Options* document:

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

FPGA Upgrade Prompt Options on the Cisco 7304 Router

In Cisco IOS Release 12.2(20)S5, the [**no**] **upgrade fpga prompt** command is introduced. This command enables and disables FPGA prompting when an FPGA incompatibility is detected. FPGA upgrading prompting is still enabled by default. If FPGA prompting is disabled (with the **no upgrade fpga prompt** command), an FPGA upgrade is automatically performed when an FPGA incompatibility is detected by the router.

For additional information about this command, see the *FPGA Bundling and Update* document:

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

New Hardware Features in Cisco IOS Release 12.2(20)S3

This section describes new and changed features in Cisco IOS Release 12.2(20)S3. Some features may be new to Cisco IOS Release 12.2S 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(20)S3. 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.

Cisco CWDM SFP Support for the NPE-G100

Supported platform: Cisco 7304

The SFP ports on the NPE-G100 processor of the Cisco 7304 router now supports the following Coarse Wavelength Division Multiplexing (CWDM) Small Form-Factor Pluggable (SFP) modules:

- Cisco CWDM SFP 1470 nm (product number CWDM-SFP-1470=)
- Cisco CWDM SFP 1490 nm (product number CWDM-SFP-1490=)
- Cisco CWDM SFP 1510 nm (product number CWDM-SFP-1510=)
- Cisco CWDM SFP 1530 nm (product number CWDM-SFP-1530=)
- Cisco CWDM SFP 1550 nm (product number CWDM-SFP-1550=)
- Cisco CWDM SFP 1570 nm (product number CWDM-SFP-1570=)
- Cisco CWDM SFP 1590 nm (product number CWDM-SFP-1590=)
- Cisco CWDM SFP 1610 nm (product number CWDM-SFP-1610=)

New Software Features in Cisco IOS Release 12.2(20)S3

This section describes new and changed features in Cisco IOS Release 12.2(20)S3. Some features may be new to Cisco IOS Release 12.2S 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(20)S3. 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.

Stateful Switchover and Nonstop Forwarding Support for Cisco 7304 Routers using the MSC-100

Supported platform: Cisco 7304

The Stateful Switchover (SSO) and Nonstop Forwarding (NSF) features are now available for the Cisco 7304 routers configured with an MSC-100 populated with SPAs.

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The SSO feature takes advantage of RP redundancy by establishing one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them.

SSO is used with the Cisco NSF feature. Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover.

Stateful Switchover and Nonstop Forwarding Support for Cisco 7304 Routers using the PCI Port Adapter Carrier Card

Supported platform: Cisco 7304

The Stateful Switchover (SSO) and Nonstop Forwarding (NSF) features are now available for the Cisco 7304 routers configured with a PCI Port Adapter Carrier Card populated with a port adapter.

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The SSO feature takes advantage of RP redundancy by establishing one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them.

SSO is used with the Cisco NSF feature. Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover.

New Hardware Features in Cisco IOS Release 12.2(20)S2

This section describes new and changed features in Cisco IOS Release 12.2(20)S2. Some features may be new to Cisco IOS Release 12.2S 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(20)S2. 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.

4-Port 10/100 Fast Ethernet Shared Port Adapter

Supported platform: Cisco 7304

The 4-port 10/100 Fast Ethernet shared port adapter (SPA) (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* at the following location:

  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* at the following location:

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

2-Port 10/100/1000 Gigabit Ethernet Shared Port Adapter

Supported platform: Cisco 7304

The 2-port 10/100/1000 Gigabit Ethernet shared port adapter (SPA) provides two 10/100/1000 Ethernet/Fast Ethernet/Gigabit Ethernet ports for the Cisco 7304. SPAs are half-height interface line cards that provide additional physical interfaces to the Cisco 7304 router 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 SPA-2GE-7304 for the Cisco 7304 router, see the following documents:

- *Cisco 7304 Router Modular Services Card and Shared Port Adapter Hardware Installation Guide* at the following location:

  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* at the following location:

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

Modular Services Card 100

Supported platform: Cisco 7304

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* at the following location:

  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* at the following location:

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

New Software Features in Cisco IOS Release 12.2(20)S2

There are no new software features in Cisco IOS Release 12.2(20)S2.

New Hardware Features in Cisco IOS Release 12.2(20)S

There are no new hardware features in Cisco IOS Release 12.2(20)S.

New Software Features in Cisco IOS Release 12.2(20)S

This section describes new and changed features in Cisco IOS Release 12.2(20)S. Some features may be new to Cisco IOS Release 12.2S 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(20)S. 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.

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* at the following location:

https://www.cisco.com/en/US/docs/routers/7300/technical_references/7304_mib_guides/7304_mib_specs_guide_v2/7304mib.html

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

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

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

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 (PXF Based) 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 additional information on this and other PXF features, see the "PXF Features" section in the *Cisco 7304 Troubleshooting and Configuration Notes* document at the following location:

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.

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

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

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.

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

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

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 at the following location:

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

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

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

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

NetFlow Export of BGP Next Hop Propagation (PXF Based)

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

The BGP Next Hop Propagation 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 at the following location:

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 *BGP Next Hop Propagation* document at the following location:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_bgpnh.html

Nonstop Forwarding (NSF) with Stateful Switchover (SSO)

Cisco IOS Release 12.2(18)S introduced the Nonstop Forwarding (NSF) with Stateful Switchover (SSO) feature for the Cisco 7500 series. Release 12.2(20)S introduces support for this feature for the Cisco 7304 router.

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

Route Processor Redundancy Plus (RPR+)

Cisco IOS Release 12.2(14)S introduced the Route Processor Redundancy Plus (RPR+) feature for the Cisco 7500 series. Release 12.2(20)S introduces support for the Route Processor Redundancy Plus (RPR+) feature for the Cisco 7304 router.

The 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 at the following location:

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

Service Assurance Agent (SAA) MPLS VPN Operation

The Service Assurance Agent (SAA) MPLS VPN Operation 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/ios122/122newft/122t/122t2/ft1csaa.htm

Service Assurance Agent (SAA) Path Jitter Operation

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft1csaa.htm

New Hardware Features in Cisco IOS Release 12.2(18)S

This section describes new and changed features in Cisco IOS Release 12.2(18)S. Some features may be new to Cisco IOS Release 12.2S 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(18)S. 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.

Cisco 7300 Series

The Cisco 7300 series includes the following two routers.

Cisco 7301 Router

The Cisco 7301 router is optimized for flexible, feature rich IP/MPLS services at the customer network edge, where service providers and enterprises link together. The Cisco 7301 router can be used for enterprise campus or Internet gateway applications, or it can be deployed by service providers as a high-end customer premises equipment (CPE) router for managed service offerings. Other applications for the Cisco 7301 router include service provider broadband aggregation and metro Ethernet CPE applications.

The compact Cisco 7301 router is the industry's highest performance single rack unit router, capable of processing million packets per second. With three built-in Gigabit Ethernet interfaces (copper or optical) and a single slot for any Cisco 7000 series port adapter, the Cisco 7301 router is highly flexible for a variety of applications. For broadband aggregation, the Cisco 7301 router also supports up to 16,000 subscribers sessions, making it ideal for pay-as-you-grow broadband deployment models.

For more information about the Cisco 7301 router, see the Cisco documents at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/7301/index.htm

Cisco 7304 Router

The compact, modular Cisco 7304 router is designed for the network edge, where high-performance IP/Multiprotocol Label Switching (MPLS) services are required to enable profitability, service differentiation, and business agility. The Cisco 7304 router is the most compact (4RU) routing system in the industry to offer route processor redundancy coupled with a comprehensive set of interfaces from DS-1 to OC-48/STM-16 to Gigabit Ethernet. The Cisco 7304 router supports two network processors designed to meet the widest variety of network requirements. The Network Service Engine 100 (NSE-100), with two built-in Gigabit Ethernet interfaces, delivers uncompromising feature acceleration using Cisco's innovative Adaptive Network Processing (ANP) technology—ideal for high-performance carrier service delivery. The Network Processing Engine G-100 (NPE-G100), with three built-in Gigabit/Fast Ethernet interfaces, offers high-performance, flexible support for the most comprehensive set of Cisco IOS features.

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

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

Cisco 7304 Router Line Cards

The Cisco 7304 router supports the following line cards:

- 1-port OC-12 Packet-over-SONET (POS) line card
- 1-port OC-48 POS line card
- 2-port OC-3 ATM line card
- 2-port OC-3 POS line card
- 4-port OC-3 POS line card
- 2-port OC-12 POS line card
- Clear Channel 6-port T3 (DS3) line card

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

Cisco 7304 Router Port Adapters

The Cisco 7304 router supports Cisco 7000 series port adapters in conjunction with the 7300-CC-PA carrier card. For information about the supported port adapters, see Table 3 and see the Cisco documents at the following location:

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

2-Port Packet over SONET OC3c/STM1 Port Adapter

Supported platforms: Cisco 7200 VXR routers, Cisco 7300 series, Cisco 7400 series, Cisco 7500 series

The 2-port Packet over SONET OC3c/STM1 port adapter (PA-POS-2OC3) provides two Packet-over-SONET (POS) ports in a single port adapter slot. The two ports function either as dual independent OC-3c/STM1 ports or as a single port with automatic protection switching (APS). The PA-POS-2OC3 is used as a direct connection between the supported router or switch and external networks.

The PA-POS-2OC3 installs into a single port adapter slot on the Cisco7204VXR, Cisco 7206VXR, Cisco 7301, and Cisco 7401ASR router, on the Cisco 7500 series, and on the Cisco 7304 PCI Port Adapter Carrier Card in a Cisco 7304 router.

For more information about the PA-POS-2OC3, see the Cisco documents at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/portadpt/sonet_pa/3028_2oc/index.htm

New Software Features in Cisco IOS Release 12.2(18)S

This section describes new and changed features in Cisco IOS Release 12.2(18)S. Some features may be new to Cisco IOS Release 12.2S 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(18)S. 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.

ACL Performance Enhancement

Supported platforms: Cisco 7200 series, Cisco 7300 series, Cisco 7500 series

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.

Before Cisco IOS Release 12.2(18)S, 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(18)S 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.

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

AutoSecure

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/ftatosec.htm

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/index.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/ios120/120newft/120limit/120s/120s24/s_bgpct.htm

BGP Convergence Optimization

Supported platforms: Cisco 7200 series, Cisco 7300 series, Cisco 7500 series

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 may also be 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 Dynamic Update Peer-Groups

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

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

BGP 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/ios122/122newft/122t/122t15/ftiaaspa.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/ios122/122newft/122t/122t15/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/ios123/123newft/123t/123t_2/gt_brmcs.htm

BGP Route-Map Policy List Support

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

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

Cisco 7304 Software Features

The following features were ported from other Cisco IOS releases and are now supported in Cisco IOS Release 12.2(18)S and later releases for the Cisco 7304 router.

ACL Accounting Enhancements

The Access Control List Accounting feature keeps internal statistics and reports so network managers can ascertain which access control lists (ACLs) have been tested. This knowledge provides network managers with an understanding of how intruders are attempting to enter their enterprise networks. ACL accounting provides source and destination address information, source and destination port numbers, and packet counts. Use the **show ip access-lists** [*access-list-number* | *name*] command to view how many times a particular ACL has permitted or denied packets. For example:

```
Router# show ip access-lists source_only
Extended IP access list source_only (Compiled)
    permit udp host 1.1.1.3 eq snmp host 2.1.1.3 (994598 matches)
    permit udp host 1.1.1.3 eq snmptrap host 2.1.1.3 (994598 matches)
    permit udp host 1.1.1.3 eq domain host 2.1.1.3 (994598 matches)
    permit udp host 1.1.1.3 eq bootps host 2.1.1.3 (994598 matches)
.
.
.
```

Cisco 7304 Router High Availability NSE Redundancy

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

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

Cisco 7304 Router Platform-Specific Commands

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

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/12e_73x.htm

Cisco 7304 Router Power-On Diagnostics

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

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

FPGA Bundling and Update

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

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

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/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html

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/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html

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/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html

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/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html

Pv6 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

MPLS AToM—Ethernet over MPLS

In Cisco IOS Release 12.2(18)S, this feature is introduced for 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/ios122/122newft/122limit/122sz/12214sz/eompls.htm

MPLS Traffic Engineering

Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) enables an MPLS backbone to replicate and expand upon the TE capabilities of Layer 2 ATM and Frame Relay networks.

TE is essential for service provider and Internet service provider (ISP) backbones. Such backbones must support a high use of transmission capacity, and the networks must be very resilient, so that they can withstand link or node failures.

MPLS TE provides an integrated approach to traffic engineering. With MPLS, TE capabilities are integrated into Layer 3, which optimizes the routing of IP traffic, given the constraints imposed by backbone capacity and topology.

MPLS TE routes traffic flows across a network based on the resources the traffic flow requires and the resources available in the network.

MPLS TE employs "constraint-based routing," in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic flow. In MPLS TE, the flow has bandwidth requirements, media requirements, a priority over other flows, and so on.

MPLS TE gracefully recovers to link or node failures that change the topology of the backbone by adapting to the new set of constraints.

In Cisco IOS Release 12.2(18)S, the following MPLS TE features are introduced. This list also notes the features that were introduced in the Parallel Express Forwarding (PXF) switching path:

- MPLS Traffic Engineering—basic PXF switching and accounting (introduced in the PXF switching path)
- Basic PXF switching and accounting of MPLS TE traffic.
- MPLS Traffic Engineering—Load Balancing (introduced in the PXF switching path)

  Allows a router to balance traffic engineering traffic over multiple traffic engineering tunnels.
- MPLS Traffic Engineering—Automatic Bandwidth Adjustment (introduced in the PXF switching path)

  Automatically resizes a tunnel based on the tunnel's utilization. Automatic Bandwidth Adjustment decides whether to resize a tunnel at a specified collection frequency. The frequency is the number of seconds between samples of the tunnel output rate.
- MPLS Traffic Engineering—1-hop MPLS-Traffic Engineering tunnel support (introduced in the PXF switching path)

  An MPLS TE tunnel where the tunnel-head and the tunnel-tail routers are connected back to back is referred to as a 1-hop tunnel. In the 1-hop tunnel, the label switched path (LSP) terminates at the next hop. 1-hop MPLS TE tunnels are supported in PXF.
- MPLS Traffic Engineering over Frame Relay, 802.1q, and ATM subinterfaces (introduced in the PXF switching path)
- MPLS Traffic Engineering—Auto Route Calculation

  The MPLS Traffic Engineering Auto Route Calculation is used to instruct the Interior Gateway Protocol to use a tunnel in it's shortest path first (SPF)/next-hop calculation if the tunnel is up.

- MPLS Traffic Engineering—IP Explicit Address Exclusion Support

  The ability to include and exclude given explicit IP addresses during LSP setup.

- MPLS Traffic Engineering—Link Coloring

  The affinity bits are an MPLS label distribution tunnel's requirements on the attributes of the links the tunnel will cross. The tunnel's affinity bits and affinity mask must match up with the attributes of the various links carrying the tunnel.

For sample MPLS TE configurations, see the *Cisco 7304 Troubleshooting and Configuration Notes* document at the following location:

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

NSE-100 Hardware MAC Address Filtering

Each native Gigabit Ethernet port on the Network Service Engine 100 (NSE-100) can support up to 64 hardware MAC addresses. The MAC addressees of each port are stored in a hardware MAC address filtering table. With two NSE-100s installed, the Cisco 7304 router chassis can support up to four native Gigabit Ethernet ports and a total of 256 MAC address entries.

POS Alarm Trigger Delay

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121ex/121ex12c/e_posde.htm

PXF features

The Cisco 7304 router has a Parallel Express Forwarding (PXF) processor tot speed up the processing of various features that are supported in the PXF processing path. For a comprehensive list of the features that are supported in PXF on the Cisco 7304 and other information about PXF support, see the *Cisco 7304 Router Troubleshooting and Configuration Notes* document at the following location:

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

show redundancy Command Enhancements

The **show redundancy** command has been enhanced to include the following outputs: Operating mode, system up time, active up time, and the number of standby failures.

T3 Bit Error Rate Testing

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121ex/121ex12c/e_t3bert.htm

T3 Maintenance Data Link Messages

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121ex/121ex13/e_t3mdl.htm

Unicast Reverse Path Forwarding

The Unicast Reverse Path Forwarding (RPF) feature helps to mitigate difficulties that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the Internet service provider (ISP), its customer, and the rest of the Internet.

On the Cisco 7304 router, the following configuration options are available for RPF:

- **ip verify unicast reverse-path** [**allow-self-ping**] [*list*]

  The **ip verify unicast reverse-path** command configures RPF verification on an interface. In this configuration, the router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received. If the source address of the packet does not match the interface on which the packet was received, the packet is dropped if no access list is specified or filtered by the access list if an access list is specified in the command line. An access list is specified for packets failing the RPF by specifying a previously configured access list number using the list option in the command line.

  A hole exists in the verification check to allow the router to ping it's own interface. This hole could be exploited by attackers to spoof packets and attack the router. To prevent this type of DoS attack, the **allow-self-ping** option has to be configured for a router to ping it's own interface.

- **ip verify unicast source reachable-via** {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*list*]

  The **ip verify unicast source reachable-via** any command configures RPF to accept the incoming packet if the source IP address exists in the router's Forwarding Information Base (FIB), while the **ip verify unicast source reachable-via rx** command configures RPF to insure the source IP address is reachable via the interface on which the packet was received. The **allow-default** option is used to signal that RPF can lookup the default route on a router and use if for RPF verification.

The **show c7300 pxf accounting** command can be used to show the number of packets dropped on account of a failed RFP check, and the **show c7300 pxf interface all** command will show the RPF Verification Drops (the packets dropped by RPF check) and RPF Suppressed Drops (the packets dropped by RPF but permitted by the configured access list.) The **show ip access-list** command will show the number of packets dropped by RPF and permitted or denied by the configured access list.

Control Plane Policing

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

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

EIGRP NonStop Forwarding Support

Supported platforms: Cisco 7500 series

The EIGRP NonStop Forwarding Support feature introduces Cisco Nonstop Forwarding (NSF) Stateful Switchover (SSO) support on Cisco 7500 series routers that are running Enhanced Interior Gateway Routing Protocol (EIGRP). Cisco NSF SSO support allows the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps, which reduces loss of service outages for customers. This capability allows the EIGRP peers of the failing router to retain the routing information that is advertised by the failing router and continue to use this information until the failed router has returned to normal operating behavior and is able to exchange routing information. The peering session is maintained throughout the entire NSF operation.

The following commands have been introduced on the Cisco 7500 series routers to support NSF SSO. These commands are enabled in router configuration mode under an EIGRP routing process.

- **nsf**

  The **nsf** command enables Cisco NSF SSO operation. Use the **no** form of this command to disable NSF SSO operation. This command can be issued only on NSF-capable routers, such as Cisco 7500 series routers.

- **timers nsf signal** *seconds*

  The **timers nsf signal** command is used to adjust the maximum time of the initial restart period. During this time period the restarting router receives updates from peers. When this timer expires, a Routing Information Base (RIB) convergence notification is sent to peer routers. This command can be issued only on NSF-capable routers, such as Cisco 7500 series routers.

- **timers nsf converge** *seconds*

  The **timers nsf converge** command is used by the NSF-aware peer to adjust the maximum time that the router will wait for the convergent signal from the restarting router. This is a watchdog timer used in case the NSF-aware peer does not receive the end-of-table indication from the restarting neighbor. When this timer expires, the peer will scan its topology table looking for the stale routes from the restarting neighbor and then go active on them. This command can be issued only on NSF-capable routers, such as Cisco 7500 series routers.

- **timers nsf route-hold** *seconds*

  The **timers nsf route-hold** command sets the maximum period of time that the NSF-aware router will hold known routes for an NSF-capable neighbor during a switchover operation or a well-known failure condition. The route-hold timer is configurable so that you can tune network performance and avoid undesired effects, such as “black holing” routes if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation. This command can be issued on NSF-capable or NSF-aware routers.

- **debug eigrp nsf**

  The output from the **debug eigrp nsf** command displays NSF-specific events. This command can be issued on NSF-capable or NSF-aware routers.

For more information about EIGRP NSF awareness and support, see the *EIGRP NonStop Forwarding Awareness* document at the following location:

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

For more information about NSF SSO support, see the *Stateful Switchover* document at the following location:

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

Hot Standby MAC Address

The Hot Standby MAC Address (HSMA) feature achieves redundancy and fault tolerance and avoids a single point of failure of Cisco Channel Interface Processors (CIPs) or Channel Port Adapters (CPAs). This feature also ensures that multiple devices on the Ethernet can have a common MAC address.

See the following document for further information:

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

Image Verification

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

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_image_verifctn_ps6922_TSD_Products_Configuration_Guide_Chapter.html

Implementing OSPF for IPv6

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6/ipv6imp/sa_ospf3.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

Integrated IS-IS Multi-Topology Support for IPv6

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

http://www.cisco.com/en/US/docs/ios/12_2t/release/notes/122TNEWF.html

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

ip dhcp-client default-router distance Command

Previous to Cisco IOS Release 12.2(18)S, Dynamic Host Configuration Protocol (DHCP) originated default routes that always had an administrative distance of 254. This distance allowed a metric of 255 as a backup route, but some routing protocols would interpret 255 as route unavailable. You can now configure the default administrative distance with the new **ip dhcp-client default-router distance** *value* command. For detailed information about this command, see the following Cisco document:

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_dhc1.html#wp1033167

IPv6 Multicast

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

http://www.cisco.com/en/US/docs/ios/12_2t/release/notes/122TNEWF.html

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

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/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

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 - 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/122s18/fsimib_3.htm

MPLS - LDP MIB Version 08 Upgrade

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/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

NetFlow Export of BGP Next Hop Information

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/nfbgpnxt.htm

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 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

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

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 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 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 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 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

QA Error Recovery for the Cisco 7500 Series

Supported platform: Cisco 7500 series

The QA Error Recovery for the Cisco 7500 feature helps a networking device to recover quickly from difficulties that are known as QAERRORs. These QAERRORs can be caused by hardware or software conditions. When a QAERROR occurs, a fully loaded networking device can pause up to five minutes (300 seconds) while it tries to recover from the difficulties. With QA error recovery enabled, the time that a networking device pauses can be a short as one second.

In Cisco IOS Release 12.2S, the QA Error Recovery for the Cisco 7500 feature is enabled by default.

You can tell that recovery from an error was successful because a message that reports a successful recovery appears on the console screen. In addition, the number of QAERROR recoveries is displayed in the output of the **show controllers cbus** privileged EXEC command.

The following example shows the output of the console or show logs when the QAERROR occurs. Although the example indicates both the point at which the feature attempts to recover from the QAERROR and the point at which the networking device recovers from the error, the networking device may display many additional messages that can help service technicians to diagnose the actual cause of the difficulties.

```
%QA-3-DIAG:Trying to recover from QA ERROR.
%QA-3-DIAG:Removing buffer header 0xE360 from all queues
%QA-3-DIAG:Buffer 0xE360 is element 155 on queue 0x2E
%QA-3-DIAG:Queue 0x2E (48000170) has 154 elements
%QA-3-DIAG:Buffer 0xE360 is element 1 on queue 0x340
%QA-3-DIAG:Queue 0x340 (48001A00) has 0 elements
%QA-3-DIAG:At least one QA queue is broken
%QA-3-DIAG:Recovered from QA ERROR
```

The following example shows the relevant QA error recovery output of the **show controllers cbus** privileged EXEC command:

```
Router# show controllers cbus
MEMD at E0000000, 8388608 bytes (unused 1565056, recarves 5, lost/qaerror recoveries 0/0)
.
.
.
```

To disable QAERROR recovery on the networking device, enter the **no** version of the **hw-module main-cpu qaerror-recovery-enable** global configuration command:

no hw-module main-cpu qaerror-recovery-enable

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

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

SNMPv3 Community MIB Support

Supported platforms: Cisco 7200 series, Cisco 7300 series, Cisco 7500 series

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.

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/ITDIT/MIBS/servlet/index.

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

SSO support for Community MIB, Notification MIB, Notification Log MIB, and Entity FRU Control MIB

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/ssomibs2.htm

Warm Reload

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/gtwrmrbt.htm

New Hardware Features in Cisco IOS Release 12.2(14)S

This section describes new and changed features in Cisco IOS Release 12.2(14)S. Some features may be new to Cisco IOS Release 12.2S 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(14)S. 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.

Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Input/Output Controllers

Supported platform: Cisco 7200 VXR routers

Cisco IOS Release 12.2(14)S supports two new variants of the Cisco 7200 I/O card:

- The Cisco 7200-I/O-GE+E is an Input/Output controller that provides one Gigabit Ethernet and one Ethernet port. It is equipped with a GBIC receptacle for 1000-Mbps- operation and an RJ-45 receptacle for 10-Mbps operation.
- The Cisco 7200-I/O-2FE/E is an Input/Output controller that provides two autosensing Fast Ethernet ports and is equipped with two RJ-45 receptacles for 10/100-Mbps operation.

For more information about the Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Input/Output controllers, see the Cisco document at the following location:

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

For information about installation and configuration of the Input/Output controllers, see the Cisco document at the following location:

https://www.cisco.com/en/US/docs/routers/7200/install_and_upgrade/7200_i.o_controller_install/4447io.html

Cisco 7401 ASR-BB and Cisco 7401 ASR-CP

The Cisco 7401 series Application Specific Router (ASR) platforms provide application-specific features for broadband subscriber aggregation and network application services with high processing performance. The Cisco 7401 series ASR platforms provide the following hardware features:

- A compact one-rack unit chassis.
- Two fixed 10/100/1000-Mbps Ethernet ports.
- A processor with Parallel Express Forwarding technology.
- Support for a broad range of WAN media interfaces from DS0 to OC-3 (40+ port adapters).
- Common port adapters with the Cisco 7500 series and Cisco 7200 series.

Cisco IOS Release 12.2(14)S supports the following two Cisco 7401 series ASR platforms:

- Cisco 7401 ASR-BB for broadband subscriber aggregation including digital subscriber line (xDSL), ISDN, fiber-to-the-curb (FTTC), and wireless services.
- Cisco 7401 ASR-CP for managed service (CPE) and customer-leased equipment and full MPLS provider edge (PE) and MPLS VPN services.

For information about installation and configuration of the Cisco 7401 series ASR platforms, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/7401/index.htm

Enhanced Gigabit Ethernet Interface Processor

Supported platform: Cisco 7500 series

The Enhanced Gigabit Ethernet Interface Processor (GEIP+) dual-wide port adapter provides enhanced data throughput compared to the GEIP for high density environments.

Gigabit Ethernet (GE) continues to be the choice media for both Enterprise backbone and Internet service providers (ISP) intra-point of presence (POP) interconnects. The GEIP+ supplies the high-throughput solution for integrating Cisco 7500 series into GE infrastructures.

The GEIP+ supports the following features:

- Applicable IEEE 802.3z standards; full-duplex operation only
- IEEE 802.3x flow control
- Layer 3 distributed services, including Route Processor (RP) Cisco Express Forwarding (CEF) switching, fast switching, flow switching, and Committed Access Rate (CAR)
- IEEE 802.1Q frames (in tagged or untagged modes)
- Maximum transmission unit (MTU) of 4476 bytes
- Ethernet Inter-Switch Link (ISL) encapsulation
- Online insertion and removal of the GEIP+ and the Gigabit Interface Converter (GBIC)
- Support for 1000BASE-SX (short wavelength=850-nm), 1000BASE-LX (long wavelength=1300-nm), and Long-Haul (long wavelength=1300-nm) operation by way of GBICs

For information about installation and configuration of the GEIP+, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/vip1/vip4/10699dwg/index.htm

Integrated Service Adapter

Supported platform: Cisco 7200 series

The Integrated Service Adapter (ISA) is a single-width service adapter that provides high-performance, hardware-assisted tunneling and encryption services suitable for Virtual Private Network (VPN) remote access, site-to-site intranet, and extranet applications, as well as platform scalability and security, while working with all services necessary for successful VPN deployments—security, quality of service (QoS), firewall and intrusion detection, and service-level validation and management.

The ISA offloads IP security (IPSec) and Microsoft Point-to-Point Encryption (MPPE) processing from the main processor of Cisco 7200 series, thus freeing resources on the processing engine (that is, the network processing engine [NPE] on the Cisco 7200 series) for other tasks.

The ISA provides hardware-accelerated support for multiple encryption functions:

- 56-bit Data Encryption Standard (DES) standard mode: Cipher Block Chaining (CBC)
- 3-key triple DES (168-bit)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5) hash algorithms

- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40

For information about installation and configuration of the ISA, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/portadpt/service/sa_isa/index.htm

Multichannel STM-1 Port Adapter

Supported platforms: Cisco 7200 VXR routers, Cisco 7400 series, Cisco 7500 series

The PA-MC-STM-1 is a high-speed, single-port multichannel STM-1 port adapter. You can configure the PA-MC-STM-1 as a multichannel E1/E0 STM-1 port. The PA-MC-STM-1 can be configured into 63 individual E1 links. Each E1 link can carry a single channel at full or fractional rates or be broken down into multiple DS0 or Nx64 Kbps rates. The PA-MC-STM-1 supports up to three TUG-3/AU-3 transport slots numbered 1 through 3. You can configure each TUG-3/AU-3 to carry 21 SDH TU-12s. Each SDH TU-12 is capable of carrying a channelized E1 frame, which can be unchannelized to nx64-Kbps time slots.

For more information about the PA-MC-STM-1, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e7/12e_stm.htm

For information about installation and configuration of the PA-MC-STM-1, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/portadpt/multi_ch/pa_mcstm/index.htm

Network Services Engine

Supported platform: Cisco 7200 VXR routers

The Network Services Engine (NSE) is the latest processor engine for Cisco 7200 VXR series. The NSE delivers wire rate OC-3 throughput while concurrent high-touch WAN edge services are running. It is the first Cisco processing engine to offer integrated hardware acceleration, increasing Cisco 7200 VXR series system performance by 50 to 300 percent for combined “high touch” edge services. The NSE takes advantage of a new technology called Parallel Express Forwarding (PXF).

The PXF processor enables IP parallel processing functions that work with the primary processor to provide accelerated IP Layer 3 feature processing. The PXF processor off-loads IP packet processing and switching functions from the Route Processor (RP) to provide accelerated and highly consistent switching performance when coupled with one or more of several IP services features such as access control lists (ACLs), address translation, quality of service (QoS), flow accounting, and traffic shaping.

For information about installation and configuration of the NSE, see the Cisco document at the following location:

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

NPE-400

Supported platform: Cisco 7200 VXR routers

The NPE-400 is a new version of network processing engine for Cisco 7200 VXR routers with the following enhancements:

- RM7000 microprocessor that operates at an internal clock speed of 350 MHz
- Up to 512-MB ECC SDRAM
- 100-MHz SysAD and memory bus speed
- 4-MB Layer 3 cache

The NPE-400 leverages technology from the NPE-225 and NSE-1 to provide a higher performance NPE card.

For information about installation and configuration of the NPE-400, see the Cisco document at the following location:

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

NPE-G1

Supported platform: Cisco 7200 VXR routers

The NPE-G1 is the first network processing engine (NPE) for the Cisco 7200 VXR routers to provide the functionality of both a network processing engine and I/O controller. If used without an I/O controller, an I/O blank panel must be in place.

While its design provides I/O controller functionality, it can also work with any I/O controller that is supported in the Cisco 7200 VXR routers. The NPE-G1, when installed with an I/O controller, provides the primary I/O functionality; that is, the NPE-G1 I/O functionality enhances that of the existing I/O controller. However, when both the I/O controller and NPE-G1 are present, the functionality of the auxiliary port and console port are on the I/O controller.

The NPE-G1 maintains and executes the system management functions for the Cisco 7200 VXR routers and also holds the system memory and environmental monitoring functions.

The NPE-G1 consists of one board with multiple interfaces. The board is keyed so that it can be used only in the Cisco 7200 VXR routers.

For information about installation and configuration of the NPE-G1, see the Cisco document at the following location:

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

PA-MC-2T3+ Phase-II (T3 Subrate)

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The PA-MC-2T3+ is a single-width port adapter that provides two T3 interface connections. Each T3 interface can now be independently configured to be either channelized or unchannelized. A channelized T3 provides 28 T1 lines multiplexed into the T3. Each T1 line can be configured into one or more serial interface data channels.

Using the **no channelized** command, you can configure the T3 as a single, unchannelized serial interface data channel. You can configure this data channel to use all of the T3 bandwidth or a portion of it.

For more information about the PA-MC-2T3+, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e5/5e_ct3.htm

For information about installation and configuration of the PA-MC-2T3+, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/portadpt/multi_ch/mc_2t3/index.htm

PA-MC-8TE1+ Port Adapter

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The PA-MC-8TE1+ port adapter is a T1/E1 multichannel port adapter that provides eight DSX-1/DS1 or eight G.703 interfaces. The PA-MC-8TE1+ interfaces can be channelized, fractional, ISDN PRI, or nonframed. You configure the same port adapter to support either T1 or E1 physical links. The PA-MC-8TE1+ provides a total of 8 T1 or E1 links.

The PA-MC-8TE1+ provides up to 256 channels, as compared to a maximum of 128 for the PA-MC-8T1 (or PA-MC-8E1) port adapters. This allows for full channelization (down to the DS0 rate) for both T1 and E1 WAN links.

The PA-MC-8TE1+ supports Facility Data Link (FDL) in Extended Superframe (ESF) framing on T1 networks and network and payload loopbacks. Bit error rate testing (BERT) is supported on each of the T1 or E1 links and can run on all of the eight ports at the same time.

The PA-MC-8TE1+ provides channel group loopback. Channel group loopback for T1/E1 enables you to do section testing for a channel group without bringing down the whole T1/E1 line.

The PA-MC-8TE1+ does not support the aggregation of multiple T1s or E1s (called inverse muxing or bonding) for higher bandwidth data rates. The multichannel PA-MC-8TE1+ port adapter supports Cisco High-Level Data Link Control (HDLC), Frame Relay, PPP, and Switched Multimegabit Data Service (SMDS) Data Exchange Interface (DXI) encapsulations over each T1 or E1 link. For SMDS only, DXI is sent on the T1 or E1 line, so it needs to connect to an SMDS switch that has direct DXI input.

The PA-MC-8TE1+ has been designed to support a hardware watchdog facility in the MPC860 processor. The SRAM memory in the PA-MC-8TE1+ is mapped into the host (a Virtual Interface Processor on a Cisco 7500 series router, for example) memory space, allowing additional debugging capabilities.

For information about installation and configuration of the PA-MC-8TE1+, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/portadpt/multicha/8port_t1/index.htm

VIP4

Supported platform: Cisco 7500 series

The VIP4 is the fourth generation of Versatile Interface Processors for use with Cisco 7000 series using the Cisco 7000 series Route Switch Processor (RSP7000) and Cisco 7000 series Chassis Interface (RSP7000CI) with Cisco 7500 series (which also include the Cisco 7507-MX and Cisco 7513-MX routers). The VIP4 installs in the interface processor slots in your Cisco 7000 series or Cisco 7500 series router.

For information about installation and configuration of the VIP4, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/vip1/vip4/6927vip4.htm

VIP6-80

Supported platform: Cisco 7500 series

The Versatile Interface Processor (VIP6-80) is an option available for use with the Cisco 7500 series and the Cisco 7000 series using the Cisco 7000 series Route Switch Processor (RSP7000) and Cisco 7000 series Chassis Interface (RSP7000CI). The VIP6-80 improves high-performance switching over previous generation VIPs.

The VIP6-80 supports online insertion and removal (OIR), a feature that allows you to remove and replace a VIP6-80 without first shutting down the system. However, VIP6-80 does not support OIR of port adapters (PAs). The VIP6-80 is removed before the port adapter is removed or installed.

The VIP6-80 also supports Single Line Card Reload (SLCR), a feature that enables a failed line card to reload on the network backplane without reloading other line cards.

The VIP6-80 supports any combination of LAN and WAN PAs, including Fast Ethernet, T1/E1, High-Speed Serial Interface (HSSI), T3/E3, T3/E3 ATM, multichannel T1/E1, multichannel T3/E3, OC-3 ATM, Packet over SONET (POS), and OC-12 ATM.

For information about installation and configuration of the VIP6-80, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/vip1/14372v68.htm

New Software Features in Cisco IOS Release 12.2(14)S

This section describes new and changed features in Cisco IOS Release 12.2(14)S. Some features may be new to Cisco IOS Release 12.2S 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(14)S. 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.

Any Transport over MPLS Features

The following sections describe various Any Transport over Multiprotocol Label Switching (AToM) features. For more information about the AToM features, see the Cisco document at the following location:

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

ATM AAL5 over MPLS

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The ATM AAL5 over MPLS feature provides an ATM permanent virtual circuit (PVC) for transporting ATM adaptation layer 5 (AAL5) protocol data units (PDUs) across an IP/Multiprotocol Label Switching (MPLS) backbone with rate-limit policing and configurable PVC priority values. A dynamic MPLS tunnel is configured to enable label imposition and disposition of encapsulated ATM PDUs transported between two edge routers having a Label Distribution Protocol (LDP) neighbor relationship.

Each routed PVC label stack has two levels of labels prepended to each ATM PDU: an Interior Gateway Protocol (IGP) stack consisting of zero or more labels and a PVC-based label. Label imposition and disposition are performed by routers at the edge of the MPLS backbone. The imposition router takes the ATM PDU and encapsulates it in an MPLS PDU for transport to the correct disposition router. The disposition router takes the MPLS PDU, de-encapsulates the ATM PDU, and delivers it to the correct ATM interface and virtual path identifier/virtual circuit identifier (VPI/VCI).

Cell Relay over MPLS

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

With ATM cell relay functionality, ATM cells can be transported across Multiprotocol Label Switching (MPLS) networks transparently. This setup allows transportation of ATM signaling and Operations, Administration, and Maintenance (OAM) cells across a packet network, making a packet network invisible to the ATM network. The ATM Cell Relay over MPLS feature enables service providers to use the same tools for provisioning and to aggregate the existing frame and ATM installations to a high-speed packet core that is based on IP/MPLS.

Ethernet over MPLS

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The Ethernet over MPLS (EoMPLS) feature enables you to connect two VLAN networks that are in different locations, without using expensive bridges, routers, or switches at the VLAN locations. You can enable the Multiprotocol Label Switching (MPLS) backbone network to accept Layer 2 VLAN traffic by configuring the label edge routers (LERs) at both ends of the MPLS backbone.

Frame Relay over MPLS

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

With the Frame Relay over MPLS feature, Frame Relay traffic can be encapsulated in Multiprotocol Label Switching (MPLS) packets and forwarded over an MPLS backbone to other Frame Relay destinations. Service providers can quickly add new sites with less effort than with typical Frame Relay provisioning.

HDLC over MPLS

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The HDLC over MPLS feature enables a customer router to emulate a High-Level Data Link Control (HDLC) connection to another customer router across the packet backbone. Like PPP, this technology allows transportation of Cisco HDLC frames across the packet networks. HDLC over Multiprotocol Label Switching (MPLS) also works in transparent mode.

PPP over MPLS

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The PPP over MPLS feature enables service providers to encapsulate PPP frames across a Multiprotocol Label Switching (MPLS) core in order to emulate a PPP link across any layer transport. Using PPP over MPLS on Packet-over-SONET (POS) links enables service providers to create a “multiplexed” subinterface that can then be used to individually peer with other providers.

PPP over MPLS further enables service providers to provide a transparent PPP pass-through where the customer-edge routers can exchange the traffic via an end-to-end PPP session. Service providers can offer a virtual leased-line solution and use the PPP subinterface capability to peer with multiple providers via a single POS connection.

PPP over MPLS Restrictions

The following restrictions pertain to the PPP over MPLS feature:

- Zero hops between provider edge (PE) routers: Zero hops on one router is not supported. However, you can configure back-to-back PE routers.
- Asynchronous interfaces: Asynchronous interfaces are not supported. The connections between customer edge (CE) and PE routers on both ends of the backbone must have similar link layer characteristics. The connections between the CE and PE routers must both be synchronous.
- Multilink PPP: Multilink PPP (MLP) is not supported.
- Distributed CEF (dCEF): On the Cisco 7500 series, distributed processing for PPP over MPLS is not supported. This restriction does not affect other features that are processed in distributed mode.

BGP Features

The following sections describe various Border Gateway Protocol (BGP) features.

BGP 4 MIB Support for per-Peer Received Routes

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The BGP 4 MIB Support for per-Peer Received Routes feature introduces a new table in the CISCO-BGP4-MIB that provides the capability to query (by using Simple Network Management Protocol commands) for routes that are learned from individual Border Gateway Protocol (BGP) peers.

For more information about the BGP 4 MIB Support for per-Peer Received Routes features, see the Cisco document at the following location:

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

BGP Conditional Route Injection

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Cisco IOS software provides several methods to originate a prefix into the Border Gateway Protocol (BGP) routing table. The existing methods include using the **network** or **aggregate-address** commands and redistribution. These methods assume the existence of more specific routing information (matching the route to be originated) in either the routing table or the BGP table.

The BGP Conditional Route Injection feature enables you to originate a prefix into a BGP routing table without the corresponding match. The routes are injected into the BGP table only if certain conditions are met. The most common condition is the existence of a less specific prefix.

The BGP Conditional Route Injection feature is configured using the **bgp inject-map** command. The **bgp inject-map** command uses two route maps (inject-map and exist-map) to install one or more new prefixes into a BGP routing table. The exist-map specifies the prefixes that the BGP speaking router will track. The inject-map defines the prefixes that will be created and installed into the local BGP table.

For more information about the BGP Conditional Route Injection feature, see the Cisco document at the following location:

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

BGP Hide Local-Autonomous System

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

When the **neighbor local-as** command is configured on a Border Gateway Protocol (BGP) speaking router, the local autonomous system number is automatically prepended to all routes that are learned from external peers by default. This behavior makes changing the autonomous system number for a service provider or large existing BGP network difficult because paths, with the prepended autonomous system number, will be rejected by internal routers that are configured with the same autonomous system number. For example, if the network operator configures an internal router with the **neighbor 10.0.0.2 local-as 20** command, all paths that are learned from the 10.0.0.2 external peer will have the autonomous system number 20 prepended. Internal routers that are configured with the autonomous number 20 will detect these routes as routing loops and reject them. This behavior required a network operator to change the autonomous system number for all internal peers at the same time in order to change the autonomous system number for a BGP network.

The BGP Hide Local-Autonomous System feature introduces the **no-prepend** keyword to the **neighbor local-as** command. The use of the **no-prepend** keyword will allow a network operator to configure a BGP speaker to not prepend the local autonomous system number to any routes that are received from external peers. This feature can be used to help transparently change the autonomous system number of a BGP network and ensure that routes can be propagated throughout the autonomous system, while the autonomous system number transition is incomplete. Because the local autonomous system number is not prepended to these routes, external routes will not be rejected by internal peers during the transition from one autonomous system number to another.

Caution Configuring this feature incorrectly could potentially create routing loops and should be attempted only by an experienced network operator.

For more information about the BGP Hide Local-Autonomous System feature, see the Cisco document at the following location:

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

BGP Hybrid CLI Support

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The BGP Hybrid CLI Support feature allows the network operator to configure the Border Gateway Protocol (BGP) using the Network Layer Reachability Information (NLRI) format for IPv4 unicast commands and the address-family identifier (AFI) format for address family commands, such as IPv6, VPNv4, and Connectionless Network Service (CLNS) protocol commands.

For more information about the BGP Hybrid CLI Support feature, see the Cisco document at the following location:

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

BGP Link Bandwidth

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The BGP Link Bandwidth feature is used to advertise the bandwidth of an autonomous system exit link as an extended community. The BGP Link Bandwidth feature is supported by the internal BGP (iBGP) and external BGP (eBGP) multipath features. The link bandwidth extended community indicates the preference of an autonomous system exit link in terms of bandwidth. The link bandwidth extended community attribute may be propagated to all iBGP peers and used with the BGP multipath features to configure unequal cost load balancing. When a router receives a route from a directly connected external neighbor and advertises this route to iBGP neighbors, the router may advertise the bandwidth of that link.

The link bandwidth extended community attribute is a 4-byte value that is set by the network administrator on the demilitarized zone (DMZ) interface that connects two single hop eBGP peers. The link bandwidth extended community attribute should be used as a traffic sharing value relative to other paths while forwarding traffic. Two paths are designated as equal for load balancing if the weight, local-pref, as-path length, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) costs are the same.

For more information about the BGP Link Bandwidth feature, see the Cisco document at the following location:

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

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

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN feature allows you to configure multipath load balancing with both external BGP (eBGP) and internal BGP (iBGP) paths in Border Gateway Protocol (BGP) networks that are configured to use Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). This feature provides improved load-balancing deployment and service offering capabilities and is useful for multihomed autonomous systems and provider edge (PE) routers that import both eBGP and iBGP paths from multihomed and stub networks.

BGP installs up to the maximum number of paths allowed (configured using the **maximum-paths** command). BGP uses the best path algorithm to select one multipath as the best path, insert the best path into the routing information base (RIB), and advertise the best path to BGP peers. Other multipaths may be inserted into the RIB, but only one path will be selected as the best path.

Note See the **maximum-paths** command documentation to determine the maximum number of configurable paths.

The multipaths are used by Cisco Express Forwarding (CEF) to perform load balancing, which can be performed on a per-packet or per-source or destination-pair basis. The BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN feature performs unequal cost load balancing by default by selecting BGP paths that do not have an equal cost of the Interior Gateway Protocol (IGP). In order to enable this feature, configure the router with MPLS VPNs that contain VPN routing and forwarding instances (VRFs) that import both eBGP and iBGP paths. The number of multipaths can be configured separately for each VRF.

Note The BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN feature will operate within the configuration parameters of the existing outbound routing policy.

For more information about the BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN feature, see the Cisco document at the following location:

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

BGP Named Community Lists

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Border Gateway Protocol (BGP) communities are attributes that are used to group and filter routes. Communities are designed to give the network operator the ability to apply policies to large numbers of routes by using match and set clauses in the configuration of route maps. Community lists are used in this process to identify and filter routes by their common attributes.

The BGP Named Community Lists feature introduces a new type of community list called the named community list. The BGP Named Community Lists feature allows the network operator to assign meaningful names to community lists and increases the number of community lists that can be configured. A named community list can be configured with regular expressions and with numbered community lists. All rules of numbered communities apply to named community lists except that there is no limitation on the number of community attributes that can be configured for a named community list.

Note Both standard and expanded community lists have a limitation of 100 community groups that can be configured within each type of list. A named community list does not have this limitation.

For more information about the BGP Named Community Lists feature, see the Cisco document at the following location:

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

BGP Policy Accounting

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The BGP Policy Accounting feature provides a means of charging customers according to the route that their traffic travels. Trans-Pacific, Trans-Atlantic, satellite, domestic, and other provider traffic can be identified and accounted for on a per-customer basis when customers are on a unique software interface. This feature also allows the accounting of traffic to known autonomous system numbers in order to better engineer and plan network circuit peering and transit agreements.

The BGP Policy Accounting feature classifies IP traffic by autonomous system number, autonomous system path, or community list, and increments packet and byte counters per input interface. It performs this function using route maps to classify the traffic into one of eight possible indexes, which represent a traffic classification.

For more information about the BGP Policy Accounting feature, see the Cisco document at the following location:

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

BGP Prefix-Based Outbound Route Filtering

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The BGP Prefix-Based Outbound Route Filtering feature uses Border Gateway Protocol (BGP) outbound route filter (ORF) send and receive capabilities to minimize the number of BGP updates that are sent between peer routers. The configuration of this feature can help reduce the amount of resources required for generating and processing routing updates by filtering out unwanted routing updates at the source. For example, this feature can be used to reduce the amount of processing required on a router that is not accepting full routes from a service provider network.

The BGP Prefix-Based Outbound Route Filtering feature is enabled through the advertisement of ORF capabilities to peer routers. The advertisement of the ORF capability indicates that a BGP-speaking router will accept a prefix list from a neighbor and apply the prefix list to locally configured ORFs (if any exist). When this capability is enabled, the BGP speaker can install the inbound prefix list filter to the remote peer as an outbound filter, which reduces unwanted routing updates.

The BGP Prefix-Based Outbound Route Filtering feature can be configured with send, receive, or send and receive ORF capabilities. The local peer advertises the ORF capability in send mode. The remote peer receives the ORF capability in receive mode and applies the filter as outbound policy. The local and remote peers exchange updates to maintain the ORF for each router. Updates are exchanged between peer routers by address family depending on the ORF prefix list capability that is advertised. The remote peer starts sending updates to the local peer after it receives a route refresh request or an ORF prefix list with immediate status. The BGP speaker will continue to apply the inbound prefix list to received updates after the speaker pushes the inbound prefix list to the remote peer.

For more information about the BGP Prefix-Based Outbound Route Filtering feature, see the Cisco document at the following location:

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

Bidirectional PIM

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Bidirectional PIM (bidir-PIM) is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco IOS implementation of PIM supports three modes for a multicast group:

- Bidirectional mode
- Dense mode
- Sparse mode

A router can simultaneously support all three modes or any combination of them for different multicast groups. In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be for a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. This technique is the preferred configuration method for establishing a redundant RP configuration for bidir-PIM.

Membership to a bidirectional group is signalled via explicit join messages. Traffic from sources is unconditionally sent up the shared tree toward the RP and passed down the tree toward the receivers on each branch of the tree.

Bidir-PIM is designed to be used for many-to-many applications within individual PIM domains. Multicast groups in bidirectional mode can scale to an arbitrary number of sources without incurring overhead because of the number of sources.

Bidir-PIM is derived from the mechanisms of PIM-SM and shares many shortest-path tree (SPT) operations. Bidir-PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but no registering process for sources as in PIM-SM. These modifications are necessary and sufficient to allow forwarding of traffic in all routers solely on the basis of the (*, G) multicast routing entries. This feature eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

Note As of Cisco IOS Release 12.2 and later releases, bidir-PIM is disabled by default and must be explicitly enabled by configuring the **ip pim bidir-enable** command in global configuration mode.

Cisco 7500 Single Line Card Reload

Supported platform: Cisco 7500 series

The Cisco 7500 Single Line Card Reload feature, the only method of correcting a line card hardware failure or a severe software error for one line card on a Cisco 7500 series router, requires the execution of a CBus Complex, a process that reloads every line card on the network backplane. The time it takes to complete the CBus Complex is often inconvenient, and no network traffic can be routed or switched during the CBus Complex process.

The Single Line Card Reload (SLCR) feature enables users to correct a line card failure on a Cisco 7500 series router by reloading the failed line card without reloading any other line cards on the network backplane. During the single line card reload process, all physical lines and routing protocols on the other line cards of the network backplane remain active. A single line card reload is also significantly faster than the CBus Complex process.

The SLCR feature works on all RSP images for all Cisco IOS releases that support the SLCR feature.

For more information about the SLCR feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e5/e5_slcr.htm

Cisco IOS Server Load Balancing (SLB)

Supported platforms: Cisco 7200 series

The Cisco IOS Server Load Balancing (SLB) feature is a Cisco IOS software-based solution that provides IP server load balancing. Using the Cisco IOS SLB feature, you can define a virtual server that represents a group of real servers in a cluster of network servers known as a server farm. In this environment, the clients connect to the IP address of the virtual server. When a client initiates a connection to the virtual server, the Cisco IOS SLB function chooses a real server for the connection based on a configured load-balancing algorithm.

Cisco IOS SLB also provides firewall load balancing, which balances flows across a group of firewalls called a firewall farm.

Note Cisco IOS SLB does not support load balancing of flows between clients and real servers that are on the same LAN or VLAN. The packets that are being load balanced cannot enter and leave the load-balancing device on the same interface.

Cisco IOS SLB provides the following functions and capabilities:

- Algorithms for Server Load Balancing:
  - Weighted Round Robin
  - Weighted Least Connections
- Alternate IP Addresses
- Automatic Server Failure Detection
- Automatic Unfail
- Backup Server Farms
- Bind ID Support (also referred to as “Specifying a Bind ID”)
- CISCO-SLB-MIB
- Client-Assigned Load Balancing
- Content Flow Monitor Support
- Delayed Removal of TCP Connection Context
- Dynamic Feedback Protocol for Cisco IOS SLB
- Firewall Load Balancing
- GPRS Load Balancing
- Maximum Connections
- Multiple Firewall Farm Support
- Network Address Translation (NAT)
- Port-Bound Servers
- Probes (HTTP probes, ping probes, and WSP probes)
- Protocol Support
- Redundancy Enhancements (Stateless and Stateful Backup, and Active Standby)
- Route Health Injection
- Slow Start
- Sticky Connections
- SynGuard
- TCP Session Reassignment
- Transparent Webcache Load Balancing
- WAP Load Balancing

For more information about Cisco IOS SLB, see the Cisco document at the following location:

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

Cisco Quality of Service Device Manager

Supported platforms: Cisco 7200 series, Cisco 7500 series that are VIP-enabled

Cisco Quality of Service Device Manager (QDM) is a web-based Java application through which you can configure and monitor advanced IP-based quality of service (QoS) functionality within Cisco routers.

QDM is available as a separate product and may be downloaded free of charge.

For more information about QDM, see the *Release and Installation Notes for Cisco Quality of Service Device Manager* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qdm/

Class-Based Quality of Service MIB

Supported platforms: Cisco 7200 series, Cisco 7500 series

The Class-Based Quality of Service MIB (Class-Based QoS MIB) provides read access to QoS configurations. This MIB also provides QoS statistics information based on the modular quality of service command-line interface (MQC), including information regarding class-map and policy-map parameters.

The Class-Based QoS MIB actually consists of two MIBs: CISCO-CLASS-BASED-QOS-MIB and CISCO-CLASS-BASED-QOS-CAPABILITY-MIB.

For more information, see the Cisco Network Management Toolkit for the MIBs at the following location:

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

DCBWFQ, DWRED, and DLLQ Support for PA-A3-8E1IMA and PA-A3-8T1IMA Port Adapters on Cisco 7500 Series Routers

Supported platform: Cisco 7500 series

PA-A3-8E1IMA and PA-A3-8T1IMA port adapters on Cisco 7500 series now support Distributed Class-Based WFQ (DCBWFQ), Distributed Weighted Random Early Detection (DWRED), and Distributed Low Latency Queueing (DLLQ).

Distributed Class-Based WFQ

Weighted Fair Queueing (WFQ) offers dynamic, fair queueing that divides bandwidth across queues of traffic based on weights. WFQ ensures that all traffic is treated fairly, given its weight.

Distributed Class-Based WFQ (DCBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes on the VIP. These user-defined traffic classes are configured in the Modular Quality of Service Command-Line Interface feature. For information on how to configure quality of service (QoS) with the modular quality of service command-line interface (MQC), see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xe/120xe5/mqc/mcli.htm

For information on how to configure DCBWFQ, see the "Configuring Weighted Fair Queueing" chapter in the "Congestion Management" part of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.1, at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt2/qcdwfq.htm

Distributed Weighted Random Early Detection

Weighted Random Early Detection (WRED), the Cisco implementation of Random Early Detection (RED), combines the capabilities of the RED algorithm with IP precedence to provide preferential traffic handling for higher priority packets. It can selectively discard lower priority traffic when the interface begins to get congested and can provide differentiated performance characteristics for different classes of service.

Distributed WRED (DWRED) is the Cisco high-speed version of WRED. The DWRED algorithm was designed with Internet service providers (ISPs) in mind; it allows an ISP to define minimum and maximum queue depth thresholds and drop capabilities for each class of service.

For more information about DWRED, see the "Quality of Service Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.1, at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcdintro.htm

Distributed Low Latency Queueing

Distributed Low Latency Queueing (DLLQ) enables you to specify low latency behavior for a traffic class. LLQ allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

DLLQ also introduces the ability to limit the depth of a device transmission ring. Before the introduction of DLLQ, the maximum transmission ring depth was not a user-configurable parameter. Therefore, particles could accumulate on a transmission ring without limitation, which could result in unavoidable high latencies. DLLQ allows users to limit the number of particles that may exist on a transmission ring, effectively lowering the latency incurred by packets sitting on that transmission ring.

For more information about DLLQ, see the Cisco document at the following location:

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

PA-A3-8E1IMA and PA-A3-8T1IMA

For more information about the PA-A3-8E1IMA and PA-A3-8T1IMA port adapters, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/portadpt/atm_port/a3_8t_8e/index.htm

DFP Agent Subsystem

Supported platforms: Cisco 7200 series

The Dynamic Feedback Protocol (DFP) enables a DFP agent in a local load-balancing environment to collect status information from one or more real host servers, convert the information to relative weights, and report the weights to a DFP manager, such as a Cisco IOS Server Load Balancing (SLB) device. The DFP manager factors in the weights when load balancing the real servers. DFP also supports global load-balancing environments, with Cisco IOS SLB reporting weights to DistributedDirector.

In earlier Cisco IOS releases, the DFP agent was implemented only in Cisco IOS SLB. The new DFP Agent Subsystem feature enables client subsystems other than Cisco IOS SLB to act as DFP agents. However, currently Cisco IOS SLB is the only supported subsystem. You can use multiple DFP agents from different client subsystems at the same time.

For more information about DFP, see the Cisco document at the following location:

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

DiffServ Compliant Weighted Random Early Detection

Supported platform: Cisco 7500 series

Note The DiffServ Compliant Weighted Random Early Detection feature is also referred to as the Differentiated Services Compliant Distributed Weighted Random Early Detection feature or as the DiffServ Compliant DWRED feature.

The DiffServ Compliant Weighted Random Early Detection feature enables Weighted Random Early Detection (WRED) to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet. The DSCP value is the first six bits of the IP type of service (ToS) byte.

For more information about the DiffServ Compliant Weighted Random Early Detection feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e5/dsdwrede.htm

Distributed GRE Tunneling Support

Supported platform: Cisco 7500 series

The Distributed GRE Tunneling Support feature allows Cisco IOS software to switch packets into and out of the generic routing encapsulation (GRE) tunnels using distributed Cisco Express Forwarding (dCEF). The tunneling is performed using recursive or “double” switching techniques that are currently deployed on existing nondistributed platforms. The relevant bits are ported into this development.

Double switching is performed by the handling of the received IP packet in the existing code path until it is determined that the packet needs encapsulation or de-encapsulation. Recursively forwarding the IP packet through the IP switching path again explains the “double” aspect of the switching.

For more information about the Distributed GRE Tunneling Support feature, see the Cisco document at the following location:

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

Distributed Network-Based Application Recognition

Supported platforms: Cisco 7500 series

Distributed Network-Based Application Recognition (dNBAR) introduces the existing NBAR feature for Cisco 7500 series that are configured with a Versatile Interface Processor (VIP).

The dNBAR feature allows packet classification by adding intelligent network classification to network infrastructures. dNBAR is a classification engine that recognizes a wide variety of applications, including web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments.

When an application is recognized and classified by dNBAR, a network can invoke services for that specific application. dNBAR ensures that network bandwidth is used efficiently by working with quality of service (QoS) features to provide the following features:

- Guaranteed bandwidth
- Bandwidth limits
- Traffic shaping

- Traffic policing
- Packet marking

For more information about the dNBAR feature, see the Cisco document at the following location:

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

DLR Enhancements: PGM RFC-3208 Compliance

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

In compliance with RFC 3208, the DLR Enhancements feature adds off-tree designated local repairer (DLR) support and redirecting poll response (POLR) capability for upstream DLRs to the Cisco implementation of Pragmatic General Multicast (PGM).

Enhanced Password Security, Phase I

Supported platforms: Cisco 7200 series, Cisco 7500 series

Using the Enhanced Password Security feature, you can configure Message Digest 5 (MD5) encryption for username passwords. Before the introduction of this feature, there were two types of passwords associated with usernames. Type 0 is a clear text password visible to any user who has access to privileged mode on the router. Type 7 is a password with a weak, exclusive-or type encryption. Type 7 passwords can be retrieved from the encrypted text by using publicly available tools.

MD5 encryption is a one-way hash function that makes reversal of an encrypted password impossible, providing strong encryption protection. Using MD5 encryption, you cannot retrieve clear text passwords. MD5 encrypted passwords cannot be used with protocols that require that the clear text password be retrievable, such as Challenge Handshake Authentication Protocol (CHAP).

Use the **username (secret)** command to configure a username and an associated MD5 encrypted secret.

For more information about the Enhanced Password Security, Phase I feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e8/8e_md5.htm

EXEC Commands in Configuration Mode

Supported platforms: Cisco 7200 series, Cisco 7500 series

You can now issue EXEC-level Cisco IOS commands (such as **show**, **clear**, and **debug** commands) from within global configuration mode or other modes by issuing the **do** command followed by the EXEC command.

For more information about the EXEC-level Cisco IOS commands, see the Cisco document at the following location:

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

Express RTP Header Compression

Supported platform: Cisco 7200 series

Before the introduction of the Express RTP Header Compression feature, if compression of Real-Time Transport Protocol (RTP) headers was enabled, compression was performed in the process-switching path. That meant that packets traversing interfaces that had RTP header compression enabled were queued and passed up to the process to be switched. This procedure slowed down transmission of the packet, and therefore some users preferred to fast-switch uncompressed RTP packets.

Now, if RTP header compression is enabled, it occurs by default in the fast-switched path or the Cisco Express Forwarding switched (CEF-switched) path, depending on which switching method is enabled on the interface. Furthermore, the number of RTP header compression connections was increased to 1000 connections each.

If neither fast switching nor CEF switching is enabled, then if RTP header compression is enabled, it will occur in the process-switched path as before.

For more information about the Express RTP Header Compression feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e4/rtpfast.htm

Frame Relay Queueing and Fragmentation at the Interface

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The Frame Relay Queueing and Fragmentation at the Interface feature introduces support for low latency queueing (LLQ) and FRF.12 end-to-end fragmentation on a Frame Relay interface. This new feature simplifies the configuration of low latency, low jitter quality of service (QoS) by enabling the queueing policy and fragmentation configured on the interface to apply to all permanent virtual circuits (PVCs) and subinterfaces under that main interface. Before the introduction of this feature, queueing and fragmentation had to be configured on each individual PVC. Subrate shaping can also be configured on the interface.

For more information about the Frame Relay Queueing and Fragmentation at the Interface feature, see the Cisco document at the following location:

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

Functionality Changed for the tunnel mpls traffic-eng autoroute metric Command

Supported platforms: Cisco 7200 series, Cisco 7500 series

The default behavior of the **tunnel mpls traffic-eng autoroute metric** interface configuration command has been changed in Cisco IOS Release 12.2(14)S. This command now combines the costs of all Intermediate System-to-Intermediate System (IS-IS) routes that are downstream from a Traffic Engineering (TE) tunnel into an additive path metric. IS-IS uses the additive path metric to set the metric of the TE tunnel.

Generic Routing Encapsulation (GRE) Tunnel Keepalive

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The Generic Routing Encapsulation (GRE) Tunnel Keepalive feature provides the capability of configuring keepalive packets to be sent over IP-encapsulated GRE tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive.

For more information about the Generic Routing Encapsulation (GRE) Tunnel Keepalive feature, see the Cisco document at the following location:

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

GLBP: Gateway Load Balancing Protocol

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The Gateway Load Balancing Protocol (GLBP) feature provides automatic router backup for IP hosts that are configured with a single default gateway on an IEEE 802.3 LAN. Multiple first-hop routers on the LAN combine to offer a single virtual first-hop IP router while sharing the IP packet forwarding load between them. Other routers on the LAN may act as redundant GLBP routers that will become active if any of the existing forwarding routers fail.

For more information about GLBP, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs_glbp2.htm

iBGP Multipath Load Sharing

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

When a Border Gateway Protocol (BGP) speaking router with no local policy configured receives multiple network layer reachability information (NLRI) from the internal BGP (iBGP) for the same destination, the router will choose one iBGP path as the best path. The best path is then installed in the IP routing table of the router.

The iBGP Multipath Load Sharing feature enables the BGP speaking router to select multiple iBGP paths as the best paths to a destination. The best paths or multipaths are then installed in the IP routing table of the router. The iBGP Multipath Load Sharing feature functions similarly in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) with a service provider backbone.

For multiple paths to the same destination to be considered as multipaths, the following criteria must be met:

- All attributes must be the same. The attributes include weight, local preference, autonomous system path (entire attribute and not just length), origin code, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance.
- The next hop router for each multipath must be different.

Even if the criteria are met and multiple paths are considered multipaths, the BGP speaking router will still designate one of the multipaths as the best path and advertise this best path to its neighbors.

For more information about the iBGP Multipath Load Sharing feature, see the Cisco document at the following location:

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

IGMP State Limit

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

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

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

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Note The IGMP Version 3—Explicit Tracking of Hosts, Groups, and Channels feature is also referred to as the Explicit Tracking of Hosts, Group, and Channels for IGMP Version 3 feature.

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to neighboring multicast routers. IGMP is available in versions 1, 2, and 3. The Explicit Tracking of Hosts, Groups, and Channels for IGMP Version 3 feature enables a multicast router to explicitly track the membership of all multicast hosts in a particular multiaccess network. This enhancement to the Cisco IOS implementation of IGMPv3 enables the router to keep track of each individual host that is joined to a particular group or channel. The main benefits of this feature are that it provides minimal leave latencies, faster channel changing, and improved diagnostics capabilities for IGMP.

For more information about IGMPv3 and related features such as Source Specific Multicast (SSM), see the *Cisco IOS IP Configuration Guide*, Release 12.2, at the following location:

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

For more information about the IGMP Version 3—Explicit Tracking of Hosts, Groups, and Channels feature, see the Cisco document at the following location:

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

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

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

When a network consists of only two networking devices that are connected to broadcast media and uses the integrated Intermediate System-to-Intermediate System (IS-IS) protocol, it is better for the system to handle the link as a point-to-point link instead of as a broadcast link. This feature introduces a new command to make IS-IS behave as a point-to-point link between the networking devices.

Using this feature provides performance improvements to the network convergence times of the customer network because the feature saves the system from electing a designated router (DR), prevents flooding from using complete sequence number PDUs (CSNPs) for database synchronization, and simplifies shortest path first (SPF) computations.

For more information about the Integrated IS-IS Point-to-Point Adjacency over Broadcast Media feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fissp2p.htm

Interface Range Configuration Mode

Supported platforms: Cisco 7200 series, Cisco 7500 series

The interface range configuration mode allows you to configure multiple interfaces with the same configuration parameters. Once you enter the interface range configuration mode, all command parameters that you enter are attributed to all interfaces within that range until you exit the interface range configuration mode.

The interface range command mode has the following syntax:

interface range {**vlan** *vlan_ID - vlan_ID*} | {{**ethernet** | **fastethernet** | **gigabitethernet** | **macro** *macro_name*} *slot/interface - interface*} [, {{**ethernet** | **fastethernet** | **gigabitethernet** | **macro** *macro_name*} *slot/interface - interface*}]

Note that the space before the dash is required, you can enter up to five comma-separated ranges, and you are not required to enter spaces before or after the comma.

Interface Range Specification

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The Interface Range Specification feature allows specification of a range of interfaces to which subsequent commands are applied and supports definition of macros that contain an interface range. The Interface Range Specification feature is implemented with the **range** keyword, which is used with the **interface** command. In the interface configuration mode with the **range** keyword, all entered commands are applied to all interfaces within the range until you exit interface configuration mode.

IP Access List Entry Sequence Numbering

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The IP Access List Entry Sequence Numbering feature allows the user to add a sequence number to every access control element (ACE) in an access control list (ACL) and simplifies and accelerates ACE resequencing.

Before the release of this feature, there is no way to specify the position of an ACE within an ACL. When a user wants to insert an ACE in the middle of an existing list, all of the ACEs after the desired position must be removed, the new ACE is then applied, and finally all deleted ACEs must be reapplied in their new positions after the new ACE. This method is cumbersome and error prone.

This feature allows users to add sequence numbers to ACEs and resequence existing ACEs. When a user adds a new ACE, the user chooses the sequence number so that it is in a desired position in the ACL. And when a new ACE must be inserted, the ACEs currently on the ACL can be resequenced to create room on the ACL to insert the new ACE.

This feature works with numbered and named ACLs, and it supports standard and extended ACLs.

For backward compatibility with previous releases, if ACEs with no sequence numbers are applied, the first ACE will have a sequence number of 10, and successive ACEs will have sequence numbers incremented by 10. The maximum sequence number is 2147483647. If the generated sequence number exceeds this maximum number, the following message is displayed:

```
Exceeded maximum sequence number.
```

If an ACE that already belongs to an existing ACL is entered without a sequence number, then it is assigned a sequence number that is 10 greater than the last sequence number in that ACL and is placed at the end of the list.

Distributed support will be provided so that the sequence numbers of ACEs in the Route Processor (RP) and LC are in synchronization at all times. Sequence numbers will not be nvgened.

If an ACE matches an already existing entry (except for the sequence number), then no changes are made. If a new ACE has a sequence number that is already present, the following error message is generated:

```
Duplicate sequence number.
```

If an ACL is entered from global configuration mode, then sequence numbers for that ACL are generated automatically.

For more information about the IP Access List Entry Sequence Numbering feature, see the Cisco document at the following location:

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

IP Event Dampening

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing tables and protocols. This feature allows the network operator to configure a router to identify and dampen flapping interfaces, which reduces the utilization of system processing resources and improves network stability and performance. This feature is configured on a per-interface basis and supports Connectionless Network Service (CLNS) and IP routing protocols.

For more information about the IP Event Dampening feature, see the Cisco document at the following location:

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

IP MMLS Global Threshold

Supported platforms: Cisco 7200 series, Cisco 7500 series

The IP Multicast Multilayer Switching (MMLS) Global Threshold feature allows you to configure a global multicast rate threshold, specified in packets per second, below which all multicast traffic is routed by the Multilayer Switch Feature Card, which prevents creation of switching cache entries for low-rate Layer 3 flows.

IPSec—SNMP Support

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The IPSec—SNMP Support feature introduces support for industry standard IP Security (IPSec) MIBs and Cisco IOS software specific IPSec MIBs. The IPSec MIBs allow IPSec configuration monitoring and IPSec status monitoring using Simple Network Management Protocol (SNMP), and can be integrated into a variety of Virtual Private Network (VPN) management solutions. Cisco IOS command-line interface (CLI) commands allow you to examine the version of the MIBs, to enable (or disable) SNMP notifications for IPSec, and to monitor and control the size of the buffers that are used by this feature.

Full details of management options can be found in the CISCO-IPSEC-FLOW-MONITOR- MIB, the CISCO-IPSEC-MIB, and the CISCO-IPSEC-POLICY-MAP-MIB. These MIB modules can be obtained from Cisco Network Management Toolkit for the MIBs at the following location:

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

For more information about the IPSec—SNMP Support feature and related Cisco IOS commands, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e4/dtipmib.htm

IPv6 Features

The following sections describe various IP version 6 (IPv6) features. For more information about the IPv6 features, see the *Cisco IOS IPv6 Configuration Library* at the following location:

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

CEFv6/dCEFv6—Cisco Express Forwarding

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Cisco Express Forwarding for IPv6 (CEFv6) is advanced, Layer 3 IP switching technology for the forwarding of IPv6 packets. Distributed CEF for IPv6 (dCEFv6) performs the same functions as CEFv6 but for distributed architecture platforms such as the Cisco 12000 series Internet routers. CEFv6 and dCEFv6 function the same and offer the same benefits as CEFv4 and dCEFv4.

In Cisco IOS Release 12.2S, dCEFv6 and CEFv6 support IPv6 addresses and prefixes, separate Forwarding Information Bases (FIBs) for IPv6 global, site-local, and link-local addresses, and a separate global FIB for each Virtual Private Network (VPN).

IPv6 CEF supports a subset of the IPv4 CEF commands using the **ipv6 cef** root rather than **ip cef**. The behavior of all commands is analogous to that of the IPv4 CEF commands. Furthermore, a number of existing CEF commands that start with the root **show cef** now display IPv6 CEF information in addition to IPv4 CEF information.C

Table 32 lists the IPv6 commands that are related to the CEFv6/dCEFv6—Cisco Express Forwarding feature and that are supported in Cisco IOS Release 12.2S.

Table 32 IPv6 Commands Related to the CEFv6/dCEFv6—Cisco Express Forwarding Feature

Command	Description
Global Configuration Commands	
ipv6 cef	Enables/disables IPv6 CEF forwarding globally. To enable IPv6 CEF, IPv4 CEF must first be enabled by configuring **ip cef**.
ipv6 cef accounting [**per-prefix**] [**prefix-length**]	Configures per IPv6 prefix accounting and/or prefix length accounting.
ipv6 cef distributed	Enables/disables IPv6 distributed forwarding globally. To enable distributed IPv6 CEF, distributed IPv4 CEF must first be enabled by configuring **ip cef distributed**.
Debug Commands	
debug ipv6 cef drops	Enables debugging of packets dropped by CEFv6 switching.
debug ipv6 cef events	Enables debugging of control plane events for CEFv6.
debug ipv6 cef hash	Enables debugging of load balancing hash setup events for CEFv6.
debug ipv6 cef receive	Enables debugging packets passed to IPv6 process level switching.
debug ipv6 cef table	Enables debugging of CEFv6 table modification events.
Show Commands	
show ipv6 cef *interface* [**detail**]	Shows all IPv6 prefixes using the specified interface.
show ipv6 cef *prefix* [**detail**]	Shows IPv6 CEF information for the specified prefix.
show ipv6 cef adjacency *adjacency*	Shows all IPv6 prefixes resolving through the specified adjacency.
show ipv6 cef non-recursive [**detail**]	Shows nonrecursive prefixes.
show ipv6 cef summary	Shows CEF table summary information.
show ipv6 cef traffic prefix-length	Shows per-prefix length accounting statistics.
show ipv6 cef unresolved	Shows unresolved prefixes
Other Commands	
show cef drop	Shows counters of IPv6 and IPv4 dropped packets.
show cef interface [**detail**] [**statistics**] *interface*	Shows CEF interface status and configuration.
show cef linecard [**detail**] [**internal**] *slot*	Shows CEF information related to line cards.
show cef not-cef-switched	Show counters of IPv6 and IPv4 packets passed on to the next switching layer.

CEFv6 Switching for Tunnels

This section discusses the following three features:

- CEFv6 Switching for 6to4 Tunnels
- CEFv6 Switching for Automatic IPv6 over IPv4 Tunnels
- CEFv6 Switching for IPv6 ISATAP Tunnels

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Cisco Express Forwarding (CEF) switching is on by default when the IP version 6 (IPv6) protocol is configured on an interface. IPv6 overlay tunneling mechanisms (6to4, automatic, and Intra-Site Automatic Tunnel Addressing Protocol [ISATAP]) use CEF to transport IPv6 packets.

For information about implementing tunneling for IPv6, see the Cisco document at the following location:

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

Cisco Discovery Protocol (CDP) - IPv6 Address Family Support for Neighbor Information

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The CDP IPv6 Address Family Support for Neighbor Information feature adds the ability to transfer IP version 6 (IPv6) addressing information between two Cisco devices using Cisco Discovery Protocol (CDP). CDP support for IPv6 addresses allows CDP to exchange IPv6 addressing information. CDP support for IPv6 addresses provides IPv6 information to network management products and troubleshooting tools.

DNS Lookups over an IPv6 Transport

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The DNS Lookups over an IPv6 Transport feature adds support for IPv6 AAAA record types over an IPv6 transport in the Domain Name System (DNS) name-to-address and address-to-name lookup processes.

IPv6 Extended Access Control Lists

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Extended access control lists in IPv6 function the same and offer the same benefits as access control lists in IPv4—IPv6 extended access lists use source and destination addresses for matching operations and IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control.

IPv6 access lists are identified by user selected names and are defined by a list of permit and deny statements entered within IPv6 access list configuration mode. Each access list statement must specify the protocol and source and destination prefixes to match against (where the **any** keyword is equivalent to the IPv6 prefix ::/0). Every IPv6 access list has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for Internet Control Message Protocol for IPv6 [ICMPv6] neighbor discovery.) IPv6 access lists can be used only to filter traffic; IPv6 prefix lists must be used to filter routing protocol prefixes.

Table 33 lists the IPv6 commands that are related to the IPv6 Extended Access Control Lists feature and that are supported in Cisco IOS Release 12.2S.

Table 33 IPv6 Commands Related to the IPv6 Extended Access Control Lists Feature

Command	Description
Global Configuration Commands	
ipv6 access-list *name*	Defines the IPv6 extended access list and enters IPv6 access list configuration mode.
ipv6 access-list log-update threshold *value*	Specifies the access list entry hit threshold when entries marked as log or log-input are logged.
IPv6 Access List Configuration Commands	
deny *protocol* {*src-prefix* | **any** | **host** *addr*} [**eq** | **neq** | **lt** | **gt** | **range** *src-ports*] {*dst-prefix* | **any** | **host** *addr*} [**eq** | **neq** | **lt** | **gt** | **range** *dst-ports*] [**undetermined-transport**] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**routing**] [**reflect** *reflexive-acl-name* [**timeout** *val*]] [**time-range** *time-range-name*] [**log** | **log-input**] [**sequence** *value*]	Specifies deny conditions for the defined access list.
permit *protocol* {*src-prefix* | **any** | **host** *addr*} [**eq** | **neq** | **lt** | **gt** | **range** *src-ports*] {*dst-prefix* | **any** | **host** *addr*} [**eq** | **neq** |**lt** | **gt** | **range** *dst-ports*] [**undetermined-transport**] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**routing**] [**reflect** *reflexive-acl-name* [**timeout** *val*]] [**time-range** *time-range-name*] [**log** | **log-input**] [**sequence** *value*]	Specifies permit conditions for the defined access list.
evaluate *reflexive-acl*	Evaluates a reflexive access list.
remark *text-string*	Allows a user to specify a description for this access list.
Clear and Debug Commands	
clear ipv6 access-list [*name*]	Clears the access list hit counters. Use the **show ipv6 access-list** command to display the number of matches for each entry.
debug ipv6 packet [**access-list** *ipv6-acl-name*] [**detail**]	Enables IPv6 packet-level debugging. The default setting is off. An access list can be specified such that only packets matching the access list permit entries are displayed.
Other Commands	
show ipv6 access-list [*name*]	Displays the currently defined access lists. The number of matches made against each access list entry is displayed and can be cleared using the **ipv6 clear access-list** command.

IPv6 for Cisco IOS Software

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

IPv6, formerly called IPng (next generation), is the latest version of IP and offers many benefits, such as a larger address space, over the previous version of IP (version 4).

In Cisco IOS Release 12.2(14)S, the IPv6 for Cisco IOS Software feature is being integrated into the 12.2S Cisco IOS software release train along with the following additional, new feature enhancements:

- Integrated Intermediate System-to-Intermediate System (IS-IS) for IPv6
- Static cache entry for IPv6 neighbor discovery
- Use of the first MAC address as the IPv6 interface identifier for point-to-point links
- Link-local address peering in multiprotocol BGP extensions for IPv6

IPv6 ISATAP Tunnel Support

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an automatic overlay tunneling mechanism that uses the underlying IP version 4 (IPv4) network as a nonbroadcast multiaccess (NBMA) link layer for IP version 6 (IPv6). The IPv4 address is encoded in the last 32 bits of the IPv6 address, enabling automatic IPv6-in-IPv4 tunneling within an IPv4 network. ISATAP tunnels allow individual IPv4/IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure. ISATAP uses a normal global IPv6 prefix (/64) which can be used with both local and global unicast IPv6 prefixes, enabling IPv6 routing on the Internet.

For information about implementing tunneling for IPv6, see the Cisco document at the following location:

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

IPv6 MIBs

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The IPv6 MIBs feature adds network management support for IP version 6 (IPv6) using Simple Network Management Protocol (SNMP). New MIB tables have been added for monitoring IP and IP forwarding traffic in an IPv6 environment.

No new or modified Cisco IOS commands are associated with this feature. For details on the MIB enhancements, see the CISCO-IETF-IP-FORWARD-MIB.my and CISCO-IETF-IP-MIB.my MIB files, available from the Cisco MIB FTP site at http://tools.cisco.com/ITDIT/MIBS/servlet/index.

IPv6 Provider Edge Router over MPLS

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The IPv6 Provider Edge Router over MPLS feature (also referred to as Cisco 6PE) enables IPv6 sites to communicate over a Multiprotocol Label Switching (MPLS) IPv4 network with no software or hardware upgrades in the core MPLS infrastructure and with no disruption to existing customer services.

IPv6 RIP Enhancements

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The IPv6 RIP Enhancements feature adds support for a separate IPv6 Routing Information Protocol (RIP) routing table, the ability to delete routes from the IPv6 RIP routing table, and the ability to set route tags. The hold-down timer default is now set to zero, and a maximum number of parallel routes can be configured.

Secure Shell (SSH) over an IPv6 Transport

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Secure Shell (SSH) in IPv6 functions the same as and offers the same benefits as SSH in IPv4—the SSH Server feature enables an SSH client to make a secure, encrypted connection to a Cisco router and the SSH Client feature enables a Cisco router to make a secure, encrypted connection to another Cisco router or to any other device running an SSH server. IPv6 enhancements to SSH consist of support for IPv6 addresses that enable a Cisco router to accept and establish secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

IS-IS: Allows BGP to Control the Configuration of the Overload Bit

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The Intermediate System-to-Intermediate System (IS-IS) protocol defines a special bit in each link-state packet (LSP) called the overload-bit. IS-IS uses the overload bit to "tell" other routers to ignore this router in their shortest path first (SPF) calculations. This function prevents transit traffic from passing through the router before the routing table has converged, and transit traffic is not lost.

This feature provides IS-IS with the ability to set the overload bit and then to wait for Border Gateway Protocol (BGP) convergence. After the BGP routing table has fully converged, BGP sends a notification to IS-IS that BGP is ready for the IS-IS protocol to unset the overload bit. When the IS-IS protocol receives the notification from BGP, IS-IS unsets the overload bit and returns the router to normal operation, allowing transit traffic to pass through the router.

The configuration of this feature allows a network operator to bring a new router into a network without immediately routing traffic through the new router. The network operator can configure the router that is running IS-IS to wait until the BGP routing table converges or the configured timer expires. The configuration of this feature can improve network performance and stability by making the router available much faster without the risk of losing traffic that is destined for other networks.

Note This feature is configured on the router that is running IS-IS and does not require any specific configuration for BGP.

This feature introduces three configuration options for the **set-overload-bit** IS-IS router configuration command. See Table 34 for syntax descriptions.

set-overload-bit [on-startup {*announce-time* | **wait-for-bgp}]**

no set-overload-bit [on-startup {*announce-time* | **wait-for-bgp}]**

Table 34 set-overload-bit Syntax Descriptions

on-startup (Optional)	Configures IS-IS to set the overload bit at startup.
announce-time (Optional)	Sets the overload bit for the specified time interval. The configurable range is from 5 to 86,400 seconds. There is no default timer value for this configuration option.
wait-for-bgp (Optional)	Sets the overload bit on the router until BGP routing tables have converged and BGP notifies IS-IS or the default timer has expired. The default timer is 600 seconds.

IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication feature adds an HMAC-MD5 digest to each Intermediate System-to-Intermediate System (IS-IS) protocol data unit (PDU). HMAC is a mechanism for message authentication codes (MAC) using cryptographic hash functions. The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing messages from being injected into the network routing domain. IS-IS clear text (plain text) authentication is enhanced so that passwords are encrypted when the software configuration is displayed and passwords are easier to manage and change.

For more information about the IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/ftismd5.htm

Low Latency Queuing for the VIP Enhancement

Supported platform: Cisco 7500 series

The optional *bytes* argument has been added to the **priority** command.

For more information about the Low Latency Queuing for the VIP feature, including information about the *bytes* argument in the **priority** command, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xe/120xe5c/llqvip.htm

Manual TFTP Certificate Enrollment

Supported platforms: Cisco 7200 series, Cisco 7500 series

The Manual TFTP Certificate Enrollment feature allows users to generate a certificate request and accept certification authority (CA) certificates, as well as the router's certificates; these tasks are accomplished via a TFTP server or manual cut-and-paste operations. Users may wish to use TFTP or manual cut-and-paste enrollment in the following situations:

- Their CA does not support Simple Certificate Enrollment Protocol (SCEP) (which is the most commonly used method for sending and receiving requests and certificates).
- A network connection between the router and CA is not possible (which is how a router running Cisco IOS software obtains it certificate).

MPLS Label Distribution Protocol (LDP)

Supported platforms: Cisco 7200 series, Cisco 7500 series

The Cisco Multiprotocol Label Switching (MPLS) label distribution protocol (LDP), as standardized by the Internet Engineering Task Force (IETF) and as enabled by Cisco IOS software, allows the construction of highly scalable and flexible IP Virtual Private Networks (VPNs) that support multiple levels of services.

LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths or LSPs, forward label

traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement the Cisco MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

LDP provides the means for label switch routers (LSRs) to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and to establish LDP sessions with those peers for the purpose of exchanging label binding information.

From an historical and functional standpoint, LDP is a superset of the Cisco prestandard Tag Distribution Protocol (TDP), which also supports MPLS forwarding along normally routed paths. For those features that LDP and TDP share in common, the pattern of protocol exchanges between network routing platforms is identical. The differences between LDP and TDP for those features supported by both protocols are largely embedded in their respective implementation details, such as the encoding of protocol messages.

This release of LDP, which supports both the LDP and TDP protocols, provides the means for transitioning an existing network from a TDP environment to an LDP environment. Thus, you can run LDP and TDP simultaneously on any router platform. The routing protocol that you select can be configured on a per-interface basis for directly connected neighbors and on a per-session basis for nondirectly connected (targeted) neighbors. In addition, an LSP across an MPLS network can be supported by LDP on some hops and by TDP on other hops.

For more information about MPLS LDP, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs2sldp.htm

MPLS Label Distribution Protocol (LDP) MIB

Supported platforms: Cisco 7200 series, Cisco 7500 series

The Multiprotocol Label Switching (MPLS) label distribution protocol (LDP) MIB (MPLS LDP MIB) has been implemented to enable standard, Simple Network Management Protocol (SNMP)-based network management of the label switching features in Cisco IOS software. Providing this capability requires SNMP agent code to execute on a designated network management system (NMS) in the network. The NMS serves as the medium for user interaction with the network management objects in the MPLS LDP MIB.

The SNMP agent embodies a layered structure that is compatible with Cisco IOS software and presents a network administrative and management interface to the objects in the MPLS LDP MIB and, thence, to the rich set of label switching capabilities supported by Cisco IOS software.

By means of an SNMP agent, you can access MPLS LDP MIB objects using standard SNMP GET operations to accomplish a variety of network management tasks. All the objects in the MPLS LDP MIB follow the conventions defined in the Internet Engineering Task Force (IETF) draft MIB entitled “draft-ietf-mpls-ldp-mib-07.txt,” which defines network management objects in a structured and standardized manner. This draft MIB is continually being evolved toward the status of a standard. Accordingly, the MPLS LDP MIB will be implemented in a manner that tracks the evolution of this IETF document.

Slight differences that exist between the IETF draft MIB and the implementation of equivalent functions in Cisco IOS software require some minor translations between the MPLS LDP MIB objects and the internal data structures of Cisco IOS software. Such translations are accomplished by the SNMP agent, which runs in the background on the NMS workstation as a low-priority process.

The extensive label switching capabilities supported in Cisco IOS software provide an integrated approach to managing the large volumes of traffic carried by WANs. These capabilities are integrated into the Layer 3 network services, thus optimizing the routing of high volume traffic through Internet service provider backbones while, at the same time, ensuring the resiliency of the network to link or node failures.

This release of Cisco IOS software supports the following functionality in relation to the MPLS LDP MIB:

- Generation and sending of event notification messages to signal changes in the status of LDP sessions.
- Enabling and disabling of event notification messages by means of extensions to existing SNMP command-line interface (CLI) commands.
- Specification of the name or the IP address of an NMS workstation in the operating environment to which Cisco IOS event notification messages are to be sent to serve network administrative and management purposes.
- Storage of the configuration that pertains to an event notification message into the NVRAM of the NMS.

The structure of the MPLS LDP MIB conforms to Abstract Syntax Notation One (ASN.1), thereby forming a highly structured and idealized database of network management objects.

Using any standard SNMP application, you can retrieve and display information from the MPLS LDP MIB by means of standard SNMP GET operations; similarly, you can traverse and display information in the MIB by means of SNMP GETNEXT operations.

Note Because the MPLS LDP MIB was not given an Internet Assigned Numbers Authority (IANA) Experimental object identifier (OID) at the time of its implementation, Cisco chose to implement the MIB under the Cisco Experimental OID number, as follows:

ciscoExperiment 1.3.6.1.4.1.9.10
mplsLdpMIB 1.3.6.1.4.1.9.10.65

If the MPLS LDP MIB is assigned an IANA Experimental OID number, Cisco will deprecate all objects in the MIB under the ciscoExperimental OID and reposition the objects under the IANA Experimental OID.

For more information about the MPLS LDP MIB, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/ldpmb2.htm

MPLS Label Switching Router MIB

Supported platforms: Cisco 7200 series, Cisco 7500 series

The Multiprotocol label Switching (MPLS) label switch router (LSR) MIB (MPLS LSR MIB) allows you to use the Simple Network Management Protocol (SNMP) to remotely monitor an LSR that is using the MPLS technology. The MPLS LSR MIB mirrors the Cisco Label Switching subsystem, specifically, the LSR management information that is provided by the Label Forwarding Information Base (LFIB).

The MPLS LSR MIB contains managed objects that support the retrieval of label switching information from a router and is based on Revision 05 of the IEFT MPLS LSR MIB. This implementation enables a network administrator to get information on the status, character, and performance of the following:

- MPLS capable interfaces on the LSR
- Incoming MPLS segments (labels) to an LSR and their associated parameters
- Outgoing segments (labels) at an LSR and their associated parameters

In addition, the network manager can retrieve the status of cross-connect entries that associate MPLS segments with each other.

For more information about the MPLS LSR MIB, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fslsrm2s.htm

MPLS Traffic Engineering (TE) Features

The following sections describe various Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) features.

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

Supported platforms: Cisco 7200 series, Cisco 7500 series

Traffic engineering automatic bandwidth adjustment provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels on the basis of their measured traffic load.

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, it periodically (for example, once per day) adjusts the tunnel's allocated bandwidth to be the largest sample for the tunnel since the last adjustment.

The frequency with which tunnel bandwidth is adjusted and the allowable range of adjustments is configurable on a per-tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate are user-configurable on a per-tunnel basis.

For more information about the MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels feature, see the Cisco document at the following location:

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

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

Supported platforms: Cisco 7200 series, Cisco 7500 series

When Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) is configured in a network, the Interior Gateway Protocol (IGP) floods two metrics for every link: the normal IGP (Open Shortest Path First [OSPF] or Intermediate System-to-Intermediate System [IS-IS]) link metric and a TE link metric. The IGP uses the IGP link metric in the normal way to compute routes for destination networks. In previous releases, MPLS TE used the TE link metric to calculate and verify paths for TE tunnels. When the traffic engineering metric was not explicitly configured, the traffic engineering metric was the IGP metric.

The current enhancement enables you to control the metric used in path calculation for TE tunnels on a per-tunnel basis. It allows you to specify that the path calculation for a given tunnel be based on either of the following:

- IGP link metrics.
- TE link metrics, which you can configure so that they represent the needs of a particular application. For example, the TE link metrics can be configured to represent link transmission delay.

For more information about the MPLS Traffic Engineering (TE)—Configurable Path Calculation Metric for Tunnels feature, see the Cisco document at the following location:

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

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

Supported platforms: Cisco 7200 series, Cisco 7500 series

Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) allows constraint-based routing of IP traffic. One of the constraints satisfied by constraint-based routing (CBR) is the availability of required bandwidth over a selected path. Diff-Serv Aware Traffic Engineering (DS-TE) extends MPLS TE to enable you to perform CBR of "guaranteed" traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. The more restrictive bandwidth is termed a *sub-pool*, while the regular TE tunnel bandwidth is called the *global pool*. (The sub-pool is a portion of the global pool.) This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher quality of service (QoS) performance (in terms of delay, jitter, or loss) for the guaranteed traffic.

For example, DS-TE can be used to ensure that traffic is routed over the network so that, on every link, there is never more than 40 percent (or any assigned percentage) of the link capacity of guaranteed traffic (for example, voice), while there can be up to 100 percent of the link capacity of regular traffic. Assuming QoS mechanisms are also used on every link to queue guaranteed traffic separately from regular traffic, it then becomes possible to enforce separate "overbooking" ratios for guaranteed and regular traffic. (In fact, for the guaranteed traffic it becomes possible to enforce no overbooking at all—or even an underbooking—so that very high QoS can be achieved end-to-end for that traffic, even while for the regular traffic a significant overbooking continues to be enforced.)

Also, through the ability to enforce a maximum percentage of guaranteed traffic on any link, the network administrator can directly control the end-to-end QoS performance parameters without having to rely on over-engineering or on expected shortest path routing behavior. This is essential for transport of applications that have very high QoS requirements (such as real-time voice, virtual IP leased line, and bandwidth trading), where over-engineering cannot be assumed everywhere in the network.

DS-TE involves extending the Open Shortest Path First (OSPF) routing protocol, so that the available sub-pool bandwidth at each preemption level is advertised in addition to the available global pool bandwidth at each preemption level. And DS-TE modifies CBR to take this more complex advertised information into account during path computation.

DS-TE enables service providers to perform separate admission control and separate route computation for discrete subsets of traffic (for example, voice and data traffic).

Therefore, by combining DS-TE with other Cisco IOS features such as QoS, the service provider can do the following:

- Develop QoS services for end customers on the basis of signaled rather than provisioned QoS.
- Build the higher-revenue generating "strict-commitment" QoS services, without over-provisioning.

- Offer virtual IP leased-line, Layer 2 service emulation and point-to-point guaranteed bandwidth services including voice-trunking.
- Use the scalability properties offered by MPLS.

For more information about the DS-TE feature, see the Cisco document at the following location:

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

MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

Supported platforms: Cisco 7200 series, Cisco 7500 series

The MPLS Traffic Engineering (TE) IP Explicit Address Exclusion feature provides a means to exclude a link or node from the path for a Multiprotocol Label Switching (MPLS) traffic engineering label-switched path (LSP).

The feature is accessible via the **ip explicit-path** command that allows you to create an IP explicit path and enter a configuration submode for specifying the path. The feature adds to the submode commands the **exclude-address** command for specifying addresses to exclude from the path.

If the exclude-address for an MPLS traffic engineering LSP identifies a flooded link, the constraint-based shortest path first (CSPF) routing algorithm does not consider that link when it computes paths for the LSP. If the exclude-address specifies a flooded MPLS traffic engineering router ID, the CSPF routing algorithm does not allow paths for the LSP to traverse the node that is identified by the router ID.

For more information about the MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion feature, see the Cisco document at the following location:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_expl_address_ps6017_TSD_Products_Configuration_Guide_Chapter.html

MPLS Traffic Engineering (TE) MIB

Supported platforms: Cisco 7200 series, Cisco 7500 series

The Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) MIB (MPLS TE MIB) enables a standardized, Simple Network Management Protocol (SNMP)-based approach to managing the MPLS traffic engineering features in Cisco IOS software. Providing this capability requires SNMP agent code implementation of the MPLS TE MIB.

The MPLS TE MIB is based on the Internet Engineering Task Force (IETF) draft MIB entitled "draft-ietf-mpls-te-mib-05.txt," which includes objects describing features that support MPLS traffic engineering. This IETF draft MIB, which undergoes revisions from time to time, is being evolved toward becoming a standard. Accordingly, the Cisco implementation of the MPLS TE MIB is expected to track the evolution of the IETF draft MIB.

Slight differences between the IETF draft MIB and the implementation of the traffic engineering capabilities within Cisco IOS software require some minor translations between the MPLS TE MIB and the internal data structures of Cisco IOS software. These translations are accomplished by means of the SNMP agent code that is installed and operating on various hosts within the network. This SNMP agent code, running in the background as a low priority process, provides a management interface to Cisco IOS software.

The SNMP objects defined in the MPLS TE MIB can be viewed by any standard SNMP utility. All MPLS TE MIB objects are based on the IETF draft MIB; accordingly, no specific Cisco SNMP application is required to support the functions and operations that pertains to the MPLS TE MIB.

The following functionality is supported in the MPLS TE MIB:

- The ability to generate and queue notification messages that signal changes in the operational status of MPLS traffic engineering tunnels.
- Extensions to existing SNMP command-line interface (CLI) commands that provide the ability to enable, disable, and configure notification messages for MPLS traffic engineering tunnels.
- The ability to specify the name or the IP address of a network management system (NMS) in the operating environment to which notification messages are to be sent.
- The ability to write notification configurations into non-volatile memory.

For more information about the MPLS TE MIB, see the Cisco document at the following location:

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

MPLS Traffic Engineering (TE)—Scalability Enhancements

Supported platforms: Cisco 7200 series, Cisco 7500 series

Implementation of Multiprotocol Label Switching (MPLS) traffic engineering scalability has been improved so that scalability performs better for large numbers of traffic engineering tunnels. These improvements enable the following:

- An increase in the number of traffic engineering tunnels that a router can support when acting as a tunnel headend and when acting as a tunnel midpoint.
- A reduction in the time required to establish large numbers of traffic engineering tunnels.

User-observable scalability enhancements include the following:

- Pacing for Resource Reservation Protocol (RSVP) messages.
- Signaling and management for MPLS traffic engineering tunnels.
- Controlling Intermediate System-to-Intermediate System (IS-IS) and MPLS traffic engineering topology database interactions.
- Improved diagnostic capabilities for MPLS traffic engineering and RSVP signaling.

Pacing for RSVP Messages

A burst of RSVP traffic engineering signaling messages can overflow the input queue of a receiving router, causing some messages to be dropped. Dropped messages cause a substantial delay in completing label-switched path (LSP) signaling.

A new mechanism controls the transmission rate for RSVP messages and reduces the likelihood of input drops on the receiving router. The default transmission rate is 200 RSVP messages per second to a given neighbor. The rate is configurable.

Signaling and Management for MPLS Traffic Engineering Tunnels

The following changes improve the responsiveness of LSP recovery when a link used by an LSP fails:

- When the upstream end of a failed link detects the failure, it generates an RSVP No Route path error message. This enables the LSP headend to detect the link failure and initiate recovery, even when the Interior Gateway Protocol (IGP) update that announces the link failure is delayed.
- The LSP headend marks the link in question so that subsequent constraint-based shortest path first (SPF) calculations ignore the link until either a new IGP update arrives or a configurable timeout occurs. This ensures that resignaling to restore the LSP avoids the failed link.

Controlling IS–IS and MPLS Traffic Engineering Topology Database Interactions

The delay between when the IS-IS protocol receives an IGP update and when it delivers the update to the MPLS traffic engineering topology database has been reduced in most situations.

Previously, when IS-IS received a new LSP that contained traffic engineering type, length, and value (TLV) objects, a delay of several seconds could occur before IS-IS passed the traffic engineering TLVs to the traffic engineering database. The purpose of the delay was to provide better scalability during periods of network instability and to give the router an opportunity to receive more fragments of the LSP before passing the information to the traffic engineering database. However, this delay increased the convergence time for the traffic engineering database.

Now IS-IS extracts traffic engineering TLVs from received LSPs and passes them to the traffic engineering database immediately. The exception to this occurs when there are large numbers of LSPs to process and it is important to limit CPU consumption, such as during periods of network instability.

The arguments that control IS-IS delivery of traffic engineering TLVs to the traffic engineering topology database are configurable.

Improved Diagnostic Capabilities for MPLS Traffic Engineering and RSVP Signaling

The following enhancements improve diagnostic and troubleshooting capabilities for MPLS traffic engineering and RSVP:

- Counters record tunnel headend error events such as no route (link down), preemption, and insufficient bandwidth on a per-tunnel basis.
- Counters record RSVP messages. The counters are per-interface and record the number of RSVP messages of each type sent and received on the interface.

More Information

For more information about the MPLS Traffic Engineering (TE)—Scalability Enhancements feature, see the Cisco document at the following location:

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

MPLS VPN Features

The following sections describe various Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) features.

MPLS Virtual Private Networks

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The IP Virtual Private Network (VPN) feature for Multiprotocol Label Switching (MPLS) allows a Cisco IOS network to deploy scalable IP version 4 (IPv4) Layer 3 VPN backbone services. An IP VPN is the foundation that companies use for deploying or administering value-added services including applications and data hosting network commerce, and telephony services to business customers. In private LANs, IP-based intranets have fundamentally changed the way companies conduct their business. Companies are moving their business applications to their intranets to extend over a WAN. Companies are also embracing the needs of their customers, suppliers, and partners by using extranets (an intranet that encompasses multiple businesses). With extranets, companies reduce business process costs by facilitating supply-chain automation, electronic data interchange (EDI), and other forms of network commerce. To take advantage of this business opportunity, service providers must have an IP VPN infrastructure that delivers private network services to businesses over a public infrastructure.

MPLS VPNs offer the following benefits:

- A platform for rapid deployment of additional value-added IP services, including intranets, extranets, voice, multimedia, and network commerce.
- Privacy and security equal to that provided by Layer 2 VPNs by limiting the distribution of VPN routes to only those routers that are members of the VPN seamless integration with customer intranets.
- Increased scalability over current VPN implementations, with thousands of sites per VPN and hundreds of thousands of VPNs per service provider IP class of service (CoS), with support for multiple classes of service and priorities within VPNs, as well as between VPNs.
- Management of VPN membership and provisioning of new VPNs for rapid deployment.
- Scalable any-to-any connectivity for extended intranets and extranets that encompass multiple businesses.

For more information about the MPLS Virtual Private Networks feature, see the Cisco document at the following location:

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

MPLS VPN Carrier Supporting Carrier

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Carrier supporting carrier is a term that is used to describe a situation in which one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

The carrier supporting carrier feature enables one Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN)-based service provider to allow other service providers, such as Internet service providers (ISPs) or a Border Gateway Protocol (BGP)/MPLS VPN service providers, to use a segment of its backbone network.

For more information about the MPLS VPN Carrier Supporting Carrier feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs2scsc.htm

MPLS VPN Carrier Supporting Carrier—IPv4 BGP Label Distribution

Supported platforms: Cisco 7200 series, Cisco 7500 series

The MPLS VPN Carrier Supporting Carrier—IPv4 BGP Label Distribution feature enables you to configure your carrier supporting carrier network to enable Border Gateway Protocol (BGP) to transport routes and Multiprotocol Label Switching (MPLS) labels between the backbone carrier provider edge (PE) routers and the customer carrier customer edge (CE) routers. The backbone carrier offers BGP and MPLS Virtual Private Network (VPN) services. The customer carrier can be either of the following:

- An Internet service provider (ISP) with an IP core
- An MPLS service provider with or without VPN services

Previously you had to use Label Distribution Protocol (LDP) and an Internal Gateway Protocol (IGP) between PE and CE routers to achieve the same goal. Using BGP to distribute IPv4 routes and MPLS label routes has the following benefits:

- BGP takes the place of an IGP and LDP. You can use BGP to distribute routes and MPLS labels. Using a single protocol instead of two simplifies the configuration and troubleshooting.
- BGP is the preferred routing protocol for connecting two ISPs, mainly because of its routing policies and ability to scale. ISPs commonly use BGP between two providers. This feature enables those ISPs to use BGP.

For more information about the MPLS VPN Carrier Supporting Carrier—IPv4 BGP Label Distribution feature, see the Cisco document at the following location:

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

MPLS VPN ID

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Using the MPLS VPN ID feature, you can identify Virtual Private Networks (VPNs) by a VPN identification (ID) number, as described in RFC 2685. This implementation of the MPLS VPN ID feature is used for identifying a VPN. The MPLS VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with Multiprotocol Label Switching (MPLS) VPN ID numbers in routing updates.

Multiple VPNs can be configured in a router. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the router. Alternately, you can use a VPN ID to identify a particular VPN in the router. The VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the routers in the service provider network that services that VPN.

You can use several applications, such as RADIUS and Dynamic Host Configuration Protocol (DHCP), to manage VPNs by VPN ID.

Note Configuration of a VPN ID for a VPN is optional. You can still use a VPN name to identify configured VPNs in the router. The VPN name is not affected by the VPN ID configuration. The VPN name and the VPN ID configuration are two independent mechanisms to identify VPNs.

For more information about the MPLS VPN ID feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/vpnid2.htm

MPLS VPN Inter-AS—IPv4 BGP Label Distribution

Supported platforms: Cisco 7200 series, Cisco 7500 series

The MPLS VPN Inter-AS—IPv4 BGP Label Distribution feature enables you to set up a Virtual Private Network (VPN) service provider (SP) network to exchange IPv4 routes with Multiprotocol Label Switching (MPLS) labels. You can configure the VPN service provider network as follows:

- Route reflectors exchange VPNv4 routes, using multihop, multiprotocol External Border Gateway Protocol (EBGP). This configuration also preserves the next hop information and the VPN labels across the autonomous systems.

- A local provider edge (PE) router needs to know the routes and label information for the remote PE router. This information can be exchanged between the PE routers and autonomous system boundary routers (ASBRs) in one of two ways:
  - Internal Gateway Protocol (IGP) and Label Distribution Protocol (LDP): the ASBR can redistribute the IPv4 routes and MPLS labels that it learned from EBGP into IGP and LDP and vice versa.
  - Internal Border Gateway Protocol (IBGP) IPv4 label distribution: the ASBR and PE router can use direct IBGP sessions to exchange VPNv4 and IPv4 routes and MPLS labels.

    Alternatively, if you enable the ASBR to exchange IPv4 routes and MPLS labels with the route reflector, the route reflector can reflect the IPv4 routes and MPLS labels learned from the ASBR to the PE routers in the VPN. The route reflector also reflects the VPNv4 routes to the PE routers in the VPN (as mentioned in the first bullet). Using the route reflectors to store the VPNv4 routes and forward them through the PE routers and ASBRs allows for a scalable configuration.
- ASBRs exchange IPv4 routes and MPLS labels for the PE routers, using EBGP.

Using Border Gateway Protocol (BGP) to distribute IPv4 routes and MPLS label routes has the following benefits:

- Improved scalability because the route reflectors store VPNv4 routes.
- Ability to enable a non-VPN core network to act as a transit network for VPN traffic.
- Elimination of the need for any other LDP between adjacent label switch routers (LSRs).

For more information about the MPLS VPN Inter-AS—IPv4 BGP Label Distribution feature, see the Cisco document at the following location:

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

MPLS VPN—SNMP MIB Support

Supported platforms: Cisco 7200 series, Cisco 7500 series

Simple Network Management Protocol (SNMP) agent code that is operating in conjunction with the Provider-Provisioned Virtual Private Network (PPVPN) Multiprotocol Label Switching (MPLS) VPN MIB (PPVPN MPLS VPN MIB) enables a standardized, SNMP-based approach in managing MPLS VPNs in Cisco IOS software.

The PPVPN MPLS VPN MIB is based on the Internet Engineering Task Force (IETF) draft MIB "draft-ietf-ppvpn-mpls-vpn-mib-03.txt," which includes objects describing features that support MPLS VPN events. This IETF draft MIB, which undergoes revisions from time to time, is evolving toward becoming a standard. The Cisco implementation of features of the PPVPN MPLS VPN MIB is expected to track the evolution of the IETF draft MIB and may change accordingly.

Some slight differences between the IETF draft MIB and the actual implementation of MPLS VPNs within Cisco IOS software require some minor translations between the PPVPN MPLS VPN MIB and the internal data structures of Cisco IOS software. These translations are accomplished by means of the SNMP agent code. Also, while running as a low priority process, the SNMP agent provides a management interface to Cisco IOS software. SNMP adds little overhead to the normal functions of the device.

The SNMP objects that are defined in the PPVPN MPLS VPN MIB can be viewed by any standard SNMP utility. The network administrator can retrieve information in the PPVPN MPLS VPN MIB using standard SNMP **get** and **getnext** operations for SNMP v1, v2, and v3.

All PPVPN-MPLS-VPN MIB objects are based on the IETF draft MIB; thus, no specific Cisco SNMP application is required to support the functions and operations that pertain to the PPVPN MPLS VPN MIB features.

In Cisco IOS Release 12.2(14)S, the PPVPN MPLS VPN MIB provides you with the ability to do the following:

- Gather routing and forwarding information for MPLS VPNs on a router.
- Expose information in the VPN routing/forwarding (VRF) routing table.
- Gather information on Border Gateway Protocol (BGP) configuration related to VPNs and VRF interfaces and statistics.
- Emit notification messages that signal changes when critical MPLS VPN events occur.
- Enable, disable, and configure notification messages for MPLS VPN events by using extensions to existing SNMP command-line interface (CLI) commands.
- Specify the IP address of a network management system (NMS) in the operating environment to which notification messages are sent.
- Write notification configurations into nonvolatile memory.

For more information about the MPLS VPN—SNMP MIB Support feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsvnmb2s.htm

Multicast-VPN—IP Multicast Support for MPLS VPNs

Supported platforms: Cisco 7200 series, Cisco 7500 series

The Multicast-VPN—IP Multicast Support for MPLS VPNs feature enables a service provider to configure and support multicast traffic in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment. This feature supports routing and forwarding of multicast packets for each individual VPN routing and forwarding (VRF) instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone.

The Multicast-VPN—IP Multicast Support for MPLS VPNs feature in Cisco IOS software provides the ability to support the multicast feature over a Layer 3 VPN. As enterprises extend the reach of their multicast applications, service providers can accommodate these enterprises over their MPLS core network. IP multicast is used to stream video, voice, and data to an MPLS VPN network core.

A VPN is network connectivity across a shared infrastructure, such as an internet service provider (ISP). Its function is to provide the same policies and performance as a private network, at a reduced cost of ownership, thus creating many opportunities for cost savings through operations and infrastructure.

Historically, IP in IP generic route encapsulation (GRE) tunnels was the only way to connect through a service provider network. Although such tunneled networks tend to have scalability issues, they represent the only means of passing IP multicast traffic through a VPN.

MPLS was derived from tag switching and various other vendor methods of IP-switching support enhancements in the scalability and performance of IP-routed networks by combining the intelligence of routing with the high performance of switching. MPLS is now used for VPNs, which is an appropriate combination because MPLS decouples information used for forwarding of the IP packet (the label) from the information carried in the IP header.

A Multicast-VPN allows an enterprise to transparently interconnect its private network across the network backbone of a service provider. The use of a Multicast-VPN to interconnect an enterprise network in this way does not change the way that enterprise network is administered, nor does it change general enterprise connectivity.

Because MPLS VPNs support only unicast traffic connectivity, deploying the Multicast-VPN feature in conjunction with MPLS VPN allows service providers to offer both unicast and multicast connectivity to MPLS VPN customers.

For more information about the Multicast-VPN—IP Multicast Support for MPLS VPNs feature, see the Cisco document at the following location:

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

Multilink Frame Relay (FRF.16)

Supported platforms: Cisco 7200 series, Cisco 7400 series

The Multilink Frame Relay (FRF.16) feature introduces functionality that is based on the Frame Relay Forum's Multilink Frame Relay UNI/NNI Implementation Agreement (FRF.16). This feature provides a cost-effective way to increase bandwidth for particular applications by enabling multiple serial links to be aggregated into a single bundle of bandwidth. Multilink Frame Relay is supported on User-Network Interfaces (UNI) and Network-to-Network Interfaces (NNIs) in Frame Relay networks.

For more information about the Multilink Frame Relay feature, see the Cisco document at the following location:

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

Multilink PPP Minimum Links Mandatory

Supported platforms: Cisco 7200 series, Cisco 7500 series

Multilink PPP (MLP) allows for the establishing of multiple PPP links in parallel to the same destination. This is often used with dialup lines or ISDN connections to easily increase the amount of bandwidth between points.

With the introduction of the Multilink PPP Minimum Links Mandatory feature, you can configure the minimum number of links in an MLP bundle required to keep that bundle active by entering the **multilink min-links** *links* **mandatory** command. When you configure this command, all Network Control Protocols (NCPs) for an MLP bundle are disabled until the MLP bundle has the required minimum number of links. When a new link is added to the MLP bundle that brings the number of links up to the required minimum number of links, the NCPs are activated for the MLP bundle. When a link is removed from an MLP bundle, and the number of links falls below the required minimum number of links for that MLP bundle, the NCPs are disabled for that MLP bundle.

For more information about the Multilink PPP Minimum Links Mandatory feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e11/12e_mlp.htm

NetFlow Features

The following sections describe various NetFlow features.

NetFlow Multiple Export Destinations

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to the destination host. Currently, the maximum number of export destinations allowed is two. The NetFlow Multiple Export Destinations feature is available only if NetFlow is configured.

For more information about the NetFlow Multiple Export Destinations feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s19/12s_mdnf.htm

NetFlow Subinterface Support

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The NetFlow Subinterface Support feature provides the ability to enable NetFlow on a per-subinterface basis. In a scenario in which your network contains thousands of subinterfaces and you want to collect export records for only a few interfaces, you can fine-tune your collection of data to only specified subinterfaces. The result is a lower bandwidth requirement for NetFlow Data Export (NDE) and reduced platform requirements for NetFlow data collection devices.

For more information about the NetFlow Subinterface Support feature, see the Cisco document at the following location:

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

NetFlow ToS-Based Aggregation

Supported platforms: Cisco 7200 series, Cisco 7200 series, Cisco 7500 series

The NetFlow ToS-Based Router Aggregation feature provides the ability to enable limited router-based type of service (ToS) aggregation of NetFlow Export data, which results in summarized NetFlow Export data to be exported to a collection device. The results are lower bandwidth requirements for NetFlow Export data and reduced platform requirements for NetFlow data collection devices.

For more information about the NetFlow ToS-Based Router Aggregation feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/dtnfltos.htm

Network-Based Application Recognition

Supported platform: Cisco 7200 series

Network-Based Application Recognition (NBAR) allows you to add intelligent network classification to network infrastructures. NBAR is a classification engine that recognizes a wide variety of applications, including web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application.

NBAR ensures that network bandwidth is used efficiently by working with quality of service (QoS) features to provide the following:

- Guaranteed bandwidth
- Bandwidth limits
- Traffic shaping
- Packet coloring
- Packet marking

In addition, NBAR supports the following:

- Citrix, including matching on Citrix application name.
- Novadigm and Printer protocols.
- Subport classification of HTTP traffic by host name. You can classify HTTP traffic by web server names. To perform a match on the host-name portion of the URL, use the new Host matching criteria.

For more information about the NBAR feature, see the Cisco document at the following location:

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

Network-Based Application Recognition RTP Payload Classification

Supported platforms: Cisco 7200 series, Cisco 7500 series that are VIP-enabled

Note The Network-Based Application Recognition RTP Payload Classification feature is also referred to as NBAR Heuristics and NBAR Heuristics Matching.

The RTP Payload Type Matching enhancement has been added to the Network-Based Application Recognition (NBAR) feature. With the addition of NBAR RTP Payload Type Matching, Real-Time Transport Protocol (RTP) traffic can now be classified as a protocol within the modular quality of service command-line interface (MQC) framework.

For additional information about the NBAR feature, including NBAR RTP Payload Type Matching, see the Cisco document at the following location:

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

OSPF Features

The following sections describe various Open Shortest Path First (OSPF) features.

OSPF Sham-Link Support for MPLS VPN

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Note The OSPF Sham-Link Support for MPLS VPN feature is also referred to as the MPLS VPN - OSPF and Sham-Link Support feature.

In a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) configuration, the Open Shortest Path First (OSPF) protocol is one way you can connect customer edge (CE) routers to service provider edge (PE) routers in the VPN backbone. OSPF is often used by customers who run OSPF as their intrasite routing protocol, subscribe to a VPN service, and want to exchange routing information between their sites using OSPF (during migration or on a permanent basis) over an MPLS VPN backbone.

Using an OSPF sham-link in an MPLS VPN has the following benefits:

- Client site connection across the MPLS VPN backbone: a sham-link overcomes the OSPF default behavior for selecting an intra-area backdoor route between VPN sites instead of an interarea (PE-to-PE) route. A sham-link ensures that OSPF client sites that share a backdoor link can communicate over the MPLS VPN backbone and participate in VPN services.
- Flexible routing in an MPLS VPN configuration: nn an MPLS VPN configuration, the OSPF cost configured with a sham-link allows you to decide if OSPF client site traffic will be routed over a backdoor link or through the VPN backbone.

For more information about the OSPF Sham-Link Support for MPLS VPN feature, see the Cisco document at the following location:

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

OSPF Shortest Paths First Throttling

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The OSPF Shortest Paths First Throttling feature makes it possible to configure Shortest Paths First (SPF) scheduling in intervals of milliseconds and to delay SPF calculations during network instability. SPF calculates the Shortest Path Tree (SPT) when there is a change in topology. One SPF run may include multiple topology change events.

The interval at which SPF runs is dynamically chosen, based on the frequency of topology changes. However, this automatically selected interval is still within the range of values that are defined by the user. If the network topology is unstable, SPF throttling calculates SPF scheduling intervals to be of longer duration until the network topology becomes stable again.

For more information about the OSPF Shortest Paths First Throttling feature, see the Cisco document at the following location:

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

OSPF Stub Router Advertisement

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The OSPF Stub Router Advertisement feature allows you to bring a new router into a network without immediately routing traffic through the new router and allows you to gracefully shut down or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration options that allow you to configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum or infinite metric to all neighbors.

When any of these three configuration options are enabled on a router, the router will originate link-state advertisements (LSAs) with a maximum metric (LSInfinity: 0xFFFF) through all nonstub links. The advertisement of a maximum metric causes other routers to assign a cost to this router that is higher than the cost of using an alternate path. Because of the high cost that is assigned to paths that pass through this router, other routers will not use a path through this router as a transit path to forward traffic that is destined for other networks, allowing switching and routing functions to be up and running and routing tables to converge before transit traffic is routed through this router.

Note Directly connected links in a stub network are not affected by the configuration of a maximum or infinite metric because the cost of a stub link is always set to the output interface cost.

For more information about the OSPF Stub Router Advertisement feature, see the Cisco document at the following location:

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

OSPF Support for Multi-VRF on CE Routers

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The OSPF Support for Multi-VRF on CE Routers feature provides the capability of suppressing provider edge (PE) checks. The checks are needed to prevent loops when the PE is performing a mutual redistribution of packets between Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP). When Virtual Private Network routing/forwarding (VRF) is used on a router that is not a PE (that is, one that is not running BGP), the checks can be turned off to allow for correct population of the VRF routing table with routes to IP prefixes.

The OSPF Support for Multi-VRF on CE Routers feature allows you to split the router into multiple virtual routers, where each contains its own set of interfaces, routing table, and forwarding table. On the basis of routing information that is stored in the VRF IP routing table and VRF Cisco Express Forwarding (CEF) table, packets are forwarded to their destination using Multiprotocol Label Switching (MPLS).

The OSPF Support for Multi-VRF on CE Routers feature gives you the ability to segment or single out parts of your network and to configure those segments to perform specific functions, yet still maintaining correct routing information.

For more information about the OSPF Support for Multi-VRF on CE Routers feature, see the Cisco document at the following location:

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

OSPF Update Packet-Pacing Configurable Timers

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

In rare situations, you might need to change Open Shortest Path First (OSPF) packet-pacing default timers to mitigate CPU or buffer utilization issues that are associated with flooding large numbers of link-state advertisements (LSAs). The OSPF Update Packet-Pacing Configurable Timers feature allows you to configure the rate at which OSPF LSA flood pacing, retransmission pacing, and group pacing updates occur.

Configuring OSPF flood pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPF transmission queue. Configuring OSPF retransmission pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPF retransmission queue. Cisco IOS software groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval that is used for group LSA refreshment; however, this timer does not change the frequency at which individual LSAs are refreshed (the default refresh occurs every 30 minutes).

Note The default settings for OSPF packet pacing timers are suitable for the majority of OSPF deployments. You should change the default timers only as a last resort.

For more information about the OSPF Update Packet-Pacing Configurable Timers feature, see the Cisco document at the following location:

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

Per-VC Queueing for ATM

Supported platforms: Cisco 7200 series, Cisco 7400 series

The Cisco IOS quality of service (QoS) software includes queueing mechanisms such as low latency queueing (LLQ), weighted fair queueing (WFQ) and class-based WFQ (CBWFQ). These mechanisms are typically configured at the interface level, the subinterface level, or the per-virtual circuit (VC) level. With the Per-VC Queueing for ATM feature, these queueing mechanisms are configured at the per-VC level using Parallel Express Forwarding (PXF).

When configuring CBWFQ and LLQ on a per-VC level using PXF, the following functionality is not supported:

- Classifying traffic based on MAC address, QoS groups, input interfaces, or Multiprotocol Label Switching (MPLS) experimental (EXP) value.
- Queueing Frame Relay class maps.
- Configuring hierarchical policy maps.

Note PXF does not include support for VC bundles. If VC bundles are configured in the Per-VC Queueing for ATM feature, PXF will not be used as the packet forwarding mechanism. Instead, Cisco Express Forwarding (CEF) will be used.

PIM Features

The following sections describe various Protocol Independent Multicast (PIM) features.

Multicast Subsecond Convergence

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The Multicast Subsecond Convergence feature comprises a comprehensive set of features and protocol enhancements that provide for improved scalability and convergence in multicast-based services. This feature set provides for the ability to scale to larger services levels and to recover multicast forwarding after service failure in subsecond time frames.

Multicast subsecond convergence allows you to send Protocol Independent Multicast (PIM) router-query messages (PIM hellos) every few milliseconds. In earlier releases, you could send the PIM hellos every few seconds. By enabling a router to send PIM hello messages more often, this feature allows the router to discover unresponsive neighbors more quickly. As a result, the router can implement failover or recovery procedures more efficiently.

The scalability enhancements improve on the efficiency of handling increases (or decreases) in service users (receivers) and service load (sources or content). Scalability enhancements in this release include the following:

- Improved Internet Group Management Protocol (IGMP) and PIM state maintenance through new timer management techniques
- Improved scaling of the Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache

The scalability enhancements provide the following benefits:

- Increased potential PIM multicast route (mroute), IGMP, and MSDP SA cache state capacity
- Decreased CPU usage

For more information about the Multicast Subsecond Convergence feature, see the Cisco document at the following location:

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

PIM MIB Extension for IP Multicast

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Protocol Independent Multicast (PIM) is an IP multicast routing protocol used for routing multicast data packets to multicast groups. The PIM MIB Extension for IP Multicast feature introduces the Cisco implementation of the PIM MIB (CISCO-PIM-MIB), which is based on RFC 2934 (Protocol Independent Multicast MIB for IPv4). The PIM MIB describes objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP). It supports dense mode and sparse mode operations of PIM.

The Cisco implementation of the PIM MIB provides the following trap enhancements to the existing version of the PIM MIB for IPv4:

- Traps for indicating when a multicast neighbor on a multicast interface is lost.
- Traps for monitoring Auto-RP sessions.
- Traps for monitoring the PIM protocol on PIM-enabled interfaces.

The Cisco implementation of the PIM MIB introduces the following modifications to the existing version of the PIM MIB for IPv4:

- The “pimIpMRouteTable” table was added. It displays PIM-specific ipMRoute entries.
- The “pimIpMRouteNextHopTable” table was added. It displays PIM-specific ipMRouteNextHop entries.
- The “pimInterfaceVersion” object was deleted.
- The “pimNeighborLoss” trap was added. It detects the loss of a multicast neighbor on a multicast interface.

For complete details on the Cisco implementation of the PIM MIB, see the CISCO-PIM-MIB.my file available from the Cisco MIB website on Cisco.com at the following location:

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

For more information about the PIM MIB Extension for IP Multicast feature, see the Cisco document at the following location:

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

PIM Multicast Scalability

Supported platforms: Cisco 7200 series, Cisco 7500 series

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

Quality of Service Feature for Parallel Express Forwarding (PXF)

Supported platforms: Cisco 7200 VXR routers with the Cisco Network Services Engine (NSE-1) Services Accelerator, Cisco 7400 series

The Quality of Service (QoS) feature, Generic Traffic Shaping (GTS), is being introduced for Parallel Express Forwarding (PXF). Note the following points:

- The **shape** (policy-map class) command was revised to include the following usage guideline for supporting PXF:

  When configuring GTS, a maximum of 256 classes can be configured in a policy map. However, for traffic shaping to be enabled along the PXF path, the maximum number of classes that can be configured in a policy map is 64. If more than 64 classes are configured, packets switched to interfaces using the policy map will be redirected to the route processor (RP).
- The **shape adaptive** command and the **shape fecn-adapt** command are not supported in the PXF path. If either command is configured, packets switched to interfaces using the policy map will be redirected to the RP.

For more information about QoS features, see the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.2, and the *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.2 T.

Quality of Service over LAN Emulation

Supported platforms: Cisco 7200 series, Cisco 7500 series

Note The Quality of Service over LAN Emulation feature is also referred to as the Local-Area Network Emulation Quality of Service feature.

The Quality of Service over LAN Emulation feature provides the capability to differentiate multiple classes of traffic by creating virtual channel connections (VCCs) with the desired quality of service (QoS) parameters. When prioritized traffic is received, the LAN Emulation (LANE) Client (LEC) forwards this traffic on a VCC with matching QoS parameters.

Currently, LANE QoS supports the creation of Unspecified Bit Rate+ (UBR+) VCCs. A UBR+ VCC is a UBR VCC for which the minimum cell rate (MCR) is guaranteed by the switch. If the switch cannot guarantee the rate you that you have specified for the UBR+ VCC, the LEC will revert to UBR with no MCR guarantee.

You can enable or disable the LANE QoS feature on a per-LEC basis by entering the **qos** option in the **lane client** command. The same emulated LAN (ELAN) can contain both QoS-capable and non-QoS-capable LECs.

For more information about the Quality of Service over LAN Emulation feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/lqos.htm

Route Processor Redundancy Plus (RPR+)

Supported platform: Cisco 7500 series

The Route Processor Redundancy Plus (RPR+) feature is an enhancement to the RPR feature. RPR+ keeps Versatile Interface Processors (VIPs) or Supervisor Engines from being reset and reloaded when a switchover occurs between the active and standby Route Switch Processors (RSPs) or Supervisor Engine.

Because VIPs are not reset on the Cisco 7500 series router, microcode is not reloaded on the VIPs, the time needed to parse the configuration is eliminated, and switchover time is reduced to 30 to 40 seconds.

Feature	Switchover Time	Notes
High System Availability (HSA)	8 to 10 minutes	System default
RPR	4 to 5 minutes	VIPs and legacy interface processors supported
RPR+	30 to 40 seconds	VIPs supported[1]
Stateful Switchover	7 seconds	—

1. Legacy interface processors default to RPR. A message similar to the following is displayed during switchover:

```
%HA-2-NO_Quiesce: Slot 11 did not quiesce, it will be disabled and then reloaded.
```

For more information about the RPR+ redundancy feature for the Cisco 7500 series, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/fs22rpr.htm

RSVP Scalability Enhancements

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

Resource Reservation Protocol (RSVP) typically performs admission control, classification, policing, and scheduling of data packets on a per-flow basis and keeps a database of information for each flow. RSVP scalability enhancements let you select a resource provider (formerly called a quality of service [QoS] provider) and disable data packet classification so that RSVP performs admission control only. This facilitates integration with service provider (differentiated services [Diff-Serv]) networks and enables scalability across enterprise networks.

Class-based weighted fair queueing (CBWFQ) provides the classification, policing, and scheduling functions. CBWFQ puts packets into classes based on the differentiated services code point (DSCP) value in the packet's Internet Protocol IP header, thereby eliminating the need for per-flow state and per-flow processing.

For more information about the RSVP Scalability Enhancements feature, see the Cisco document at the following location:

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

SNMP Support for VLAN Subinterfaces

Supported platforms: Cisco 7200 series, Cisco 7500 series

The SNMP Support for VLAN Subinterfaces feature provides MIB-2 interfaces sparse table support for Fast Ethernet subinterfaces. This enhancement is similar to the functionality supported in Frame Relay subinterfaces.

For more information about the SNMP Support for VLAN Subinterfaces feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e7/ft_snmpv.htm

Tunnel Type of Service (ToS)

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

The Tunnel Type of Service (ToS) feature allows you to configure the ToS and Time-to-Live (TTL) byte values in the encapsulating IP header of tunnel packets for an IP tunnel interface on a router. The Tunnel ToS feature is supported on Cisco Express Forwarding (CEF), fast switching, and process switching forwarding modes.

Turbo Access Control Lists

Supported platforms: Cisco 7200 series, Cisco 7500 series

Access control lists (ACLs) are normally searched sequentially to find a matching rule, and ACLs are ordered specifically to take this factor into account. Because of the increasing needs and requirements for security filtering and packet classification, ACLs can expand to the point at which searching the ACL adds a significant amount of time and memory when packets are being forwarded. Moreover, the time taken by the router to search the list is not always consistent, adding a variable latency to the packet forwarding. A high CPU load is necessary for searching an ACL with several entries.

The Turbo Access Control Lists feature, also referred to as the Turbo ACL feature, compiles the ACLs into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries.

The feature has the following benefits:

- For ACLs larger than three entries, the CPU load required to match the packet to the predetermined packet-matching rule is lessened. The CPU load is fixed, regardless of the size of the ACL, allowing for larger ACLs without incurring any CPU overhead penalties. The larger the ACL, the greater the benefit.
- The time taken to match the packet is fixed, so that latency of the packets is smaller (significantly in the case of large ACLs) and more importantly, consistent, providing better network stability and more accurate transit times.

For more information about the Turbo ACL feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e4/turbacl.htm

Virtual Router Redundancy Protocol

Supported platforms: Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

- Proxy ARP—The client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router will respond to the ARP request with its own MAC address.
- Routing protocol—The client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- IRDP (ICMP Router Discovery Protocol) client—The client runs an Internet Control Message Protocol (ICMP) router discovery client.

The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

The Virtual Router Redundancy Protocol (VRRP) feature can solve the static configuration problem. VRRP enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

VRRP is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, and on MPLS VPNs and VLANs.

For more information about the Virtual Router Redundancy Protocol feature, see the Cisco document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st18/st_vrrpx.htm

MIBs

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

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

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

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

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

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

Limitations and Restrictions

The following sections contain information about limitations and restriction in Cisco IOS Release 12.2S that can apply to the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 routers, Cisco 7400 series routers, Cisco 7500 series routers, Cisco ONS 15530 platform, and Cisco ONS 15540 platform.

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 http://tools.cisco.com/ITDIT/MIBS/servlet/index. 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 12.2 S that can apply to the Cisco 7200 series routers, Cisco 7301 router, Cisco 7304 routers, Cisco 7400 series routers, Cisco 7500 series routers, Cisco ONS 15530 platform, and Cisco ONS 15540 platform.

Deferrals

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

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

Field Notices and Bulletins

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

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

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

Important Notes for Cisco IOS Release 12.2(25)S15

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(25)S15.

NBAR Classification for HTTP Traffic on NPE-G100

When using a NPE-G100 to classify HTTP traffic with NBAR, the configuration is different than how it would be done on software-based platforms. To get the feature to function correctly on the NPE-G100, it requires an *action* accompanied under the class referenced in the policy-map i.e. police, set, etc. It is not enough to configure just “match protocol http”. Here is a working example:

```
class-map match-any http
  match protocol http
!
policy-map nbar_test
  class http
  set ip precedence 2
!
interface GigabitEthernet2
 ip address 211.1.1.1 255.255.255.0
 service-policy output nbar_test
!
```

Important Notes for Cisco IOS Release 12.2(25)S

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(25)S.

High-Capacity Counters in the Output of the show interfaces Command

The counters in the output of the **show interfaces** command for the Cisco ONS 15530 and Cisco ONS 15540 now support a higher capacity than in previous Cisco IOS releases.

Memory Requirements for the VIP2-40 and VIP2-50

The minimum memory requirements for both a VIP2-40 and a VIP2-50 are 64 MB. These requirements apply to all Cisco IOS 12.2S releases.

Important Notes for Cisco IOS Release 12.2(22)S

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(22)S.

Changes to the Output of the show version Command

The output of the **show version** EXEC command has been modified slightly to reflect general updates to Cisco IOS software. If you are currently using any automated tools (such as scripts) that parse the output of the **show version** EXEC command, you should review the new output format and make changes as needed.

Important Notes for Cisco IOS Release 12.2(20)S

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(20)S.

Protocol Independent Multicast on Cisco 7304 Routers

Beginning in Cisco IOS Release 12.2(20)S, Protocol Independent Multicast (PIM) does not function on Cisco 7304 routers. This is a temporary situation that we plan on correcting as soon as we possibly can in a future Cisco IOS release.

Important Notes for Cisco IOS Release 12.2(14)S18

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(14)S18.

RPR and RPR+ for the Cisco 7500 Series Routes

Cisco IOS Release 12.2(14)S18 does not support Route Processor Redundancy (RPR+) and RPR Plus (RPR)+ for the Cisco 7500 series routers.

Important Notes for Cisco IOS Release 12.2(14)S

This section describes important issues that you should be aware of for Cisco IOS Release 12.2(14)S.

Configuring MD5 Authentication for BGP Peering Sessions

This document provides general information about deploying MD5 authentication for a BGP session. You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection. If authentication is invoked and a segment fails authentication, then an error message will be displayed in the console.

Old Behavior

In previous versions of Cisco IOS software, configuring MD5 authentication for a BGP peering session was generally considered to be difficult because the initial configuration and any subsequent MD5 configuration changes required the BGP neighbor to be reset.

New Behavior

This behavior has been changed in current versions of Cisco IOS software. CSCdx23494 (integrated in Cisco IOS release 12.2(14)S) introduced a change to MD5 authentication for BGP peering sessions. The BGP peering session does not need to be reset to maintain or establish the peering session for initial configuration or after the MD5 configuration has been changed. However, the configuration must be completed on both the local and remote BGP peer before the BGP hold timer expires. If the hold down timer expires before the MD5 configuration has been completed on both BGP peers, the BGP session will time out.

The following example enables the authentication feature between this router and the BGP neighbor at 10.108.1.1. The password that must also be configured for the neighbor is *bla4u00=2nkq*. The remote peer must be configured before the holddown timer expires.

```
router bgp 109
 neighbor 10.108.1.1 password bla4u00=2nkq
```

When the password has been configured, the MD5 key is applied to the tcp session immediately. If one peer is configured before the other, the TCP segments will be discarded on both the local and remote peers due to an authentication failure. The peer that is configured with the password will print an error message in the console similar to the following:

```
  00:03:07: %TCP-6-BADAUTH: No MD5 digest from 10.0.0.2(179) to 10.0.0.1(11000)
```

The time period in which the password must changed is typically the life time of a stale BGP session. When the password or MD5 key is configured, incoming TCP segments will only be accepted if the key is known. If the key is unknown on both the remote and local peer, the TCP segments will be dropped, and the BGP session will time out when the holddown timer expires.

If the BGP session has been preconfigured with a hold time of 0 seconds, no keepalive messages will be sent. The BGP session will stay up until one of the peers, on either side, tries to transmit a message (For example, a prefix update).

Note Configuring a new timer value for the holddown timer will only take effect after the session has been reset. So, it is not possible to change the configuration of the holddown timer to avoid resetting the BGP session.

PPP over MPLS Restrictions

The following restrictions pertain to the PPP over MPLS feature:

- Zero hops between provider edge (PE) routers: Zero hops on one router is not supported. However, you can configure back-to-back PE routers.
- Asynchronous interfaces: Asynchronous interfaces are not supported. The connections between customer edge (CE) and PE routers on both ends of the backbone must have similar link layer characteristics. The connections between the CE and PE routers must both be synchronous.
- Multilink PPP: Multilink PPP (MLP) is not supported.
- Distributed CEF (dCEF): On the Cisco 7500 series, distributed processing for PPP over MPLS is not supported. This restriction does not affect other features that are processed in distributed mode.

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 12.2S is based on Cisco IOS Release 12.2, many caveats that apply to Cisco IOS Release 12.2 also apply to Cisco IOS Release 12.2S. 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 **Technical Support & Documentation > Tools & Resources > Bug Toolkit** (which is listed under Troubleshooting). Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

This section consists of the following subsections:

Release 12.2(30)S and its rebuilds:

- Resolved Caveats—Cisco IOS Release 12.2(30)S1, page 143
- Open Caveats—Cisco IOS Release 12.2(30)S, page 144
- Resolved Caveats—Cisco IOS Release 12.2(30)S, page 144

Release 12.2(25)S and its rebuilds:

- Resolved Caveats—Cisco IOS Release 12.2(25)S15, page 157
- Resolved Caveats—Cisco IOS Release 12.2(25)S14, page 158
- Resolved Caveats—Cisco IOS Release 12.2(25)S13, page 161
- Resolved Caveats—Cisco IOS Release 12.2(25)S12, page 171
- Resolved Caveats—Cisco IOS Release 12.2(25)S11, page 174
- Resolved Caveats—Cisco IOS Release 12.2(25)S10, page 179
- Resolved Caveats—Cisco IOS Release 12.2(25)S9, page 182
- Resolved Caveats—Cisco IOS Release 12.2(25)S8, page 186
- Resolved Caveats—Cisco IOS Release 12.2(25)S7, page 191
- Resolved Caveats—Cisco IOS Release 12.2(25)S6, page 192
- Resolved Caveats—Cisco IOS Release 12.2(25)S5, page 203
- Resolved Caveats—Cisco IOS Release 12.2(25)S4, page 211
- Resolved Caveats—Cisco IOS Release 12.2(25)S3, page 212
- Open Caveats—Cisco IOS Release 12.2(25)S2, page 224
- Resolved Caveats—Cisco IOS Release 12.2(25)S2, page 227
- Resolved Caveats—Cisco IOS Release 12.2(25)S1, page 235
- Open Caveats—Cisco IOS Release 12.2(25)S, page 238
- Resolved Caveats—Cisco IOS Release 12.2(25)S, page 240

Release 12.2(22)S and its rebuilds:

- Resolved Caveats—Cisco IOS Release 12.2(22)S2, page 283
- Resolved Caveats—Cisco IOS Release 12.2(22)S1, page 288
- Open Caveats—Cisco IOS Release 12.2(22)S, page 289
- Resolved Caveats—Cisco IOS Release 12.2(22)S, page 290

Release 12.2(20)S and its rebuilds:

- Resolved Caveats—Cisco IOS Release 12.2(20)S14, page 305
- Resolved Caveats—Cisco IOS Release 12.2(20)S13, page 308
- Resolved Caveats—Cisco IOS Release 12.2(20)S12, page 316
- Resolved Caveats—Cisco IOS Release 12.2(20)S11, page 317
- Resolved Caveats—Cisco IOS Release 12.2(20)S10, page 323
- Resolved Caveats—Cisco IOS Release 12.2(20)S9, page 326
- Resolved Caveats—Cisco IOS Release 12.2(20)S8, page 335
- Resolved Caveats—Cisco IOS Release 12.2(20)S7, page 340
- Resolved Caveats—Cisco IOS Release 12.2(20)S6, page 354
- Resolved Caveats—Cisco IOS Release 12.2(20)S5, page 364
- Resolved Caveats—Cisco IOS Release 12.2(20)S4, page 369
- Resolved Caveats—Cisco IOS Release 12.2(20)S3, page 373
- Resolved Caveats—Cisco IOS Release 12.2(20)S2, page 381
- Resolved Caveats—Cisco IOS Release 12.2(20)S1, page 388
- Open Caveats—Cisco IOS Release 12.2(20)S, page 394
- Resolved Caveats—Cisco IOS Release 12.2(20)S, page 397

Release 12.2(18)S and its rebuilds:

- Resolved Caveats—Cisco IOS Release 12.2(18)S13, page 411
- Resolved Caveats—Cisco IOS Release 12.2(18)S12, page 418
- Resolved Caveats—Cisco IOS Release 12.2(18)S11, page 422
- Resolved Caveats—Cisco IOS Release 12.2(18)S10, page 423
- Resolved Caveats—Cisco IOS Release 12.2(18)S9, page 424
- Resolved Caveats—Cisco IOS Release 12.2(18)S8, page 426
- Resolved Caveats—Cisco IOS Release 12.2(18)S7, page 432
- Resolved Caveats—Cisco IOS Release 12.2(18)S6, page 434
- Resolved Caveats—Cisco IOS Release 12.2(18)S5, page 439
- Resolved Caveats—Cisco IOS Release 12.2(18)S4, page 442
- Resolved Caveats—Cisco IOS Release 12.2(18)S3, page 446
- Resolved Caveats—Cisco IOS Release 12.2(18)S2, page 452
- Resolved Caveats—Cisco IOS Release 12.2(18)S1, page 454
- Open Caveats—Cisco IOS Release 12.2(18)S, page 457
- Resolved Caveats—Cisco IOS Release 12.2(18)S, page 463

Release 12.2(14)S and its rebuilds:

- Resolved Caveats—Cisco IOS Release 12.2(14)S19, page 497
- Resolved Caveats—Cisco IOS Release 12.2(14)S18, page 499
- Resolved Caveats—Cisco IOS Release 12.2(14)S17, page 503
- Resolved Caveats—Cisco IOS Release 12.2(14)S16, page 505
- Resolved Caveats—Cisco IOS Release 12.2(14)S15, page 508
- Resolved Caveats—Cisco IOS Release 12.2(14)S14, page 509
- Resolved Caveats—Cisco IOS Release 12.2(14)S13, page 510
- Resolved Caveats—Cisco IOS Release 12.2(14)S12, page 513
- Resolved Caveats—Cisco IOS Release 12.2(14)S10, page 515
- Resolved Caveats—Cisco IOS Release 12.2(14)S9, page 516
- Resolved Caveats—Cisco IOS Release 12.2(14)S7, page 517
- Resolved Caveats—Cisco IOS Release 12.2(14)S5, page 520
- Resolved Caveats—Cisco IOS Release 12.2(14)S3, page 524
- Resolved Caveats—Cisco IOS Release 12.2(14)S2, page 526
- Resolved Caveats—Cisco IOS Release 12.2(14)S1, page 532

Resolved Caveats—Cisco IOS Release 12.2(30)S1

Cisco IOS Release 12.2(30)S1 is a rebuild release for Cisco IOS Release 12.2(30)S. The caveats in this section are resolved in Cisco IOS Release 12.2(30)S1 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCei61732

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

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

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

Open Caveats—Cisco IOS Release 12.2(30)S

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(30)S. All the caveats listed in this section are open in Cisco IOS Release 12.2(30)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCsb26802

  Symptoms: When a client or trunk laser failure occurs, the output of the **show facility-alarm status** reports that a "Line laser failure detected" but does not indicate which laser has failed.

  Conditions: This symptom is observed on a Cisco ONS15530 and ONS15540 when there are transparent transponders.

  Workaround: There is no workaround.

- CSCsb29080

  Symptoms: A flapping or intermittent laser failure alarm may be reported with a 15540-TSP2 2.5-Gbps transponder module even though both the lasers are in a good state. Such a spurious alarm stops in less than 20 seconds after it has started.

  Conditions This symptom is observed very rarely on a Cisco ONS15540. If the alarm stops in less than 20 seconds after it has started, the alarm is spurious and can be ignored.

  Workaround: There is no workaround.

- CSCsb36475

  Symptoms: An FC or FICON link may not initialize correctly through a 2.5-Gbps transponder module. The interface may remain in the down state while the link LEDs flap continuously.

  Conditions: This symptom is observed rarely on a Cisco ONS15530 that is configured with a 15530-TSP1-xxxx transponder module and a Cisco ONS15540 that is configured with a 15540-TSP1-xxxx or 15540-TSP2-xxxx transponder module. The transponder modules run a functional image with version 1.A3 or an earlier image. The symptom occurs when Speed Negotiation is enabled on the client device and when FLC is enabled on all transponder interfaces on the link.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(30)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(30)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdx38037

  Symptoms: A router may reset unexpectedly with a bus error when the command- line interface (CLI) **test gssapi init_sec_contxt** *server name* command is issued.

  Conditions: This symptom is observed on any platform that supports the CLI **test gssapi init_sec_contxt** *server name* command.

Workaround: Configure the **kerberos local-realm** *kerberos-realm* global configuration command.

- CSCed05135

  Symptoms: A Cisco platform that is configured for Kerberos authentication may crash.

  Conditions: This symptom is observed when you attempt to make an encrypted Kerberized Telnet connection.

  Workaround: There is no workaround.

- CSCee28796

  Symptoms: A Cisco 7304 may crash because of low I/O memory as a result of an IPC storm that is associated with writing the CDP multicast address to an Ethernet MAC filter.

  Conditions: This symptom is observed on Cisco 7304 with an Ethernet, Fast Ethernet, or Gigabit Ethernet port adapter. However, the symptom is platform-independent and may occur on any Cisco platform.

  Workaround: If CDP is not required for network management (SNMP), enter the **no cdp run** command in the startup configuration.

  If CDP is required for network management (SNMP), enter the **no cdp enable** command on each interface and subinterface in the startup configuration, except for the management interfaces and subinterfaces. (There is a maximum of 10 management interfaces and subinterfaces.)

- CSCee71685

  Symptoms: A Cisco router may crash because of low I/O memory as a result of an IPC storm that is associated with writing the CDP multicast address to an Ethernet MAC filter.

  Conditions: This symptom is observed on Cisco 7304 with an Ethernet, Fast Ethernet, or Gigabit Ethernet port adapter. However, the symptom is platform-independent and could occur on any Cisco platform.

  Workaround: If CDP is not required for SNMP network management, enter the **no cdp run** command in the startup configuration.

  If CDP is required for SNMP network management, enter the **no cdp enable** command on each interface and subinterface in the startup configuration, except for the management interfaces and subinterfaces. (There is a maximum of 10 management interfaces and subinterfaces.)

- CSCee91044

  Symptoms: A network operations center (NOC) may receive many false alerts indicating that an IKE tunnel is down. (The IKE tunnel is torn down but immediately rebuilt.)

  Conditions: This symptom is observed when SNMP traps are sent for every IKE timeout or rekey but not for an IPSec timeout or rekey.

  Workaround: There is no workaround.

  Further Problem Description: When the NMS receives an ikeTunnelStop message for the IKE tunnel, the NMS can issue an SNMP get request for the cikeTunnelHistTable in order to receive details about the IKE tunnel. The History Table provides the reason why the IKE tunnel was deleted. The cikeTunHistTermReason object is particularly useful because it provides the following information:

```
The reason the IPSec Phase-1 IKE Tunnel was terminated.
          Possible reasons include:
          1 = other
          2 = normal termination
          3 = operator request
```

```
4 = peer delete request was received
5 = contact with peer was lost
6 = local failure occurred.
7 = operator initiated check point request
```

The NMS can then use this information to identify whether or not the ikeTunnelStop message was sent because of an error.

- CSCuk50643

  Symptoms: A router reloads when the NTP server association is set via SNMP.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(22)S.

  Workaround: Enter the **ntp peer** command.

IP Routing Protocols

- CSCea59206

  Symptoms: When you configure the **distribute-list** router configuration command under the **address-family ipv4 vrf** *vrf name* router configuration command, the **distribute-list** router configuration command may appear under the main routing process as may be displayed in the output of the **show running-config** EXEC command.

  Conditions: This symptom is observed in either a Routing Information Protocol version 2 (RIPv2) or a Border Gateway Protocol (BGP) configuration when you specify the *interface-type* and *interface-number* arguments of the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} [*interface-type interface-number*] router configuration command.

  The symptom does not occur when you do not define the *interface-type* and *interface-number* arguments and only enter the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} router configuration command.

  Workaround: There is no workaround.

- CSCec07636

  Symptoms: When the following Open Shortest Path First (OSPF) MIB tables are queried via snmpwalk, some interfaces may not be displayed:

  - ospfNbrTable
  - ospfIfTable
  - ospfIfMetricTable

  Conditions: This symptom is observed on any Cisco platform that runs OSPF.

  Workaround: There is no workaround.

- CSCec22723

  Symptoms: A router may unexpectedly reload because of a watchdog timeout or bus error in OSPF.

  Conditions: This symptom is observed when iSPF is configured under OSPF.

  Workaround: Remove the iSPF configuration from OSPF by entering the **no ispf** command.

- CSCed68668

  Symptoms: A Cisco router that runs Cisco IOS Release 12.3(5.13)T may reload because of a bus error. The output of the **show version** command may show the following:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xYYYYYYYY
  ```

Conditions: These symptoms occur when **clear ip nat *** is executed on the CLI.

Workaround: Do not perform **clear ip nat ***.

The following link provides general information about bus errors: http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

- CSCee36721

  Symptoms: An OSPF Designated Router (DR) may fail to regenerate the network LSA when you reload the router.

  Conditions: This symptom is observed on a Cisco router that functions as a DR for an OSPF interface when another interface with the same interface address is present in the area but is in a shut down state.

  Workaround: Remove the duplicate interface address and enter the **clear ip ospf process** command.

- CSCee49764

  Symptoms: The **redistribute maximum-prefix** command may not take effect.

  Conditions: This symptom is observed when you enter this command while OSPF is processing an SSO switchover.

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

- CSCef00535

  Symptoms: An OSPF router may reload unexpectedly.

  Conditions: This symptom is observed after a neighbor has performed a switchover.

  Workaround: Disable LLS under the OSPF process on the router by entering the **no capability lls** command or disable OSPF NSF under the OSPF process on the neighbor by entering the **no nsf** command.

- CSCef11304

  Symptoms: When performing a snmpwalk on OSPF-MIB that supports the ospfExtLsdbTable, a router can crash. In other instances alignment errors are observed when you enter the **show alignment** command.

  Conditions: These symptoms are observed on a Cisco platform that runs Open Shortest Path First (OSPF) and supports the ospfExtLsdbTable in OSPF-MIB.

  Workaround: There is no workaround.

- CSCef18838

  Symptoms: Tracebacks that are related to spurious memory accesses may occur and the spurious memory accesses may increase over time. When multicast video streaming is viewed using an IP-TV viewer, this situation causes the browser to hang.

  Conditions: This symptom is observed when NAT and multicast are configured on the same router.

  Workaround: There is no workaround. To return the browser to normal operation, reload the router.

- CSCef19137

  Symptoms: There are duplicate entries in the flow cache after an interface bounces, causing packet loss. The output of the **show ip cache flow** command may show information similar to the following:

```
SrcIf     SrcIPaddress    DstIf    DstIPaddress    Pr SrcP DstP      Pkts
Gi0/0.1   10.2.0.1        Fa2/0    10.3.0.1        06 2C26 00B3      5
```

```
Gi0/0     10.2.0.1       Null    10.3.0.1       06 2C26 00B3<<<<  7
```

Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that runs Cisco IOS Release 12.2(20)S4 when an interface bounces quickly and when the CEF structures are flushed while the ARP cache is not flushed. This situation causes incomplete adjacencies because the CEF process expects a fresh ARP entry to complete its adjacency. The symptom is platform-independent and may also occur on other platforms when the same conditions occur.

Workaround: Clear the ARP cache or enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCef26976

  Symptoms: When VRFS are removed through the **no ip vrf** *vrf-name* command, OSPF VRF router processes may run into nvgen problems and the output of the **show running-config** command may not include a protocol name as in the following example:

  ```
  router
    network 10.10.0.0 0.0.255.255 area 0
    ...
  ```

  A correct output would be:

  ```
  router ospf 1
    network 10.10.0.0 0.0.255.255 area 0
    ...
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S when you remove VRFs that are not assigned to any OSPF VRF processes.

  Workaround: There is no workaround.

- CSCef57022

  Symptoms: OSPF route redistribution in an OSPF VRF process does not function.

  Conditions: This symptom is observed when you associate the OSPF process with a VRF by entering the **router ospf** *process-id* **vrf** *vrf-name* command and configure redistribution under the OSPF VRF process by entering the **redistribute** command.

  Workaround: Do not associate the OSPF process with a VRF; only enter the **router ospf** *process-id* command.

- CSCef65500

  Symptoms: A Cisco router that is configured for OSPF may generate recurring SYS-3-CPUHOG messages and tracebacks that are caused by the OSPF process:

  ```
  %OSPF-5-ADJCHG: Process 100, Nbr 10.52.0.186 on ATM1/0.381 from LOADING to FULL,
  Loading Done
  %SYS-3-CPUHOG: Task ran for 4568 msec (243/31), process = OSPF Router, PC = 60B9DFA8.
  -Traceback= 60B9DFB0 60B7E6E0 60B7EE58
  %OSPF-5-ADJCHG: Process 100, Nbr 10.53.0.66 on ATM1/0.115 from FULL to DOWN, Neighbor
  Down: Dead timer expired
  %OSPF-5-ADJCHG: Process 100, Nbr 10.53.0.66 on ATM1/0.115 from LOADING to FULL,
  Loading Done
  %SYS-3-CPUHOG: Task ran for 4988 msec (569/120), process = OSPF Router, PC = 60B9DFA8.
  -Traceback= 60B9DFB0 60B7E6E0 60B7EE58
  ```

  At another date, the following error messages and tracebacks are generated:

  ```
  %SYS-3-CPUHOG: Task ran for 2224 msec (368/9), process = OSPF Router, PC = 60BA80BC.
  -Traceback= 60BA80C4 60B8876C 60B88EE4
  %OSPF-5-ADJCHG: Process 100, Nbr 10.61.0.26 on ATM2/0.179 from FULL to DOWN, Neighbor
  Down: Dead timer expired
  ```

```
%OSPF-5-ADJCHG: Process 100, Nbr 10.61.0.26 on ATM2/0.179 from INIT to DOWN, Neighbor
Down: Interface down or detached
%OSPF-5-ADJCHG: Process 100, Nbr 10.61.0.26 on ATM2/0.179 from LOADING to FULL,
Loading Done
%SYS-3-CPUHOG: Task ran for 2028 msec (647/283), process = OSPF Router, PC = 60BA80BC.
-Traceback= 60BA80C4 60B8876C 60B88EE4
%SYS-3-CPUHOG: Task ran for 2904 msec (552/153), process = OSPF Router, PC = 60BA80BC.
-Traceback= 60BA80C4 60B8876C 60B88EE4
```

Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-225 and that runs Cisco IOS Release 12.2(15)T5 or 12.2(15)T13. However, the symptom may be platform-independent and could also occur in other releases.

Workaround: There is no workaround.

- CSCef95026

  Symptoms: When interfaces flap, a Cisco router may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed when OSPF accesses a freed LSDB entry.

  Workaround: There is no workaround.

- CSCeg19442

  Symptoms: A router that is configured with the OSPF routing protocol may reload.

  Conditions: This symptom is observed when the OSPF process is simultaneously deconfigured via one session and configured via another session.

  Workaround: There is no workaround. Cisco strongly discourages you to configure a router via two different but simultaneous sessions.

- CSCeg41363

  Symptoms: Traffic is not load-balanced, and only a backdoor path is used to forward traffic.

  Conditions: This symptom is observed on a PE router with a parallel path to a destination when one path is over an OSPF sham-link and the other path is over a backdoor link.

  Workaround: Configure an OSPF metric in such a way that the OSPF sham-link path and the backdoor path do not have the same cost.

- CSCeg52889

  Symptoms: TE tunnels do not come up.

  Conditions: This symptom is observed when a new loopback interface is created with an IP address on an MPLE TE head router that is configured with MPLS TE tunnels and when you reload the router. The symptom occurs because of a change in router ID.

  Workaround: Shut down the newly created loopback interface, save the configuration, and reload the router.

- CSCeg74205

  Symptoms: In a simple network that consists of two routers, SPF calculations occur every minute although no topology changes occur.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS release later than Release 12.3(6b) or Release 12.3(7)T4 and that functions as an ABR router when there are static routes in the network. However, the symptom may also occur in other releases.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3(6b) and Release 12.3(7)T4: SPF calculations do not occur every minute.

- CSCeh04837

  Symptoms: ARP entries may be purged unexpectedly.

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

  Workaround: There is no workaround.

- CSCeh07510

  Symptoms: A traceback occurs on a router when you terminate an OSPF routing process by entering the **no router ospf** command.

  Conditions: This symptom is observed when MPLS TE and more than one OSPF process are configured on the router.

  Workaround: There is no workaround.

- CSCeh09588

  Symptoms: During an NSF switchover on a RP, the convergence may be delayed up to five minutes.

  Conditions: This symptom is observed when a DBD exchange error occurs while the adjacency is brought up.

  Workaround: Enter the **clear ip ospf process** command on the affected router.

- CSCeh14015

  Symptoms: Connected routes cannot be redistributed from one protocol to another.

  Conditions: This symptom is observed on EIGRP routes when you enter the **shutdown** command followed by the **no shutdown** command. The symptom may also affect other routing protocols.

  Workaround: There is no workaround.

- CSCin65241

  Symptoms: IS-IS redistribute commands are not synchronized to the standby RP. The routes that depend on these commands fail after a switchover.

  Conditions: This symptom is observed on a Cisco 7500 series but is platform-independent.

  Workaround: There is no workaround.

- CSCin87277

  Symptoms: CPUHOG messages are generated when you bring up OSPF adjacencies on hundreds of subinterfaces.

  Conditions: This symptom is observed when LSAs are configured to be refreshed every 30 minutes.

  Workaround: There is no workaround.

- CSCin89317

  Symptoms: The following CPUHOG message and tracebacks are generated when you create a NAT pool of the type “match-host” with a mask that is smaller than /12:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (87/11),process
  = Exec.
  ```

Conditions: This symptom is observed when you enter one of the following global configuration commands:

- **ip nat pool** *name start-ip end-ip* **netmask** *netmask* **type** *match-host* and the value of the *netmask* argument is smaller than 12.
- **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* **type** *match-host* and the value of the *prefix-length* argument is smaller than 12.

Workaround: Create a NAT pool with a mask that is larger than /12.

- CSCsa77947

  Symptoms: After you reload a router, the CEF adjacency or hardware route for a peer is unexpectedly removed from the FIB hardware table, causing connectivity problems.

  Conditions: This symptom is observed on a Cisco router that has a statically configured ARP alias for the peer.

  Workaround: There is no workaround.

Miscellaneous

- CSCec63011

  Symptoms: A router may reload because of an NVRAM corruption.

  Conditions: This symptom is observed when NVRAM is accessed simultaneously by two processes, when one the processes has a file open, and when the second process attempts to open a nonexistent file. The error handling for the second process clears the global NVRAM pointer that is used by the first process. This situation is more likely to occur in a configuration with redundant Route Processors (RPs) but may also occur in a configuration with a single RP when two terminal windows are open.

  Workaround: There is no workaround.

- CSCed45942

  Symptoms: A router with a configuration size that is larger than the NVRAM size reloads because of a bus error and stack overflow or stack corruption when you enter the **show config** command simultaneously with the **write terminal** or **show running-config** command.

  Conditions: This symptom is observed when the **service compress-config** command or **boot config** command is enabled.

  Workaround: Do not enter the above-mentioned commands simultaneously, reduce the size of the configuration, or increase the size of the NVRAM.

  Further Problem Description: This problem was introduced in Cisco IOS Release 12.1(8a)E1, so most Cisco IOS 12.1E releases are exposed to this problem. The problem may also occur in Release 12.2S.

- CSCee50294

  Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml.

There are multiple workarounds for this issue:

There are four possible workarounds for this vulnerability:

- Disabling the dhcp service
- Control Plane Policing
- Two versions of Access Control Lists

a. Disabling the DHCP Service

This vulnerability can be mitigated by utilizing the command:

```
no service dhcp
```

However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

a. Control Plane Policing Feature

The Control Plane Policy feature may be used to mitigate this vulnerability, as in the following example:

```
access-list 140 deny   udp host 192.168.13.1 any eq bootps
access-list 140 deny   udp any host 192.168.13.1 eq bootps
access-list 140 deny   udp any host 255.255.255.255 eq bootps
access-list 140 permit udp any any eq bootps
class-map match-all bootps-class
  match access-group 140
policy-map control-plane-policy
  class bootps-class
    police 8000 1500 1500 conform-action drop exceed-action drop
control-plane
 service-policy input control-plane-policy
```

For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afad4.html.

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

a. Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

```
In this example, any bootp/dhcp packets destined to the router interface addresses
are blocked.
access-list 100 remark permit bootps from the DHCP server
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 remark deny bootps from any to router f1/0
access-list 100 deny   udp any host 10.89.236.147 eq bootps
access-list 100 remark deny bootps from any to router f0/0
```

```
access-list 100 deny   udp any host 192.168.13.2 eq bootps
access-list 100 remark deny bootps from any to router loopback1
access-list 100 deny   udp any host 192.168.61.1 eq bootps
access-list 100 remark permit all other traffic
access-list 100 permit ip any any
```

access-list 100 is applied to f0/0 and f1/0 physical interfaces.

```
interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

An alternate configuration for the interface access-list workaround.

This example would also need to be applied to all physical interfaces, but deny statements for all of the IP addresses configured on the router are not necessary in this approach. In this example, the address 192.168.13.1 represents a legitimate DHCP server.

```
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 permit udp any host 192.168.13.1 eq bootps
access-list 100 permit udp any host 255.255.255.255 eq bootps
access-list 100 deny   udp any any eq bootps

interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

- CSCee59383

  Symptoms: The entitySensorMIB does not function.

  Conditions: This symptom is observed on a Cisco ONS 15530 that runs Cisco IOS Release 12.2S.

  Workaround: There is no workaround.

- CSCee91327

  Symptoms: Loss of synchronization occurs, causing traffic drops.

  Conditions: This symptom is observed on an uplink interface of a 10G ITU trunk line card of a peer platform of a Cisco ONS15530 when a CPU switchover occurs on the Cisco ONS15530. The traffic drops occur on the 10G ITU trunk line card of the peer platform.

  Workaround: There is no workaround.

- CSCef67682

  Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml contain fixes for this issue.

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

- CSCeg02811

  Symptoms: The power-on diagnostics loopback tests of a Cisco ONS 15530 series 8-port FC/GE aggregation card (15530-FCGE-8P) may report a failure.

  Conditions: This symptom is observed very rarely when the Cisco ONS 15530 is booted immediately after a power-cycle.

  Workaround: There is no workaround. Note, however, that no functionality is affected.

- CSCeg84037

  Symptoms: After a CPU switchover, memory use on the new primary CPU increases by 10 MB and memory use peaks may go up to 85 percent.

  Conditions: This symptom is observed on Cisco ONS15530 and ONS15540 that run Cisco IOS Release 12.2S.

  Workaround: There is no workaround.

  Further Problem Description: To clear the conditions, power-cycle the platform or enter the **redundancy reload shelf** command.

- CSCeh14446

  Symptoms: The maintenance mode on a Cisco AS5850 that is configured for RPR+ may not function.

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.3(11)T but is release- and platform-independent.

Workaround: There is no workaround.

- CSCeh73049

  Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

  Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

  This vulnerability is present in all versions of Cisco IOS that support the **tclsh** command.

  Workaround: This advisory with appropriate workarounds is posted at http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml

- CSCin75763

  Symptoms: When you enter the **no shutdown** interface configuration command on an interface of a 10-Gbps GE transponder card, the interface enters the UP state even when no client is connected.

  Conditions: This symptom is observed when you boot a Cisco ONS15540 and insert a 10-Gbps GE transponder card.

  Workaround: Perform an OIR of the card a couple of times.

- CSCin77447

  Symptoms: A Cisco ONS 15540 may reload when an APS group is deleted via a TL1 command.

  Conditions: This symptom is observed on a Cisco ONS 15540 when you are in the command-line interface (CLI) APS configuration mode while the APS group is deleted via a TL1 command.

  Workaround: Use the CLI to delete the APS group.

- CSCin79420

  This caveat consists of two symptoms, two conditions, and two workarounds in the following configuration:

  A Cisco Catalyst 6000 series connects via a Gigabit Ethernet (GE) interface and a Y cable to a Cisco ONS 15540 that connects to another Cisco ONS 15540. This second Cisco ONS 15540 connects via a Y cable to the GE interface of another Cisco Catalyst 6000 series.

  1. Symptom 1: The Cisco Catalyst 6000 series at the receiving end does not receive any light.

     Condition 1: This symptom is observed when the portfail notification is received on the working active interface on one of the Cisco ONS 15540 platforms and when auto-failover is disabled, preventing the hardware from switching. However, APS still turns the working laser off, causing the working interface to enter the standby mode. Note that the symptom may also occur when Cisco ONS 15530 platforms are used.

     Workaround 1: There is no workaround.

  2. Symptom 2: Auto-negotiation between the two Cisco Catalyst 6000 series fails.

     Condition 2: This symptom is observed when auto-failover is disabled and FLC (wave side) is enabled on the Cisco ONS 15540 platforms, causing end-to-end negotiation between the Cisco Catalyst 6000 series to fail. Because the originating Cisco Catalyst 6000 series continues to pulse its light, FLC is triggered and the wave side laser is turned on and off accordingly. Note that the symptom may also occur when Cisco ONS 15530 platforms are used.

Workaround 2: There is no workaround.

- CSCin80680

  Symptoms: A Cisco 15500 ONS series crashes when FPGA reprogramming is in progress for any of its line cards and when you enter the **show upgrade-info functional-image** command through a vty line.

  Conditions: This symptom is observed on a Cisco 15500 series that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S.

  Workaround: There is no workaround.

- CSCin81343

  Symptoms: During a CPU switchover on a Cisco 15540 extended range transponder, a temporary traffic interruption may occur. When the switchover is complete, traffic resumes. This symptom is intermittent and may not affect all transponders in a chassis.

  The traffic interruption may occur for the following types of encapsulation:

  - ETR/CLO
  - 100-Mbps Fast Ethernet/FDDI
  - ESCON/SBCON
  - 1-Gbps FC/FICON
  - 1-Gbps ISC (ISC1, ISC3-Peer-1gig)
  - 2-Gbps FC/FICON
  - 2-Gbps ISC (ISC3-Peer-2Gig)

  Conditions: This symptom is observed on a Cisco ONS 15540 ESP and Cisco ONS 15540 ESPx in which extended range transponders are installed.

  Workaround: There is no workaround.

- CSCin81624

  Symptoms: A Cisco ONS 15500 series crashes because of a TLB modification exception.

  Conditions: This symptom is observed when you attempt to modify non-writable memory.

  Workaround: There is no workaround.

- CSCsa49566

  Symptoms: An error message similar to the following may be logged on a router:

  ```
  %FIB-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface for unknown if with illegal
  if_number: 0
  ```

  This message is followed by a traceback.

  Conditions: This symptom is observed on a Cisco router when a virtual interface or a virtual loopback interface is created.

  Workaround: There is no workaround.

- CSCuk58617

  Symptoms: The physical Performance Monitoring (PM) statistics may not be collected correctly.

  Conditions: This symptom is observed on a Cisco ONS15500 series that is configured when SNMP optical monitoring traps are enabled.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(25)S15

Cisco IOS Release 12.2(25)S15 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S15 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCsk73104

  Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

  Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

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

- CSCsj05519

  Symptoms: SSO Standby NSE-100 crashes with the following error messages:

  ```
  IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP or
   HA_CONFIG_SYNC-3-LBL_POLICY
  ```

  After the crash, it was observed redundancy mode changed to RPR. When manual reset is applied on the standby, redundancy mode is back to SSO.

  Conditions: This symptom is observed on a Cisco 7300 router that is configured with SSO 2xNSE-100 that is running Cisco IOS Release 12.2(25)S10. The issue seems intermittent and can sometimes be triggered by applying a large configuration (approximately 600 vrfs and 1500 sub-interfaces).

  Workaround: There is no workaround.

- CSCsj57574

  Symptoms: A success event message is sent for a malformed XML. In this situation, a failure message should be sent.

  Conditions: This symptom is observed when you send a malformed XML via the **cns-send** command, as in the example below:

  ```
  <?xml version="1.0" encoding="UTF-8" ?>^M^M
  <config-event config-action="write" no-syntax-check="TRUE">^M^M
  <identifier>IDENTIFIER</identifier>^M^M
  <config-data>^M^M
     <config-id>AAA</config-id>^M^M
     <cli>access-list 1 permit any^M^M
     <cli>access-list 2 permit any ^M^M
     <cli>access-list 1 permit any ^M^M
     <cli>access-list 2 permit any ^M^M
     <cli>access-list 1 permit any ^M^M
     <cli>access-list 2 permit any ^M^M
     <cli>access-list 1 permit any ^M^M
     <cli>access-list 2 permit any ^M^M
     <cli>access-list 2 permit any ^M^M
     <cli>access-list 2 permit any ^M^M
  ```

```
    </cli>^M^M
    </cli>^M^M
    </cli>^M^M
    </cli>^M^M
    </cli>^M^M
    </cli>^M^M
    </cli>^M^M
    </cli>^M^M
    </cli>^M^M
    </cli>^M^M
</config-data>^M^M
</config-event>^M^M
```

Workaround: There is no workaround.

- CSCsj80375

  Symptoms: A T3/E3 serial SPA may not come up because the line protocol remains down, and the output of the **show controllers serial** command does not generate any output for the T3/E3 serial SPA.

  Conditions: This symptom is observed on a Cisco 7304 when you apply the configuration for the first time after the router has booted.

  Workaround: Unconfigure and reconfigure the **card type** command for the T3/E3 serial SPA.

Resolved Caveats—Cisco IOS Release 12.2(25)S14

Cisco IOS Release 12.2(25)S14 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S14 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCsb58066

  Symptoms: A Cisco router that has the **ip pim dense-mode proxy-register** command enabled and that functions as a border router between a router that is configured for PIM dense mode and another router that is configured for PIM sparse mode may not register all non-directly connected sources.

  Conditions: This symptom is observed when more than one non-directly connected source sends traffic to the Cisco router.

  Workaround: Enter the **clear ip mroute *** or **clear ip mroute** *group-address* command.

  Alternate Workaround: Enter the **no ip mroute-cache** on the interface that has the **ip pim dense-mode proxy-register** command enabled.

Miscellaneous

- CSCee49035

  Symptoms: An incorrect update-source interface is selected for a multicast tunnel interface in an MVPN configuration.

Conditions: This symptom is observed when the provider edge (PE) router is also an ASBR with eBGP peers or has non-VPNv4 peers with higher IP addresses than the peer that has VPNv4 enabled. MVPN requires that the BGP update source address of a VPNv4 peer is selected as the MTI source address.

Workaround: There is no workaround.

- CSCek73843

  Symptoms: A Cisco 7304 may crash when you enter the **no flowcontrol send** command.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and a carrier card in which a SPA is installed.

  Workaround: There is no workaround.

- CSCir01277

  Symptoms: A Cisco 7304 may reload unexpectedly because of a watchdog reset condition, which can be seen in the output of the **show version** command.

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

  Workaround: There is no workaround.

- CSCsa65826

  Symptoms: The flow control for an on-board RJ45 GE interface of an NPE-G1 may not function properly.

  Conditions: This symptom is observed on a Cisco 7200 series and a Cisco 7301.

  Workaround: There is no workaround.

- CSCse56501

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

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml.

- CSCsg87729

  Symptoms: A Gigabit Ethernet interface on a Cisco 7304 that has an NPE-G100 does not support flow control. When the traffic profile results in micro burst on a segment, the output of the **show interface** command may shows overrun errors.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2S or Release 12.2SB. Note that the symptom does not occur on a Cisco 7304 that has an NSE-100 or NSE-150.

  Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables you to configure flowcontrol in interface configuration mode, thereby allowing pause frames to be sent to the peer. Enable flow control by entering the following commands on the Gigabit Ethernet interface:

```
Router#conf t
Router(config) # interface gig0
Router(config-if) # flowcontrol send
Router(config-if) # end
```

Enable flowcontrol only when autonegotiation is also enabled to allow the NPE-G100 to negotiate with its peers as to whether it can recognize the pause frames.

Note that an additional change is made via caveat CSCsg39245 to increase the default receive ring limit from 64 Kbps to 128 Kbps to help absorb micro bursts.

- CSCsg90929

  Symptoms: When you configure MR-APS between a Cisco 7304 and another router such as a Cisco 7500 series or Cisco 7600 series with PA-MC-STM-1 port adapters, the following tracebacks are logged on the Cisco 7304:

  ```
  -Process= "APS process", ipl= 0, pid= 191
  -Traceback= 406DC2E0 40741174 400C24BC 400C2BF0 400C6D9C 400C79EC 400C8814 400C8894
  400C90B8
  ```

  Conditions: This symptom is observed on a Cisco 7304 when the working or protect PA-MC-STM-1 port adapter in the active state.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs with the following Cisco IOS software images:

  On the Cisco 7304:

  - Release 12.2(27)SBC5 (PGP ver.4)
  - Release 12.2(28)SB5 (PGP ver.4)

  Note that Release 12.2S could also be affected.

  On the Cisco 7600 series:

  - Release 12.2(18)SXD5 (PGP ver.3)
  - Release 12.2(33)SRA1 (PGP ver.4)

- CSCsi01470

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

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

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

- CSCsi16819

  Symptoms: An end-to-end ping between CE routers may fail in an ATMoMPLS environment.

  Conditions: This symptom is observed when a Cisco router that functions as a PE router has ATMoMPLS configured as “ATM single cell relay over MPLS: port mode” via the **xconnect** command under an ATM Main interface.

  Workaround: There is no workaround.

- CSCsi73899

  Symptoms: A Cisco 7301 or Cisco 7304 that is configured to use MPLS service policies on some interfaces may crash. The crash may be preceded by following error messages:

  ```
  %SYS-2-CHUNKBOUNDSIB: Error noticed in the sibling of the chunk pak subblock c, Chunk index : 25, Chunk real max :25
  ```

  and

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 45FE855C data 45FE862C chunkmagic 15A3C78B chunk_freemagic 1000000
  ```

  Conditions: This symptom is observed on a Cisco 7301 and Cisco 7304 that run Cisco IOS Release 12.2(31)SB and is not related to a specific command sequence. However, note that the crash is platform-independent. For example, the crash could also occur on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsj29558

  Symptoms: When you configure the CNS Exec Agent, a traceback and spurious memory accesses may be generated.

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

  Workaround: There is no workaround. However, the functionality of the CNS Exec Agent is not affected.

Resolved Caveats—Cisco IOS Release 12.2(25)S13

Cisco IOS Release 12.2(25)S13 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S13 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsg24971

  Symptoms: A memory leak may occur on a line card, eventually causing IPC to fail.

  Conditions: This symptoms is observed on a Cisco platform that is configured for NetFlow. The symptom affects distributed platforms only.

  Workaround: There is no workaround.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

IP Routing Protocols

- CSCin95836

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

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

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

  NHRP is not enabled by default for Cisco IOS.

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

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Miscellaneous

- CSCeb21064

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

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

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

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

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

- CSCef77013

  Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also result in a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

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

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml.

- CSCeg74562

  Symptoms: A router may take a very long time to establish LDP sessions with its peers and advertise its label bindings. In some cases, the LDP sessions may flap.

  Conditions: This symptom may occur when a Cisco router that uses LDP for label distribution has a large number (greater than 250) of LDP neighbors and several thousand label bindings to advertise.

  Workaround: The time required to establish the neighbor sessions and advertise the label bindings when TDP is used in place of LDP may be substantially less. Using TDP in place of LDP will result in an acceptable convergence behavior.

- CSCeh54615

  Symptoms: LSPs that support AToM circuits may fail to come up.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that includes the fix for DDTS ID CSCeg74562. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74562. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCej01615

  Symptoms: On a router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), the CPU usage may increase considerably for an extended period of time when a large number of label bindings are withdrawn or released at the same time.

  Conditions: This symptom is observed on a Cisco router only when LDP (as opposed to TDP) is used and when a large number (more than 250) of LDP neighbors and a large number of IP prefixes become unreachable at the same time.

  Workaround: There is no workaround.

- CSCek76486

  Symptoms: A spurious memory access may occur when you load Cisco IOS Release 12.2(25)S.

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

  Workaround: There is no workaround.

- CSCsa92748

  Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

  ```
  Last reset from watchdog reset
  ```

  Conditions: This symptom is observed only on Cisco 7200 and Cisco 7301 series routers that are configured with an NPE-G1 Network Processing Engine.

  Workaround: There is no workaround.

- CSCsb12598

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

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

Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- CSCsb40304

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- CSCsc02825

  Symptoms: In Cisco IOS software that is running the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), the router could reload while trying to access a bad virtual address.

Conditions: This symptom may be observed when LDP is being used. It will not be observed with TDP. It may happen when LDP receives a protocol message larger than 512 bytes right after receiving several Label Mapping messages smaller than 25 bytes. This problem is likely to be accompanied by the presence of one of the following error message:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0xD0D0D0D
```

The above error message may be preceded by one of the following four error messages:

```
%ALIGN-1-FATAL: Corrupted program counter 19:45:07 CET Mon Sep 26 2005 pc=0xD0D0D0D,
ra=0x61164128, sp=0x64879B98
```

```
%TDP-3-BAD_PIE: peer x.x.x.x; unknown pie type 0x11E
```

```
%TDP-3-UNEXPECTED_PIE: peer x.x.x.x unexpected pie type 0x0
```

```
%TDP-3-PTCLREAD: peer x.xx.x0, read failure
```

This problem may be seen in releases that include the fix for CSCeg74562 but do not have the fix associated with this defect.

Workaround: There is no workaround.

- CSCsd34855

  Symptoms: The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

  Conditions: The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  – VTP Version field DoS
  – Integer Wrap in VTP revision
  – Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  – CSCsd52629/CSCsd34759 -- VTP version field DoS
  – CSCse40078/CSCse47765 -- Integer Wrap in VTP revision
  – CSCsd34855/CSCei54611 -- Buffer Overflow in VTP VLAN name

  Cisco's statement and further information are available on the Cisco public website at

  http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml.

- CSCsd81407

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

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

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

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

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

- CSCsd92405

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- CSCsd95616

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

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

- CSCse24889

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t
ip ssh version 1
end
```

Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

```
10.1.1.0/24 is a trusted network that
is permitted access to the router, all
other access is denied
```

```
access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any
```

```
line vty 0 4
access-class 99 in
end
```

Further Problem Description:

For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

https://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cntrl_acc_vtl_ps6922_TSD_Products_Configuration_Guide_Chapter.html

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

http://www.cisco.com/warp/public/707/ssh.shtml

- CSCse56501

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

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml.

- CSCsf17521

  Symptoms: When there is a hierarchical policy with a Class of Service (CoS), traffic shaping that is applied on the parent policy does not function properly for speeds that are slower than 2000 kbps because the throughput is reduced.

  Conditions: This symptom is observed on a Cisco 7304 when there is a priority class configured in a policy that is attached to an interface. The larger the packets, the more the throughput is reduced.

  Workaround: There is no workaround.

- CSCsg10075

  Symptoms: When you enter the **show policy-map interface** command, the platform may hang at the --More-- prompt.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router but may also affect other platforms.

Workaround: There is no workaround.

- CSCsg16908

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the IOS FTP Client feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

- CSCsg40567

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

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

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

- CSCsg56947

  Symptoms: When you perform and OIR of a SPA-2XOC3-POS, the HC counters may stop functioning.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S10 or a later release or Release 12.2(28)SB5.

  Workaround: Do not perform an OIR. Rather, reload the SPA when there is an opportunity.

- CSCsg70474

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

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

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

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

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

- CSCsg77139

  Symptoms: After you have reloaded a router, VRF routes disappear.

  Conditions: This symptom is observed when you reload a router the processes a heavy traffic flow.

Workaround: Enter the **clear ip route vrf** *vrf-name* command.

Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface from which the VRF routes have disappeared.

- CSCsg86121

  Symptoms: A POS SPA is unexpectedly deactivated when the traffic flow stops.

  Conditions: This symptom is observed on a Cisco 7304 after the SPA has received a Path Loss of Pointer (PLOP) alarm.

  Workaround: Perform a soft OIR of the SPA by entering the **hw-module subslot** *slot/subslot* **start** command.

- CSCsi01470

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

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

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

- CSCsi14211

  Symptoms: A CPUHOG condition may occur when an LDP session goes down.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS LDP, that has more than 30 LDP sessions with peers, and that exchanges more than 5000 label bindings for each LDP session. The symptom occurs when the LDP session goes down shortly after it came up.

  Workaround: There is no workaround.

- CSCsi26378

  Symptoms: For FE and GE SPAs, the broadcast counter value in the output of the **show interface** *type slot/port* command may be twice the value as the actual number of broadcast packets that are received by the interface.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 4-port 10/100 Fast Ethernet SPA or 2-port 10/100/1000 Gigabit Ethernet SPA.

  Workaround: There is no workaround.

  Further Problem Description: This symptom is specific to the SPA on the Cisco 7304.

- CSCsi32575

  Symptoms: The SNMP input and output counters may not be incremented or may show a wrong value.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and a POS interface that is configured for Frame Relay encapsulation.

  Workaround: Do not use SNMP for information about the input and output counters. Rather, enter the **show frame-relay pvc** command.

- CSCsi58871

  Symptoms: For a Gigabit Ethernet interface, the ifOutNUcastPkts may decrement rather than increment.

Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB but could also occur in Release 12.2S.

Workaround: There is no workaround.

- CSCsi60004

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

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

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

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

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

- CSCsi78118

  Symptoms: A traceback may be generated at the “iphc_decompress” function.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.13)T1 and that is configured for Internet Protocol Header Compression (IPHC). However, note that the symptom is not release-specific.

  Workaround: There is no workaround.

- CSCsi83866

  Symptoms: A spurious memory access may occur on Cisco 7304 that has a Frame Relay configuration.

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

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsc39357

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

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

Workaround: Increase the window size on both ends to alleviate the symptom to a certain extent. On the Cisco router, enter the **ip tcp window-size** *bytes* command. When you use a Telnet connection, reduce the *screen-length* argument in the **terminal length** *screen-length* command to 20 or 30 lines.

Resolved Caveats—Cisco IOS Release 12.2(25)S12

Cisco IOS Release 12.2(25)S12 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S12 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCdv73776

  Symptoms: A distributed QoS service policy may not function for a Fast Ethernet subinterface that has the **encapsulation dot1q** *vlan-id* command enabled.

  Conditions: This symptom is observed on a Cisco 7500 series when the FE-PA on which the subinterface is configured resides in any other slot than slot 0 and bay 0 of a VIP.

  Workaround: Install the FE-PA in slot 0 and bay 0 of the VIP.

IP Routing Protocols

- CSCei62049

  Symptom: Prioritized packets such as routing protocol packets are not punted to the process level. This situation causes the input queue to become full.

  Conditions: This symptom is observed on a Cisco router that is configured for Selective Packet Discard (SPD).

  Workaround: There is no workaround.

- CSCsg97662

  Symptoms: When you enter the **no ip nat service skinny tcp port 2000** command, NAT is not disabled on port 2000. This situation causes NAT to be applied to SCCP packets, and causes the CPU usage to be very high.

  Conditions: This symptom is observed when an application is running on the port 2000.

  Workaround: There is no workaround.

  Further Problem Description: SCCP and NAT for voice are not supported in Cisco IOS Release 12.2 or a release that is based on Release 12.2. The **no ip nat service skinny tcp port 2000** command is not supported in these releases.

Miscellaneous

- CSCek47252

  Symptoms: A Cisco 7304 may reload unexpectedly when you enter the **show diag** *slot-number* command for a Port Adapter Carrier Card (7300-CC-PA).

  Conditions: This symptom is observed rarely on a Cisco 7304 and occurs only when the **show diag** *slot-number* command causes the 7300-CC-PA to reset unexpectedly.

Workaround: To prevent the symptom from occurring, do not enter the **show diag** *slot-number* command or the **show tech-support** command, which includes the **show diag** *slot-number* command.

- CSCsb65901

  Symptoms: A Cisco 7304 may reload unexpectedly while traffic is flowing.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100, that runs Cisco IOS Release 12.2(20)S9, that is configured for MPLS, and that has PXF processing enabled. The symptom occurs in a two-way loadbalancing scenario in which one link is a GRE tunnel interface that uses a static route.

  Workaround: Do not configure a static route that sends traffic to the tunnel destination through the tunnel interface itself.

- CSCsc72722

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

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

  Workaround: There is no workaround.

- CSCse01124

  Symptoms: The Hot Standby Router Protocol (HSRP) may not come up and may remain in the "Init" state, which can be verified in the output of the **show standby brief** command.

  Conditions: This symptom is observed when dampening is configured on a native Gigabit Ethernet interface of a Cisco 7200 series or on a Fast Ethernet interface of a PA-FE-TX port adapter. Other types of interfaces are not affected.

  Workaround: When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the Gigabit Ethernet and Fast Ethernet interfaces of all routers of the standby group.

  To prevent the symptom from occurring, remove dampening from the Gigabit Ethernet and Fast Ethernet interfaces.

- CSCsg31202

  Symptoms: A Cisco 7304 with an NSE-100 may crash and generate the following error message:

  ```
  Unexpected exception, CPU signal 10, PC = 0x4008B2EC
  ```

  Conditions: This symptom is observed very rarely when the router is configured with an input policy that marks incoming IP traffic on one interface and then uses this information for classification on an output policy on another interface.

  Workaround: There is no workaround.

- CSCsg92830

  Symptoms: There is no connectivity for certain routes that are configured in BGP VRF instances on a PE router.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S or one of its rebuilds and that functions as a PE router in an MPLS VPN network with multiple redundant BGP Route Reflectors. The symptom occurs usually when there is a route flap on a CE router. However, the symptom occurs only under certain specific timing conditions, and not every time when there is a route flap.

Workaround: When the symptom has occurred, enter the **clear ip route vrf** *vrf-name network* command. To prevent the symptom from occurring, remove the redundant BGP Route Reflectors from the network.

- CSCsh02610

  Symptoms: A VIP that is installed in a Cisco 7500 series may reload unexpectedly, causing a temporary data traffic outage.

  Conditions: This symptom is observed when the router is configured for MPLS.

  Workaround: There is no workaround.

- CSCsh52963

  Symptoms: The standby RP in a High Availability (HA) configuration may enter the ROMmon mode instead of the RPR mode.

  Conditions: This symptom is observed on a Cisco router for certain combinations of mismatched Cisco IOS software images in which the active RP runs an older Cisco IOS software image and the standby RP runs a newer Cisco IOS software image.

  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.

- CSCse05736

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

  Conditions: This symptom is seen under the following conditions:

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

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

Resolved Caveats—Cisco IOS Release 12.2(25)S11

Cisco IOS Release 12.2(25)S11 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S11 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCee83917

  Symptoms: The RP of a Cisco router may crash when entering the **write memory** legacy command.

  Conditions: This symptom is observed on a Cisco router that has the **snmp mib community-map** command enabled with a very long community string and an engineID. The symptom may also occur when the long community string is removed from the configuration. The symptom does not occur when entering the **copy running-config startup-config** EXEC command.

  Workaround: A community string that is shorter than 40 characters will not cause the symptom to occur.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml.

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.

- CSCsc36517

  Symptoms: A router reloads unexpectedly when a continue statement is used in an outbound route map.

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

  Workaround: There is no workaround.

ISO CLNS

- CSCef96650

  Symptoms: A network may not be advertised via a passive interface.

  Conditions: This symptom is observed when you first shut down an interface that is configured for IS-IS routing without disabling IS-IS, then configure a passive interface for IS-IS, and then enter the **no shutdown** command on the passive interface.

  Workaround: First disable IS-IS on the interface before you configure the passive interface.

- CSCsa90719

  Symptoms: A router running Cisco IOS software will reload unexpectedly, when the **no passive-interface** command is issued under the **router isis** configuration.

  Conditions: This symptom has been observed when the interface is configured to run ISIS and later changed to passive interface.

  Workaround: Disable ISIS on the interface before changing it to passive, using the **no ip router isis** interface command.

- CSCsb34032

  Symptoms: A router may reload unexpectedly when you remove the IS-IS configuration at the interface or router level.

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

  – The router is HA-capable.

  – The **isis protocol shutdown** interface configuration command is enabled on the interface.

  – You enter an interface configuration command that enables IS-IS such as an **isis** command, a **clns** command, or the **ipv6 router isis** command before you enter a router configuration command such as the **net** command.

  When you remove the IS-IS configuration at the interface or router level, the router may reload.

  Workaround: Remove the **isis protocol shutdown** interface configuration command before you remove IS-IS from the interface or router level.

Miscellaneous

- CSCek24008

  Symptoms: Toggling an output service policy on an interface that processes a high rate of egress traffic may cause the PXF engine to crash.

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

  Workaround: There is no workaround.

- CSCin99753

  Symptoms: When you enter the **test pppoe** command on the PPPoE client, the PPPoE client or PPPoE server crashes.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that functions as a PPPoE client or PPPoE server. When the Cisco 7304 functions as a server and you enter the **test pppoe** command on another Cisco 7304 that functions as a PPPoE client, the PPPoE server crashes. When another router functions as the PPPoE server and a Cisco 7304 functions as the PPPoE client, the PPPoE client crashes.

Workaround: There is no workaround.

- CSCir00106

  Symptoms: IPC timeout messages may be generated on a Cisco 7304 that has an NSE-100.

  Conditions: This symptom is observed when the CPU usage of the router is at 100 percent, when the PXF engine is switched off, and when there is a heavy traffic that is punted to the RP.

  Workaround: Enable PXF switching by entering the **ip pxf** command.

- 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.

- CSCsd80937

  Symptoms: A Cisco 7304 crashes when you enter the **show diag** command for the slot in which a de-activated PA-CC is installed. Later, when you enter the **hw-module slot** *slot-number* **start** command, the command is not accepted for the slot in which the de-activated PA-CC is installed.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB after you have selected the “No upgrade no” option from the ROMmon Upgrade menu, causing the PA-CC to become de-activated. The symptom may also occur in Release 12.2S.

  Workaround: There is no workaround.

- CSCse39760

  Symptoms: A PA-CC does not recover when you perform a soft or hard OIR of the standby RP.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with dual RPs after a switchover has occurred that causes the standby RP to become the active RP. In this situation, when you perform a soft or hard OIR of the standby RP, the PA-CC does not recover because the PA-CC fails to initialize.

  Workaround: There is no workaround.

- CSCse68138

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

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

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

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

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

- CSCse73032

  Symptoms: Multicast routes fail, CEF routes fail, NAT translations fail, MPLS routes over an EtherChannel fail, or the router reloads unexpectedly.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100 processor that runs Cisco IOS 12.2(25)S or a rebuild of this release up to and including Release 12.2(25)S10. The symptoms occurs under stress conditions when NAT and multicast are used (but not necessarily for the same traffic flows).

  In Release 12.2(28)SB or one of its rebuilds, the symptoms may occur when a Cisco 7304 that has an NSE-100 processor functions under stress conditions and when the following combinations of features are in use (but not necessarily for the same traffic flows):

  - NAT and multicast
  - MPLS over EtherChannel and large CEF tables
  - Multicast and large CEF tables

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

- CSCse78349

  Symptoms: A Cisco 7304 that is configured for multicast may drop packets from its PXF engine.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NSE-100 and occurs when the router is at the transition of the sparse-mode and dense-mode regions and when the following events take place:

  1. A stream from the dense-mode side halts, causing the (s,g) entry to time out.
  2. The stream restarts before the corresponding (*,g) entry times out.

  This situation causes the packets to be dropped from the PXF engine and occurs because the output list interface for the (*,g) entry points toward the source in the dense-mode region.

  Workaround: Enter the **no ip mroute-cache** command on the input interface in dense mode.

- CSCse98421

  Symptoms: When a Cisco 7304 that functions in an MPLS environment as a P router receives MPLS traffic that is forwarded as pure IP traffic, the router may incorrectly apply an MPLS string rather than an IP string, causing the next PE router to drop packets that have a size larger than 1496 bytes.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that runs Cisco IOS Release 12.2(28)SB1 or Release 12.2(28)SB2, that has PXF enabled, and that has MPLS configured on the connecting interfaces.

  Workaround: Disable PXF, downgrade to Cisco IOS Release 12.2(25)S8, or disable MPLS. However, if none of these solutions is an option, there is no workaround.

  Further Problem Description: The same symptom is observed irrespective of the FPGA microcode that is used. The connecting interfaces have the **mtu 1512** and **ip mtu 1500** commands enabled so the MPLS MTU is the same as the interface MTU and the IP MTU is a bit less than the interface MTU to accommodate for two labels.

- CSCsf03959

  Symptoms: A Cisco 7304 may punt GRE traffic to the RP instead of switching it in the PXF engine.

Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(25)S or one of its rebuilds when the tunnel interface is configured for VPN forwarding with **ip vrf forwarding** command.

Workaround: There is no workaround.

Further Problem Description: You can observe the failure in the output of the **show ip pxf interface** command, as in the following example:

```
c7300#show pxf interface tunnel 1
PXF-If: Y 00018  Tu1          (Up, Punting to RP - unsupported feature)
  Features: in=CEF +Unsupp [0x401],  out=GRE  [0x800]  qstatus=XON
  Unsupported Input Features:
VPN_FORWARDING
  Ingress Packets:              0   Input Drop Packets :              0
     MPLS Packets:              0
     IPv6 Packets:              0
    MCAST Packets:              0
  Egress Packets :              0   Output Drop Packets:              0
    MCAST Packets:              0
```

- CSCsf04754

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

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

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

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

- CSCsg27043

  Symptoms: On a 7304 series Network Services Engine (NSE), the passing of packets from the PXF engine to the RP may freeze for a period from seconds to minutes. This situation causes the router to lose its routing protocol neighbors.

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

  Temporary Workaround: If the symptom occurs repeatedly, reloading the router may help.

TCP/IP Host-Mode Services

- CSCsb51019

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

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

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

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

Resolved Caveats—Cisco IOS Release 12.2(25)S10

Cisco IOS Release 12.2(25)S10 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S10 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCef18838

  Symptoms: Tracebacks that are related to spurious memory accesses may occur and the spurious memory accesses may increase over time. When multicast video streaming is viewed using an IP-TV viewer, this situation causes the browser to hang.

  Conditions: This symptom is observed when NAT and multicast are configured on the same router.

  Workaround: There is no workaround. To return the browser to normal operation, reload the router.

- CSCeg41363

  Symptoms: Traffic is not load-balanced, and only a backdoor path is used to forward traffic.

  Conditions: This symptom is observed on a PE router with a parallel path to a destination when one path is over an OSPF sham-link and the other path is over a backdoor link.

  Workaround: Configure an OSPF metric in such a way that the OSPF sham-link path and the backdoor path do not have the same cost.

- CSCei27084

  Symptoms: Configured NAT pools are not shown in the startup configuration and are not visible through CLI commands.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 when you configure NAT pools after you have first configured a discontiguous NAT pool. The symptom may also occur in other releases.

  Workaround: If you need only a single discontiguous NAT pool, configure it after you have configured other NAT pools.

Miscellaneous

- CSCee87572

  Symptoms: After creating E1 circuits such as 3/7/1 and 3/7/2, counters under 3/7/1 and 3/7/2 may hang the next day.

  Conditions: This symptom is observed on a PA-MC-STM-1SMI that is installed in a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCeh18855

  Symptoms: A router may crash when you attempt to unconfigure a service policy.

Conditions: This symptom is observed on a Cisco router that is configured for Network Based Application Recognition (NBAR).

Workaround: There is no workaround.

- CSCeh87998

  Symptoms: A Cisco 7304 that functions in a HA configuration may lose its running configuration after two switchovers have occurred.

  Conditions: This symptom is observed when 4000 virtual circuit are configured on the router.

  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.

- 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.

- 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.

- 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.

- CSCsd76528

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

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

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

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

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

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

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

- CSCsd87217

  Symptoms: For both DSCP-based and precedence-based WRED statistics counters, the output of the **show policy-map interface** command may show zero, or data for the wrong class.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  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.

- 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.

- CSCse37573

  Symptoms: The NPE-G100 in a Cisco 7304 crashes after the PA-CC has crashed.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S10 and that is configured with a PA-CC in which an 8-port ATM IMA port adapter is installed.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(25)S9

Cisco IOS Release 12.2(25)S9 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S9 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCef60452

  Symptoms: A router may stop receiving multicast traffic.

  Conditions: This symptom is observed rarely during convergence when a router receives a Join message on an RPF interface and when a downstream router converges faster than the first router that receives the Join message.

  In this situation, the router does not populate the RPF interface into the OIL (that is, the OIL remains null) because the old SP-tree has already been pruned by the downstream router. When the RPF interface of the router changes to the new path later, it does not trigger a Join message toward the multicast source until the router receives a next periodic Join message from the downstream router and populates the OIL. As a result, multicast traffic stops temporarily but no longer than the periodic Join message interval.

  Workaround: There is no workaround.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. 1. Attacks that use ICMP “hard” error messages
  2. 2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. 3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Miscellaneous

- CSCed48156

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

  Conditions: 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.

- 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.

- CSCeh93738

  Symptoms: Packets for remote 6PE destinations may be dropped. When you enter the **show ipv6 cef** *ipv6-prefix* **detail** command for a VIP, the next hop shows incorrectly for all remote 6PE prefixes. Note that the same command shows proper information when you enter it for the RP.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(25)S, that functions as a 6PE router, and that has the **ipv6 cef distributed** command enabled.

  Workaround: Do not use distributed CEF; disable the **ipv6 cef distributed** command and enable the **ipv6 cef** command.

- CSCej62850

  Symptoms: When you remove the first link member of an IMA group from a PA-A3-8T1IMA port adapter, the link remains down.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 7300-CC-PA in which a PA-A3-8T1IMA port adapter is installed.

  Workaround: There is no workaround.

- CSCin31767

  Symptoms: A Cisco router may reload when you enter the **show atm map** privileged EXEC command.

  Conditions: This symptom is observed on all Cisco routers after you have first deleted a subinterface on which a static map bundle was configured.

  Workaround: First remove the static map bundle; then, delete the subinterface.

- CSCin67253

  Symptoms: A Cisco 7500 series may stop forwarding traffic via an Any Transport over Multiprotocol Label Switching (AToM) virtual circuit (VC) that is configured on an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+).

Conditions: This symptom is observed on a Cisco 7500 series that has a PA-MC-8TE1+ that is configured for Frame Relay over Multiprotocol Label Switching (FRoMPLS) or Frame Relay/ATM/Ethernet interworking when you perform an online insertion and removal (OIR) of the Versatile Interface Processor (VIP) in which the PA-MC-8TE1+ is installed.

Workaround: Remove and reconfigure the affected AToM VC.

- 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.

- CSCsc60281

  Symptoms: A 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) that is installed in a 7304-CC-PA cannot be configured for Frame Relay over MPLS (FRoMPLS).

  Conditions: This symptom is observed on a Cisco 7304 when you enter the **xconnect** command to configure the PA-POS-2OC3 for FRoMPLS.

  Workaround: There is no workaround.

- CSCsc86262

  Symptoms: When you configure OAM on an ATM subinterface in an AToM configuration, the ATM subinterface goes down.

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

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

- 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.

- 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.

- 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 card.

- 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.

- CSCsd46274

  Symptoms: A Cisco 7304 may hangs when the Cisco IOS software image is loaded during cleaning.

  Conditions: This symptom is observed on Cisco 7304 that has an NSE-100 but rarely on a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

  Further Problem Description: Cleaning comprises of the following steps:

  1. Erase all configurations from the router.
  2. Load the boot image, load the minimum configuration, and save the configurations.
  3. Reload the router with the proper image, and load the proper configurations.

- CSCsd49081

  Symptoms: A Cisco 7304 may hang when an HA switchover occurs.

  Conditions: This symptom is observed when you have entered the **hw-module stop** command followed by the **hw-module start** command for a port adapter before the HA switchover occurs.

  Workaround: Do not enter **hw-module stop** command followed by the **hw-module start** command for a port adapter.

  Further Problem Description: The symptom occurs only for port adapters, not for SPAs and native line cards.

Resolved Caveats—Cisco IOS Release 12.2(25)S8

Cisco IOS Release 12.2(25)S8 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S8 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCef97738

  Symptoms: BGP may pass an incorrect loopback address to a multicast distribution tree (MDT) component for use as the source of an MDT tunnel.

  Conditions: This symptom is observed when you reload a Cisco router that runs Cisco IOS Release 12.0(28)S1 and when there is more than one source address that is used in BGP, such as Lo0 for IPv4 and Lo10 for VPN. If the IPv4 peer is the last entry in the configuration, the MDT tunnel interface uses lo0 as the source address instead of lo10. The symptom may also occur in other releases.

  Workaround: Remove and add the MDT statement in the VRF.

- CSCeh53906

  Symptoms: A stale non-bestpath multipath remains in the RIB after the path information changes, and BGP does not consider the stale path part of the multipath.

Conditions: This symptom is observed on a Cisco router that has the **soft-reconfiguration inbound** command enabled and occurs only when the BGP Multipath Loadsharing feature is enabled for three or more paths, that is, the *number-of-paths* argument of the **maximum-paths** *number-of-paths* command has a value of three or more.

Workaround: Disable the **soft-reconfiguration inbound** command for the neighbor sessions for which the BGP Multipath Loadsharing feature is enabled or reduce the maximum number of paths for the BGP Multipath Loadsharing feature to two.

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.

- CSCee58460

  Symptoms: When ISDN MLP calls are terminating, a spurious memory access may be generated in the “servicepolicy_copy_fields()” function.

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

  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.

  Conditions: This symptom is observed when packets are directed to the router and arrive on an Ethernet line card that is configured for dot1q.

  Workaround: There is no workaround.

- CSCej22648

  Symptoms: Connectivity between two CE routers that are configured for EoMPLS fails even though the VCs remain up.

  Conditions: This symptom is observed when EoMPLS is configured in port mode.

  Workaround: Configure EoMPLS in VLAN mode, in which a point-to-point VC is established between PE routers that transport Ethernet traffic from a source 802.1Q VLAN to a destination 802.1Q VLAN over a core MPLS network.

- 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.

  Workaround: There is no workaround.

- CSCej45747

  Symptoms: On an interface or bundle that is configured with a policy map that is defined with the **bandwidth** *percentage* or **priority** *percentage* command, when the bandwidth on the interface or bundle changes, the bandwidth percentages appear as fixed bandwidths in the output of the **show** *interface* command.

  When the bandwidth on the interface or bundle decreases, the policy map is unexpectedly removed or suspended, and an error message such as the following is generated:

  ```
  BWFQ: Not enough available bandwidth for all classes Available 4096 (kbps) Needed 5777
  (kbps)
  ```

  This situation occurs even though there is sufficient bandwidth to satisfy the fixed and percentage bandwidth requirements.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(25)S.

  Temporary Workaround: Re-attach the policy. However, the symptom may occur again.

- 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.

  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.

- 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.

Resolved Caveats—Cisco IOS Release 12.2(25)S7

Cisco IOS Release 12.2(25)S7 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S7 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCeg49796

  Symptoms: Commands on a router may be unexpectedly removed from the running configuration.

  Conditions: This symptom is observed on a router that is assigned as a neighbor to a BGP peer group. For example, when the **shutdown** command was previously configured on the router, the command is removed from the running configuration after the router is assigned as a neighbor to a BGP peer group.

  Workaround: Re-enter the commands on the router.

Miscellaneous

- CSCsa72510

  Symptoms: When you reset a module or line card, an error message and traceback that includes a reference to "%COMMON_FIB-SP-4-CHAIN_REMOVE_INCONS3" may be generated. Typically, there are no further adverse effects and the router continues to behave normally, however, in extremely rare situations, the router may crash immediately after the error occurs.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S and that is configured for IP loadbalancing when a change occurs that causes a recalculation of the loadbalancing, for example, when an interface is shut down, a route flaps, a line card resets, and so on.

  Workaround: Reconfigure the router or network to prevent equal-cost loadbalancing on routes. If this is not an option, there is no workaround.

- CSCsb10550

  Symptoms: A router reloads unexpectedly when you enter the **show access-lists compiled** command, and an error message similar to the following is generated:

  ```
  Unexpected exception, CPU signal 10, PC = 0x4035B878
  ```

  Conditions: This symptom is observed rarely on a router that is configured for Turbo ACL when you enter the **show access-lists compiled** command while a Turbo ACL compilation is in progress. Note that the symptom does not occur when you enter the **show access-lists** command, that is, without the **compiled** keyword. The symptom is more likely to occur when a "--More--" prompt is displayed in the output of the command and when you do not resume the output quickly.

  Workaround: There is no workaround.

- CSCsc29799

  Symptoms: A Cisco 7304 may reload unexpectedly.

  Conditions: This symptom is rarely observed on a Cisco 7304 that has an NSE-100 and is not associated with any specific configuration or traffic type.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(25)S6

Cisco IOS Release 12.2(25)S6 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S6 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeg64124

  Symptoms: The operation result of an IP SLA jitter probe shows a high packet MIA that is equal to the jitter's number of packets minus one. In the responder router, the responder debug message shows many error packets.

  Conditions: This symptom is observed when multiple jitter probes (either from the same router or from different routers) are configured to send packets to the same destination IP address and the same destination port number and when the responder is turned off for a short time and turned on again.

  Workaround: To prevent the symptom from occurring, configure the jitter probe to use a unique destination port number.

  Alternate Workaround: If the symptom has occurred, turn off the responder by entering the **no rtr responder** global configuration command, wait until all jitter probes report "No connection," and then turn on the responder by entering the **rtr responder** global configuration command.

- 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.

- CSCsa42366

  Symptoms: A router may crash because of a memory leak in the SAA/RTR process.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(10a) and that is configured for SAA/RTR. The symptom may also occur in other releases.

  Workaround: Do not perform a getmany command on the rttMonLatestRttOperEntry, rttMonCtrlAdminEntry, and rttMonEchoAdminEntry variable. Do not perform a getone command on the rttMonLatestRttOperAddress variable.

- CSCsa78886

  Symptoms: A memory leak may occur in the vtemplate manager process.

  Conditions: This symptom is observed on a Cisco router that is configured for SNMP when PPPOE sessions are created and deleted for subinterfaces.

  Workaround: Enter the **no virtual-template snmp** command.

- CSCuk51587

  Symptoms: The following error message is generated when you insert a VIP into a previously empty slot of a Cisco 7500 series.

  ```
  %COMMON_FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF interface for unknown if
  with illegal index: 0
  ```

Conditions: This symptom is observed on a Cisco 7500 series that is configured for CEF.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCeh10624

  Symptoms: A Cisco 7206VXR may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(10a) and that is configured with an NPE-G1 and a couple of PA-MC-8TE1+ port adapters. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCin86455

  Symptoms: Auto-provisioning may be disabled on a Cisco router that is configured with a PA-A3 port adapter.

  Conditions: This symptom is observed when a VC class that is configured for create on-demand is attached to the main ATM interface and then the create on-demand configuration is removed and re-applied to the VC class.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface of the PA-A3 port adapter.

- CSCin88976

  Symptoms: AToM Xconnect does not function.

  Conditions: This symptom is observed when L2 switching is configured.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCef57803

  Symptoms: In a VPNv4 network in which a multi-homed CE router advertises multiple paths for a prefix, a PE router may fail to withdraw the prefix previously advertised to another PE router when its best path changes from a non-imported path to an imported path because of a change in the import route map of the VRF.

  Conditions: This symptom is observed in a topology in which a CE router connects to a PE router via two different VRFs.

  Workaround: Remove the imported path either by unconfiguring the import route map of the VRF or by changing the import route target, withdraw the non-imported prefix from the CE router, and restore the import route map or import route target.

- 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.

- CSCsb78194

  Symptoms: When you enter the **clear ip route vrf RED *** command, a route is installed and then immediately deleted from the VRF RIB.

  Conditions: This symptom is observed on a Cisco router when you attempt to force a BGP route to be re-installed into a VRF RIB by entering the **clear ip route vrf RED *** command. Note that the symptom occurs only in Cisco IOS Release 12.2(25)S3, 12.2(25)S4, and 12.2(25)S5 and does not occur in other 12.2S releases.

  Workaround: Remove and reconfigure the VRF.

- 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.

- CSCuk54787

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for redistributed route maps.

ISO CLNS

- 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

- CSCed60987

  Symptoms: On a Cisco 7500 series with distributed CEF, connectivity between CE routers that are locally connected to the same interface may be broken.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or a later release when an output service policy is configured on the subinterface of one CE router but not on the subinterface of the other CE router. Traffic that is process-switched flows correctly between the CE routers.

  Workaround: Configure a dummy output service policy on the subinterface that does not have an output service policy.

- CSCee96698

  Symptoms: When you reload a Cisco 7200 series via a warm reload procedure, the NPE-G1 crashes, enters the ROMmon state, and generates the following error messages:

  ```
  System received a Bus Error exception
  Emulating mis-aligned load at 0x00005375
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2S.

  Workaround: Do not configure or attempt a warm reload procedure.

- CSCef39223

  Symptoms: A secondary RSP may fail to become active.

  Conditions: This symptom is observed on a Cisco 7500 series that functions in an SSO configuration when you perform an OIR of the primary RSP.

  Workaround: Do not perform an OIR of the primary RSP.

- CSCef56327

  Symptoms: You may not be able to configure the **clock source line** command during the configuration of the SONET controller on a Cisco router in which a PA-MC-STM1 port adapter is installed.

  When you enter the **clock source line** command during the configuration of the SONET controller, the output of the **show running-config** command indicates that the clock source is set to line. However, the output of the **show controllers sonet** command indicates that the clock is set to internal, and when you enter the **show running-config** command again, the output indicates this time that the clock source is set to internal.

  Conditions: This symptom is observed when the PA-MC-STM1 port adapter is connected back-to-back via dark fiber to another PA-MC-STM1 port adapter.

  Workaround: Enter the **overhead s1byte ignore** command on the SONET controller before you configure the clock source.

- CSCeg03837

  Symptoms: Alignment tracebacks are generated for a standby RP when an ATM subinterface is configured on the active RP.

  Conditions: This symptom is observed on a Cisco router that has two RPs that function in SSO mode.

  Workaround: There is no workaround.

- CSCeg11894

  Symptoms: The “MPLS required” status is applied to a VRF route on a PE router that has the MPLS VPN-Carrier Supporting Carrier feature enabled. This status is not meant to be imposed on VRF links.

  Conditions: This symptom is observed on a Cisco router that functions in an MPLS VPN-Carrier Supporting Carrier Layer 3 VPN environment.

  Workaround: There is no workaround.

- CSCeg43753

  Symptoms: A router that is configured for RIP and BGP may crash with the following error messages:

  ```
  System returned to ROM by bus error at PC 0x0, address 0x0
  The crashinfo reports the following:
  %ALIGN-1-FATAL: Corrupted program counter pc=0x0, ra=0x60BBD828, sp=0x64228388
  %ALIGN-1-FATAL: Corrupted program counter pc=0x0, ra=0x60BBD828, sp=0x64228388
  Unexpected exception, CPU signal 10, PC = 0x0
  -Traceback= 0 60BBD828 60BAC93C 60BAD790 61FE44C0 60BAD834 60B7C138
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN when RIP is partially configured without a network statement and when BGP is redistributed into RIP.

  Workaround: Ensure that RIP is configured correctly.

- CSCeg62979

  Symptoms: A PA carrier card that is installed in a Cisco 7304 that is configured with an NSE-100 may become deactivated and reloads, and the router generates the following error message:

  ```
  %PACC-3-HEARTBEAT_LOSS: PA Carrier Card Loss of heartbeat from linecard in slot
  <slot_number>
  ```

  Conditions: This symptom is observed when the router functions under stress and when a large number of packets are punted to the Route Processor (RP).

  Workaround: Reduce the stress by reducing the number of packets that are punted to the RP or by disabling some features on the router.

  Further Problem Description: When a large number of packets are punted to the RP and/or a high CPU load occurs on the router, heartbeat packets from the PA carrier card to the RP may be lost, causing the PA carrier card to become deactivated and reload.

- CSCeg71662

  Symptoms: A Cisco 7301 may generate duplicate packets.

  Conditions: This symptom is observed on the onboard Gigabit Ethernet interfaces and subinterfaces of the Cisco 7301.

  Workaround: Enter the **standby use-bia** command on the physical interface.

- CSCeh14580

  Symptoms: A router may reload when a fair-queue configuration is removed.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS 12.2(27)SB but could also occur in Release 12.2(25)S.

  Workaround: There is no workaround.

- CSCeh42472

  Symptoms: On a Cisco 7500 series that has redundant RSPs and that is configured for RPR, RPR+, or SSO, the standby RSP may fail to boot and may generate the following error message:

  ```
  Error : Uncompression of the image failed. Compressed image needs larger DRAM space
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2S or Release 12.4 when any of the following conditions occur:

  - The standby RSP has 128 MB of memory and the difference between the uncompressed Cisco IOS software image size and compressed Cisco IOS software image size is larger than 32 MB.
  - The standby RSP has 256 MB, 512 MB, or 1 GB of memory and the difference between the uncompressed Cisco IOS software image size and Cisco IOS compressed software image size is larger than 68 MB.
  - The standby RSP has memory of another size than what is mentioned above and the difference between the uncompressed Cisco IOS software image size and compressed Cisco IOS software image size is larger than 24 MB.
  - The standby RSP memory is smaller than 128 MB.

  Workaround: Upgrade the memory of the standby RSP so that the above-mentioned memory constraints are not applicable.

- CSCeh57063

  Symptoms: A customized UDP probe does not start properly after a router has rebooted, causing the UDP probe to remain in a TESTING phase. This situation has no affect for the availability of the real server, but the probe does not function, which is shown in the output of the **show ip slb probe** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S3.

  Workaround: To get the probe working again, remove and re-enter the response part of the custom UDP probe configuration.

- CSCeh73049

  Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

  Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

  This vulnerability is present in all versions of Cisco IOS that support the **tclsh** command.

  Workaround: This advisory with appropriate workarounds is posted at http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml

- CSCei08347

  Symptoms: When you ping a Gigabit Ethernet (GE) interface on an NPE-G1 that has the **ip pim sparse-mode** or **ip pim sparse-dense-mode** command enabled, the ping fails.

  Conditions: This symptom is observed on a Cisco 7200 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the GE interface of the NPE-G1.

Workaround: After you have shut down and brought up the GE interface, enter the **no ip pim sparse-mode** or **no ip pim sparse-dense-mode** command and then reconfigure the command.

- 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.

- CSCin78324

  Symptoms: A Cisco router that is configured with a PA-MC-8TE1 port adapter may hang.

  Conditions: This symptom is observed on a Cisco 7200 VXR router that has a PA-MC-8TE1 port adapter and that is configured for IPSec encryption, either via tunnel protection or via a crypto map. The symptom may also occur on other platforms and in other releases.

  Workaround: Disable IPSec encryption.

- CSCin86002

  Symptoms: The bandwidth of an IMA group interface may be less than the combined bandwidth of its active member links that are up and operational.

  Conditions: This symptom is observed on an IMA group interface of a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter that is installed in a Cisco 7xxx platform when the IMA group interface has more than one member link. The symptom occurs when you enter the shutdown interface configuration command quickly followed by the no shutdown interface configuration command on a member link (that is, the command sequence takes less than two seconds). When the member link comes up, the bandwidth of the IMA group interface is not increased.

  Workaround: There is no workaround.

- CSCin95530

  Symptoms: A Cisco 7304 may reload unexpectedly when you attach or detach a QoS policy to an ATM IMA PVC.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100 when you attach or detach the QoS policy while traffic passes through the router.

  Workaround: There is no workaround.

- CSCin96590

  Symptoms: A VIP crashes at the “free_wred_stats” function during an RPR+ switchover.

  Conditions: This symptom is observed on a Cisco router that is configured with a VIP that has a configuration with about 12 MLP bundles with two T1 members when QoS is applied while traffic is flowing.

  Workaround: There is no workaround.

- CSCsa42521

  Symptoms: The output of the **show policy-map** command and the cbQosPoliceCfgTable MIB table show inconsistent CIR information. The information in the cbQosPoliceCfgTable MIB table is incorrect.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2S but may not be platform-specific.

  Workaround: There is no workaround.

- CSCsa50971

  Symptoms: A Cisco platform may unexpectedly reload while attempting to resequence an access list.

  Conditions: This symptom is observed when you delete a few ACEs and then immediately enter the **ip access-list resequence** *access-list-name starting-sequence-number* **increment** command.

  Workaround: There is no workaround.

- CSCsa97217

  Symptoms: Configuring traffic shaping on subinterfaces of a 1-port Gigabit Ethernet port adapter (PA-GE) has no effect.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(25)S.

  Workaround: There is no workaround.

- 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.

  Workaround: There is no workaround.

- CSCsb16343

  Symptoms: The PXF engine of a Cisco 7304 drops 95 to 99 percent of the traffic with packet queue tail drops.

  Conditions: This symptom is observed on a Cisco 7304 when traffic passes to an interface of a 1-port ATM Enhanced port adapter (PA-A3) on the same router.

  Workaround: There is no workaround.

- CSCsb19937

  Symptoms: A router may crash while processing L2TPv3 traffic.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a policy map with a class-default class that contains a marking (set) action other than the **set qos-group** command is enabled on an interface that is also configured for L2TPv3 via an **xconnect** command.

  Workaround: There is no workaround.

- CSCsb40862

  Symptoms: VRF-Select traffic is not punted to the Route Processor on a Cisco 7304 that is configured with an NSE-100, causing traffic to be dropped because an incorrect VRF number is used for the IP lookup process.

Conditions: This symptom is observed when you configure VRF Select in Cisco IOS Release 12.2(25)S or in one of the rebuilds of this release. VRF Select is not supported in these releases and the PXF engine should therefore punt traffic to the RP, but this does not occur, and VRF-Select traffic is ignored.

Workaround: There is no workaround.

- CSCsb48482

  Symptoms: When an ATM PVC is congested, prioritized packets are delayed.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100. Note that the symptom does not occur on a Cisco 7304 that is configured with an NSE-100.

  Workaround: There is no workaround.

- CSCsb48489

  Symptoms: A Cisco 7304 that processes Frame Relay traffic crashes because of a bus error and generates the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x40, pc=0x40540BC0,
  ra=0x40540ACC, sp=0x4684DE18
  ```

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100 and that runs Cisco IOS Release 12.2(25)S5.

  Workaround: There is no workaround.

- CSCsb50776

  Symptoms: An AToM VC does not come up on a router that is configured for EoMPLS because packets are dropped at a connected P router.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that is connected to another Cisco 7304 that also has an NSE-100 and that functions as a P router.

  Workaround: There is no workaround.

- CSCsb54194

  Symptoms: A router that functions as a 6PE router and that is configured for IPv6 and multipath may crash.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S6.

  Workaround: There is no workaround.

- CSCsb54560

  Symptoms: When a FIB table is deleted, a router may crash and generate an "% ALIGN-1-FATAL: Corrupted program counter" error message.

  Conditions: This symptom is observed on a Cisco router that run Cisco IOS Release 12.2(25)S when any FIB table is deleted, for example, when you enter the **no ipv6 cef** command or when a VRF is removed.

  Workaround: There is no workaround.

- CSCsb58117

  Symptoms: A GE interface that functions in promiscuous mode cannot receive multicast traffic, causing a difficulty with HSRP or with a routing protocol such as OSPF or EIGRP because the GE interface cannot receive multicast hello packets.

  Conditions: This symptom is observed when the GE interface has eight or more subinterfaces and when all subinterfaces are configured for HSRP.

  Workaround: Enable PIM on one of the subinterfaces.

- CSCsb59507

  Symptoms: Packets that are larger then 1473 bytes are not forwarded through a router into the MPLS cloud.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S and that functions as a PE router in an EoMPLS environment.

  Workaround: Decrease the IP MTU on the CPE to 1473 bytes. Note that the symptom does not occur in Release 12.2(20)S.

- 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.

- CSCsb69080

  Symptoms: A Cisco 7304 may generate the following error message:

  ```
  %NSE100-3-VA_ERROR: Vanallen ASIC detected an error condition: TIC invalid DMA length
  ```

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100), that is configured for PXF hardware switching, and that has a GRE tunnel configured when the GRE traffic proceeds over a physical interface that is configured for dot1q VLAN encapsulation.

  Workaround: Do not use PXF hardware switching for GRE traffic. Rather, use software switching such as CEF, fast-switching, or process-switching.

- 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.

- CSCuk58481

  Symptoms: Spurious memory accesses may occur on a router that has uRPF enabled. The log may contain messages similar to the following:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x6062435C reading 0x34
  ```

  The output of the **show alignment** command may show information similar to the following:

  ```
  No alignment data has been recorded.
  Total Spurious Accesses 104, Recorded 2
  Address  Count  Traceback
       34     52  0x6062435C 0x6063E4B8 0x6018913C 0x604AA7C0
                  0x604AFBE8
        F     52  0x60624608 0x6063E4B8 0x6018913C 0x604AA7C0
                  0x604AFBE8
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S.

  Workaround: There is no workaround. However, the symptoms have no significant impact and can be safely ignored.

  Further Problem Description: Spurious memory accesses can generally be ignored. Cisco IOS software automatically recovers from a spurious memory access, although some processing overhead is incurred. If spurious memory accesses occur at a high frequency, the performance of the router is impacted.

Wide-Area Networking

- CSCeh34412

  Symptoms: CEF does not function properly with ATM LANE, and traffic on ATM LANE ports is process-switched instead of switched via CEF.

  Conditions: This symptom is observed when the **ip cef** command is enabled.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(25)S5

Cisco IOS Release 12.2(25)S5 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S5 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCds33629

  Symptoms: Closing an existing Telnet session may cause a router to crash.

  Conditions: This symptom is platform-independent

  Workaround: There is no workaround.

- CSCef68103

  Symptoms: A Cisco 7200 series may reload flash disk 1 is accessed.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2S only when the router is configured with both an NPE-G1 and an I/O controller.

  Workaround: Ensure that only flash disk 2 is accessed.

EXEC and Configuration Parser

- CSCec40348

  Symptoms: A Cisco router that functions in high availability (HA) Stateful Switchover (SSO) mode may unexpectedly reload because of a software-forced crash when the Multilink PPP configuration is changed.

  Conditions: This symptom is observed when a multilink interface is deleted.

  Workaround: Do not delete a multilink interface when the router functions in HA SSO mode.

Interfaces and Bridging

- CSCeb64384

  Symptoms: ATM subinterfaces that are created on an 1-port ATM enhanced OC-3c/STM-1 single mode port adapter (PA-A3-OC3SMI) cause the SNMP agent to malfunction, in turn causing an SNMP getmany command to hang in the ifTable.

  Conditions: This symptom is observed on a Cisco router in which a PA-A3-OC3SMI is installed when you enter an SNMP getmany command in the ifTable.

  Workaround: There is no workaround.

- CSCsa46510

  Symptoms: When you enter the **microcode reload** command, an error message similar to the following and a traceback may be generated:

  RSP-3-RESTART: interface Serial3/0/1/4:0, not transmitting -Traceback= 404436B4 4044DE10

  Conditions: This symptom is observed on a Cisco 7500 that is configured with a E1, T1, E3, or T3 port adapter.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeh47172

  Symptoms: Deny statements for an expanded list in the **ip extcommunity-list** command are ignored. Both named and numbered expanded extended community access lists are impacted.

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

  Workaround: Configure a route map, split complex extended community access lists in different simpler extended community access lists, and use permit statements and deny route-map statements.

- CSCsa57101

  Symptoms: A Cisco router may reload when the RSVP MIB object is polled via SNMP.

  Conditions: The symptom is platform- and release-independent.

  Workaround: Disable SNMP by entering the **no snmp-server host** command.

Miscellaneous

- CSCec07579

  Symptoms: Interface bit-rate counters may not be cleared when they should be cleared.

  Conditions: This symptom is observed on a Cisco router that is configured for quality of service (QoS) when you enter the **clear counters** user EXEC or privileged EXEC command. The QoS bit-rate counters are cleared, but the interface bit-rate counters are not.

  Workaround: There is no workaround. Wait for the next update interval for the bit-rate counters.

- CSCee31450

  Symptoms: IPv6 packets may not be switched via CEFv6 but may be blackholed.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S4 when the packets are switched from an FE interface to a POS interface.

  Workaround: There is no workaround.

- CSCef56980

  Symptoms: When unequal CEF loadbalancing is configured between paths, including paths with MPLS labels, incorrect weightings may be used for labeled paths.

  Conditions: This symptom is observed on a Cisco platform that is configured for MPLS and CEF.

  Workaround: There is no workaround.

- CSCeg20374

  Symptoms: If a configuration file that contains a large number (4096) of virtual circuits is downloaded or copied to the running configuration, the standby RP may reload.

  Conditions: This symptom is observed on a Cisco 7304 that functions in HA SSO mode with two NSE-100 RPs or two NPE-G100 RPs and that is configured with an OC-3 ATM or OC-12 ATM line card.

  Workaround: There is no workaround.

  Further Problem Description: To prevent the symptom form occurring again, configure the standby RP to autoboot. Doing so enables the configuration to be synchronized to the standby RP via bulk synchronization.

- CSCeg26728

  Symptoms: BGP may fail to establish a peer with another router when an output service policy is configured on an interface and the output service policy limits the bandwidth to 199 kbps for packets that have the IP precedence value set to 6.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(14)S9.

  Workaround: Remove the output service policy from the interface.

- CSCeg38482

  Symptoms: AutoRP packets are dropped because of an RPF failure.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when both the Candidate RP and Mapping Agent (MA) are configured in a VRF context and when the interface is not specified in the **ip pim vrf** *vrf-name* **send-rp-discovery** *interface-type interface-number* command. This situation may cause the MDT update source address (an address that belongs to the global table) for the MVPN to be chosen and, in turn, the AutoRP flow to be created in the downstream route with a global address as the source.

  Workaround: Configure the interface that has the highest IP address in the VPN as the Candidate RP and MA.

  Alternate Workaround: Configure the interface that is defined in the Candidate RP as the interface in the **ip pim vrf** *vrf-name* **send-rp-discovery** *interface-type interface-number* command.

- CSCeg67788

  Symptoms: The 5-minute output rate in the output of the **show interfaces** command is incorrect for serial interfaces that are configured on a PA-MC-8TE1+ port adapter.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2S or Release 12.3 and that is configured with a PA-MC-8TE1+ port adapter.

  Workaround: There is no workaround.

- CSCeg78681

  Symptoms: Removing and re-applying a valid child policy map to a parent policy map results in an error message, and the configuration is wrongly rejected.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a child policy map has a police action configured and the parent policy map has no police action configured.

  Workaround: Detach the parent service policy from the interfaces before you re-apply the child policy map.

- CSCeg86187

  Symptoms: The **ip mroute-cache distributed** interface configuration command is not retained after you reload a router.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: After the router has reloaded, reconfigure the **ip mroute-cache distributed** interface configuration command on each affected interface.

- CSCeg89677

  Symptoms: A Cisco 7304 router may crash when you enter the **clear counters** command.

  Conditions: This symptom is observed when an ATM line card has fatal hardware errors early during its initialization and may occur when the line card is programmed with an incorrect ATM FPGA image, for example, an ATM FPGA image that is not bundled in a Cisco IOS software image.

  Workaround: Ensure that the ATM line card runs an ATM FPGA image that is bundled in a Cisco IOS software image.

- CSCeh22026

  Symptoms: The standby RP of a Cisco 7304 that functions in a high-availability mode may reload unexpectedly.

  Conditions: This symptom is observed under various circumstances, one of which is the following:

  The Cisco 7304 is configured with a port adapter carrier card in which a PA-MC-2T3+ port adapter is installed and you enter the **no channelized** command for one of the ports of the port adapter.

  Workaround: Do not enter the **no channelized** command for a port of the PA-MC-2T3+ port adapter. Rather, configure the startup configuration to include the **no channelized** command for the port of the PA-MC-2T3+ port adapter.

- CSCeh27709

  Symptoms: The link line rate cannot be achieved, and more than the expected number of packets drop.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a policy-map that contains traffic shaping classes is attached to an egress interface, and when configured average shape rate is larger than link bandwidth.

  Workaround: Do not configure traffic shaping rate over link bandwidth.

- CSCeh32230

  Symptoms: IP TTL is propagated to an MPLS label during label imposition even when propagation is disabled.

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

  Workaround: There is no workaround.

- CSCeh33659

  Symptoms: NAT sessions do not expire after they have been deleted by the PXF engine, which can be observed in the number of active translations in the output of the **show ip nat translations** command.

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

  Workaround: There is no workaround.

- CSCeh34096

  Symptoms: A Cisco 7304 may decrement the time-to-live (TTL) value twice.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2, that is configured with an NSE-100, that functions as a multicast or multicast VPN provider edge (PE) router, and that has Parallel eXpress Forwarding (PXF) enabled.

  Workaround: There is no workaround.

- CSCeh34645

  Symptoms: When you enter the **match qos-group** *qos-group-value* command on a class that is used by an output policy map may cause a Cisco 7304 router to reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7304 router is configured with an NSE-100 forwarding engine and that runs Cisco IOS Releases 12.2(20)S7 or Releases 12.2(25)S3 when the QoS group is set during input processing (through either the **set qos-group** *qos-group-value* command or the **set-qos-transmit** *qos-group-value* police action).

  Workaround: There is no workaround.

- CSCeh39794

  Symptoms: A QoS service policy does not function.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when you remove a child policy map from a hierarchical policy that is attached to an interface.

  Workaround: Detach the service policy from the interface and re-attach it again.

- CSCeh50570

  Symptoms: A Cisco platform reloads when you bring up bulk asynchronous and digital SS7/VPDN calls.

  Conditions: This symptom is observed on a Cisco AS5850.

  Workaround: There is no workaround.

- CSCeh52460

  Symptoms: A standby RP of a Cisco 7304 that is configured for high availability (HA) may crash.

  Conditions: This symptom is observed when a link flap (originating on the remote end) occurs while ATM VCs are being created on a PA-A3 that is installed in a PA-CC. The symptom does not occur during the boot process of the router but only when the router is already up and running.

  Workaround: Prevent link flaps from occurring when you configure ATM VCs on a PA-A3 that is installed in a PA-CC.

  Alternate Workaround: Copy the configuration to the startup configuration and reload the router.

- CSCeh53449

  Symptoms: A router may seem to hang after you enter the **no shutdown** interface configuration command followed by the **shutdown** interface configuration command on an ATM interface that was previously a member of an IMA group. The router does not really hang and is still capable of routing packets but the EXEC process hangs.

  Conditions: This symptom is observed on a Cisco 7304 that has a PA-CC in which a PA-A3-8E1IMA or PA-A3-8T1IMA port adapter is installed.

  Workaround: There is no workaround.

- CSCeh55923

  Symptoms: A router may crash and generate an assertion-failure error message.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when you apply an hierarchical police map on an interface while traffic is being processed.

  Workaround: Stop traffic before you apply the hierarchical police map.

- CSCeh58510

  Symptoms: A Cisco 7304 that is configured for multicast may crash.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 when the router receives a multicast packet with a length of 40 bytes and an IP payload with a length of 8 bytes.

  Workaround: There is no workaround.

- CSCeh62351

  Symptoms: A router or line card may reload when you enter any of the following commands:

  On a Cisco 7304:

  - **show tech-support** command.
  - **show hw-module subslot all status** command.
  - **show hw-module subslot** *slot-number/subslot-number* status command.

  On a Cisco 7600 series or Cisco 12000 series:

  - **show tech-support** command.
  - **show hw-module subslot all status** command.
  - **show hw-module subslot** *subslot-number* **status** command.

  Conditions: This symptom is observed when you enter above-mentioned commands on the console of a Cisco 7304 or on the console of a line card on a Cisco 7600 series or Cisco 12000 series when these routers are configured with any of the following SPAs (some SPAs are specific to the Cisco 7304 and some to the Cisco 12000 series):

  - 2-port Gigabit Ethernet SPA
  - 4-port FE SPA
  - CT3 SPA
  - T1/E1 SPA
  - T3/E3 SPA

  Workaround: There is no workaround.

- CSCeh63952

  Symptoms: L2TPv3 PXF memory may be overwritten.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for L2TPv3 and many routes when an interface flaps.

  Workaround: There is no workaround.

- CSCeh76459

  Symptoms: The output of the **show policy-map interface** *interface* command does not show a configured policy map for an IMA interface, although the output of the **show running-config** command does show the policy map for the same IMA interface.

  When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the IMA interface and you reload the router, the policy map is removed.

  Conditions: These symptoms are observed on a Cisco 7304 that is configured with an IMA port adapter.

  Workaround: Attach the policy map as part of a PVC and reload the router. Note that the symptom does not occur on a Cisco 7200 series that functions in the same configuration.

- CSCei06803

  Symptoms: A Cisco 7304 may crash when you enter the **no ip vrf** *vrf-name* command to delete any VRF that carries multicast routes.

  Conditions: This symptom is observed on a Cisco 7304 series runs Cisco IOS Release 12.2(25)S and that is configured with an NSE-100.

  Workaround: There is no workaround.

- CSCei07223

  Symptoms: Multicast packets may not be forwarded by a PE router that has Parallel Express Forwarding (PXF) enabled.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router in an MVPN environment when the core-facing interface is a serial interface.

  Workaround: There is no workaround.

- CSCin78325

  Symptoms: A serial interface of a PA-MC-8TE1+ continues to process packets even after the interface is placed in the "ADMINDOWN" state. The counters in the output of the **show interfaces serial** command may continue to increment even if the serial interface is shut down.

  Conditions: This symptom is observed on a serial interface of a PA-MC-8TE1+ when there is a channel-group configuration for the interface.

  Workaround: Remove the channel-group configuration for the interface.

- CSCsa59126

  Symptoms: CPU-HOG messages may be generated and a router may crash when a large number of entries is configured on a single access control list (ACL).

  Conditions: This symptom is observed on a Cisco router that has IP ACL enabled.

  Workaround: Reduce the number of entries on the ACL.

- CSCsa60009

  Symptoms: AToM tunnels may fail when loadbalancing occurs on the core side of a PE router.

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

  Workaround: Flap the attachment circuit interface to tear down the AToM tunnel and reinstate the connection.

- CSCsa72313

  Symptoms: The following error messages may be generated on a router that has IP ACL enabled:

  ```
  %SYS-2-INSCHED: suspend within scheduler
  -Process= "<interrupt level>", ipl= 3
  -Traceback= 40525388 40628848 4060AED4 403F15BC 403F34F8 403F37EC 400901C8 4008E730
  406A0EEC 40621120
  ```

  Conditions: This symptom is observed on a Cisco router such as a Cisco 7200 series, Cisco 7304, and Cisco 7500 series when a Turbo ACL compilation is configured along with an ACL on an ingress interface and when traffic passes through the ingress interface. The symptom does not affect the Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsa77012

  Symptoms: Static NAT configurations do not function: packets are forwarded without translation because the first packet of the NAT flow is not punted to the RP to set up the translation info in PXF, and the "NAT Mappable Punt" is absent.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S3 and that is configured with an NSE-100. Note that the symptom does not occur in Release 12.2(25)S2.

  Workaround: If this is an option, disable PXF. If this is not an option, there is no workaround.

- CSCsa82091

  Symptoms: When packets are decapped, IP traffic that is encapsulated using GRE may expose corrupted packets. These packets are dropped.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a GRE tunnel termination point when the packets are encapsulated using GRE tunneling on another Cisco 7304.

  Workaround: There is no workaround.

- CSCsa89518

  Symptoms: A Cisco 7206 series may display incorrect counters in the output of the **show policy-map interface** command.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.2(25)S3 and that is configured with an NPE-G1 when an input service policy is applied to a T3 interface that is configured for Frame Relay encapsulation.

  Workaround: There is no workaround.

- CSCsa90093

  Symptoms: When a primary path is shut down, an ASBR does not forward MPLS packets to the backup path but drops the packets.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that runs Cisco IOS Release 12.2S when the following conditions are present:

  - The router functions as an inter-AS ASBR.
  - The router is configured with Gigabit Ethernet subinterfaces that are configured for dot1q encapsulation and that face a remote router with an AS number.
  - In its own AS, the router has a primary and backup path to a PE router.

  Workaround: If this is an option, disable PXF to re-activate the connectivity by entering the **no ip pxf** command. If disabling PXF is not an option, there is no workaround.

- CSCsa91159

  Symptoms: A Cisco 7304 series carrier card may run out of memory, may reload, and the following error message may be generated:

  ```
  %PACC-3-HEARTBEAT_LOSS: PA Carrier Card Loss of heartbeat from linecard in slot
  <slot_number>
  ```

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 7300-CC-PA port adapter carrier card in which a PA-2POS-OC3 port adapter is installed when a high rate of egress traffic is processed by the interfaces of the port adapter.

  Workaround: Reduce the rate of egress traffic.

- CSCsa95921

  Symptoms: A Cisco 7304 that is configured with an NSE-100 drops TCP packets that have as destination port number 465.

  Conditions: This symptom is observed when the parallel forwarding engine is enabled.

  Workaround: There is no workaround.

- CSCsb11292

  Symptoms: A Cisco 7304 with an NSE-100 may not age out NetFlow entries.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S when NetFlow is configured to export flow records.

  Workaround: If this is an option, disable PXF by entering the **no ip pxf** global configuration command. Doing so may degrade performance of the router. Note that the symptom does not occur in releases earlier than Release 12.2(25)S.

  Further Problem Description: The symptom can be observed by entering the **show pxf netflow info** command several times. The “Flow ager recovery” value increases over time.

Wide-Area Networking

- CSCef71011

  Symptoms: Pings fail when translational bridging and ATM DXI encapsulation are configured.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, Release 12.2S, or a release that is based on Release 12.2S.

  Workaround: Do not configure ATM DXI encapsulation. Rather, configure HDLC, PPP, or Frame Relay encapsulation.

Resolved Caveats—Cisco IOS Release 12.2(25)S4

Cisco IOS Release 12.2(25)S4 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S4 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsa81379

  NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

The removal of NetFlow Feature Acceleration does not affect any other aspects of NetFlow operation, for example Access-list processing. The features are separate and distinct.

Cisco Express Forwarding (CEF) supersedes the deprecated NetFlow Feature Acceleration.

Additionally, the following MIB objects and OIDs have been deprecated and removed from the NetFlow MIB (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

Resolved Caveats—Cisco IOS Release 12.2(25)S3

Cisco IOS Release 12.2(25)S3 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S3 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeg11566

  Symptoms: Intensive SNMP polling may cause the I/O memory of a router to be depleted.

  Conditions: This symptom is observed in rare situations.

  Workaround: Reduce the SNMP polling interval, frequency, or rate.

IP Routing Protocols

- CSCeg30291

  Symptoms: BGP fails to send an update or withdraw message to some peers when these peers have failed to converge properly after an earlier attempt.

  Conditions: This symptom is observed on a Cisco router when you enter the **clear ip bgp** *neighbor-address* **soft out** command while BGP is in the middle of converging. The symptom does not occur when network traffic load is low and BGP has converged.

  Workaround: To clear the error condition, enter the **clear ip bgp** *neighbor-address* **soft out** command again. Alternately, enter the **clear ip bgp** *neighbor-address* command (that is, without the **soft out** keyword).

- CSCeg54375

  Symptoms: Routing inconsistencies may occur in the RIB: routes may be missing from the RIB but may be present in the BGP table.

  Conditions: This symptom is observed on a Cisco RPM-XF when the toaster processor crashes. However, the symptom may occur on any platform that has a toaster processor.

  Workaround: Enter the **clear ip route vrf** *vrf-name* ***** command.

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

ISO CLNS

- CSCed36743

  Symptoms: A memory leak may occur on a router that has the Multi-Topology IS-IS for IPv6 feature enabled and the router may reload.

  Conditions: This symptom is platform-independent and release-independent.

  Workaround: Disable the Multi-Topology IS-IS for IPv6 feature.

- CSCef59924

  Symptoms: A router that is configured for Multi-Topology IS-IS may crash.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(25)S. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCeh00680

  Symptoms: A router that is configured for Multi-Topology IS-IS may reload.

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

Workaround: Disable M-ISIS.

Miscellaneous

- CSCef14493

  Symptoms: After a proxy ARP resolution, the corresponding RAW adjacencies on an RP and line card are incomplete with a MAC length of zero.

  Conditions: This symptom is observed in an IP routed interworking scenario.

  Workaround: There is no workaround.

- CSCef28706

  Symptoms: The memory of an RP may become low, eventually causing the router to reload.

  Conditions: This symptom is observed during an LDP checkpoint test after an SSO switchover.

  Workaround: There is no workaround.

- CSCef43691

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef49462

  Symptoms: ATM Port Mode Cell Relay over MPLS traffic and ATM Port Mode Cell Relay over L2TPv3 traffic is not switched via the PXF engine but punted to the RP.

  Conditions: This symptom is observed on a Cisco 7304 but could occur on any Cisco platform that supports the ATM Port Mode Cell Relay over MPLS feature and the ATM Port Mode Cell Relay over L2TPv3 feature in the PXF engine.

  Workaround: There is no workaround.

- CSCef51081

  Symptoms: A traceroute does not show all entries on a Cisco 7500 series that functions as a PE router and that is configured for distributed CEF.

  Conditions: This symptom is observed in an MPLS VPN network that has multiple CE routers connected to the PE router when a local CE router is connected to the PE router via a serial link and when a traceroute is sent from a remote CE router to the local CE router.

  Workaround: Do not configure dCEF on the PE router. Rather, configure CEF.

- CSCef61610

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

- CSCef87708

  Symptoms: A Virtual Router Redundancy Protocol (VRRP) operation fails on the native Gigabit Ethernet (GE) interface of a Cisco 7304. However, normal VRRP operation occurs on the same router on a Fast Ethernet interface.

  Conditions: This symptom is observed when the GE interface reduces the IP time-to-live field for a packet on the local LAN to a number below 254.

  Workaround: There is no workaround.

- CSCeg02811

  Symptoms: the power-on diagnosis loopback test of a Cisco ONS 15530 8-port FC/GE aggregation card (15530-FCGE-8P) may report a failure.

  Conditions: This symptom is observed very rarely when the Cisco ONS 15530 is booted immediately after a power-cycle.

  Workaround: There is no workaround. Note, however, that no functionality is affected.

- CSCeg04042

  Symptoms: When two Cisco 7304 routers are connected via a multilink bundle, the router that functions as the first-hop router may become stuck in the registering state, and packets are process-switched across the multilink bundle. Also, after passing traffic continuously, packets start to be dropped.

  Conditions: These symptoms are observed on Cisco 7304 routers that have an NSE-100 and that run Cisco IOS Release 12.2(20)S6 or 12.2(25)S2. However, the symptom may also occur when one router has an NSE-100 and the first-hop router has an NPE-G100.

  Workaround: There is no workaround.

- CSCeg08629

  Symptoms: A Cisco 7500 series may generate CCB playback errors and reload the secondary Route Switch Processor (RSP).

Conditions: This symptom is observed when there are channelized T3 port adapters installed in the router and when a channel-group parameter is configured before the channel group is created. To recover from the symptoms, reload the router.

Workaround: Configure the channel-group via the **t1** *t1-line-number* **channel-group** *channel-group-number* **timeslots** *list-of-timeslots* command before you configure any options such as framing of FDL on the channel group.

- CSCeg37929

  Symptoms: SLB rejects a configuration and a virtual server (vserver) does not use the table that is associated with the configuration of the **sticky radius framed-ip** command for connection assignment.

  Conditions: This symptom is observed when you attempt to enter the **sticky radius framed-ip** command on a vserver that is not configured for RADIUS service.

  Workaround: There is no workaround.

- CSCeg51382

  Symptoms: An NSE-100 does not switch OAM cells across an AAL5oMPLS tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router when end-to-end OAM management is configured between the connected CE routers. The NSE-100 drops the OAM packets rather than switching the packets through the AToM tunnel.

  Workaround: Rather than letting the OAM cells be switched through the PE router, configure the PE router to respond to the OAM cells by entering the **oam-ac emulation-enable** ATM VC configuration mode command on the PVC of the PE router.

- CSCeg55387

  Symptoms: Some arguments to Embedded Event Manager (EEM) applets are incorrectly nvgenned, that is, they are saved in the running configuration and, when configured, appear incorrectly in the output of the **show running-config** command. This situation causes errors when you attempt to restore EEM configurations.

  Conditions: This symptom is observed when quotes are placed around some argument strings and when the following EEM commands are nvgenned:

  – the **action snmp-trap** command, when using the *strdata* argument.

  – the **action publish-event** command, when using arguments *arg1* through *arg4*.

  Workaround: Do not use the EEM commands mentioned in the Conditions.

  Further Problem Description: The fix for this caveat removes the *node* argument because it is not required to configure EEM wdsysmon subevents.

- CSCeg58740

  Symptoms: Multicast packets that enter through an interface that is not a designated forwarder (DF) for the rendezvous point (RP) of the destination groups are not dropped by the Parallel eXpress Forwarding (PXF) engine. Proper behavior is that these packets are dropped.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2, that is configured for multicast PIM-BIDIR with multiple paths to the multicast group, and that has PXF enabled.

  Workaround: Remove the parallel paths for the multicast group.

- CSCeg67621

  Symptoms: A Cisco 7304 that operates in RPR redundancy mode may become unusable after a switchover occurs. Line cards may not be recognized and some hardware error messages may appear on the new active RP after the switchover.

  Conditions: This symptom is observed only when Cisco the 7304 is configured for RPR redundancy mode.

  Workaround: Configure the Cisco 7304 for RPR+ or SSO redundancy mode.

- CSCeg73443

  Symptoms: Static NAT incorrectly drops traffic to which NAT cannot be applied.

  Conditions: This symptom is observed on a Cisco 7304 router that is configured with an NSE-100 and that runs Cisco IOS Release 12.2(25)S2. The traffic that is impacted is the traffic that does not match any static NAT configuration command and for which both the ingress and egress interfaces have the **ip nat** interface configuration command enabled.

  Workaround: Configure dynamic NAT rather than static NAT by replacing each static NAT command by three commands: one for the NAT pool, one for the dynamic NAT mapping, and another one for the access list. For example, the **ip nat inside source static** *local-ip global-ip* command is equivalent to the following three commands:

  access-list *access-list-number* **permit ip host** *local-ip* **any**

  ip nat pool name *global-ip global-ip* **prefix-length** *prefix-length*

  ip nat inside source list access-list-number pool *name*

- CSCeg74308

  Symptoms: In an MPLS VPN configuration, assertion failure messages may be generated when you configure a large number of VPNs with many routes.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that has PXF enabled.

  Workaround: There is no workaround.

- CSCeg74797

  Symptoms: A standby Route Processor on a Cisco 7304 that functions in a HA configuration may fail to boot.

  Conditions: This symptom is observed when the router has a large configuration with a size of about 3 MB.

  Workaround: There is no workaround.

- CSCeg78990

  Symptoms: QoS **match not ip** commands match incorrectly.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a class-map configuration contains **match not ip** commands such as the following:

  match not ip dscp *dscp*

  match not ip precedence *precedence*

  match not ip rtp *port*

  Workaround: There is no workaround.

- CSCeg81463

  Symptoms: A memory leak may occur in Any Transport over MPLS (AToM) networks.

Conditions: This symptom is observed when an interface with an xconnect configuration flaps or when the interface that is connected to the MPLS core flaps. 96 bytes of memory are lost with each flap.

Workaround: There is no workaround.

- CSCeg87041

  Symptoms: A Cisco 7304 may reload continuously during a high-availability switchover or may become unusable when any port of a PA-MC-2T3+ port adapter is configured to operate in the non-channelized mode.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S6 or Release 12.2(25)S2 and that is configured with a port adapter carrier card (7300-CC-PA) in which a PA-MC-2T3+ port adapter is installed. The symptom occurs in both high-availability and non-high availability configurations.

  Workaround: Do not configure any port of the PA-MC-2T3+ port adapter to operate in the non-channelized mode or enter the **no cdp run** global configuration command on the router.

  Further Problem Description: When CDP is configured globally or on an interface of the PA-MC-2T3+ port adapter that is configured to operate in non-channelized mode, the router stops processing packets.

- CSCeh02678

  Symptoms: Turbo ACL tables may grow so large that the memory they require is larger than the available PXF memory, causing traffic that requires ACL classification to be punted to the RP. If this situation occurs, an error message similar to the following is generated:

  ```
  toaster_acl_init_node: failed index=[dec] type=[dec] table_size=[dec]
  ```

  This message has a logging severity level of 7 (debugging). The output of the **show pxf interfaces** command for any interface with an ACL configured on it shows the "Punting to RP - acl not ready" message.

  If you subsequently enter the **no access-list** *access-list-number* command, the **no ip access-list standard** command, or the **no ip access-list extended** command to delete an ACL from the running configuration, regardless of whether or not the ACL is attached to an interface, and then add one or more ACEs to the ACL that was deleted, any interface that you subsequently attach the ACL to (or that the ACL was already attached to) incorrectly processes this ACL in PXF instead of on the RP. In this case, the ACL processing in PXF occurs by using old Turbo ACL tables that are based on the configuration at the time when the memory that the Turbo ACL tables require first exceeded the available PXF memory.

  Any incoming packets that do not have entries in the Turbo ACL tables because similar packets have not been received previously are punted to the RP, and new entries for these packets are not added to the tables. Such packets continue to be punted to the RP and are processed correctly. Only packets for which entries already exist in the tables in PXF are processed incorrectly in PXF.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, ACLs configured, and traffic being switched in PXF.

  Workaround: Ensure that all ACLs always contain at least one ACE. If you wish to replace the contents of an ACL with a new set of ACEs, follow these steps:

  1. Add a dummy ACE to the ACL; this ACE must differ from all the ACEs in both the existing and the new configurations of the ACL.

2. Remove all ACEs and remarks except the dummy ACE from the ACL. You can do this by loading the configuration of the ACL without the dummy ACE in it into a text editor, placing the **no** keyword before every **permit**, **deny**, or **remark** keyword, and then entering the **copy** *source-url* **system:running-config** command to apply the configuration. For the *source-url* argument, enter the location of the configuration file.
3. Load the new ACL configuration onto the router, possibly by entering the **copy** command again.
4. Remove the dummy ACE from the ACL. Enter the **show pxf interfaces** command to verify that the "Punting to RP - acl not ready" message is shown in the output for the interface in question, indicating that traffic is punted to the RP for correct ACL processing.

- CSCin73206

  Symptoms: A Cisco router in which a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) is installed may reload unexpectedly.

  Conditions: This symptom is observed when ping packets of a size greater than 512 bytes are sent via the PA-MC-STM-1.

  Workaround: There is no workaround.

- CSCin80743

  Symptoms: Configurations of interfaces on a legacy interface processor such as an EIP or an FSIP on a Cisco 7500 series go down after a redundancy-forced switchover.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S or a later release or Release 12.2(25)S that is configured for SSO or RPR+.

  Workaround: Manually reconfigure the interfaces.

- CSCin82840

  Symptoms: The standby RP resets or an unexpected HA switchover occurs.

  Conditions: This symptom is observed on a Cisco 7500 series that has the Graceful Restart feature enabled. When a switchover or a standby reset occurs, each endpoint that runs an IPC slave sends a register-control-port message to the endpoint that runs the IPC master, causing Endpoint Resolution Protocol (ERP) negotiation to occur. Upon receipt of the last packet during ERP negotiation, if the timer has not stopped, the timer may expire even upon successful ERP negotiation, causing the endpoints that run the IPC slaves to enter into a continuos loop.

  Workaround: There is no workaround.

- CSCin84124

  Symptoms: After performing a Fast Software Upgrade (FSU), none of the interfaces of the active RSP come up.

  Conditions: This symptom is observed on a Cisco 7500 series after you have performed a FSU to Cisco IOS Release 12.2(25)S or Cisco IOS Release 12.0(30)S and after an SSO switchover has occurred.

  Workaround: After the FSU, enter the **microcode reload** command.

- CSCin88357

  Symptoms: A PE router may generate a traceback because of the expiration of a watchdog timer.

  Conditions: This symptom is observed when the PE router has a series of static recursive routes defined and when you enter the **show mpls forwarding** command.

  Workaround: There is no workaround.

- CSCsa43143

  Symptoms: A system exception may occur and the router may reload when you apply a service policy for which the aggregate allocated bandwidth exceeds the bandwidth that is available to the policy. The bandwidth that is available to the policy is either the maximum reserved bandwidth value of the interface (the default is 75 percent of interface bandwidth) or the shape rate of a hierarchical policy.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100. The symptom may also occur when any of the following actions occur:

  - You increase the bandwidth of the class.
  - You decrease the maximum reserved bandwidth value of the interface.
  - You decrease the shape rate of the hierarchical policy.
  - You remove the **max-reserved-bandwidth** command such that the aggregate allocated bandwidth exceeds the bandwidth that is available to the policy.

  Note that a service policy for which the aggregate allocated bandwidth exceeds the bandwidth that is available to the policy is an invalid service policy.

  Workaround: There is no workaround.

- CSCsa48377

  Symptoms: If a policy map that has a non-default class is attached to an interface that has xconnect (L2TPv3) configured, the router may crash.

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

  Workaround: Configure a class map that is the default class, and ensure that this class is the only class in the policy map because L3 classification is not supported for the L2VPN protocols.

- CSCsa57646

  Symptoms: A memory leak may occur in the Route Switch Processor (RSP) of a Cisco 7500 series that is configured for Stateful Switchover (SSO) or Route Processor Redundancy Plus (RPR+) High Availability (HA) mode.

  Conditions: This symptom is observed on a Cisco 7500 series when either SSO or RPR+ is configured and functional. When you log into the router and enter any configuration command, a block of memory that has the size of NVRAM leaks. Each time you start a new session and enter a configuration command, another block of memory leaks. The cumulative leak may consist of a significant amount of memory, depending on the RSP. For example, the RSP8 has 2 MB of NVRAM, so each time you start a new session and enter a configuration command, the router leaks 2 MB of memory.

  The symptom may be platform-independent.

  Workaround: Do not use SSO or RPR+. Rather, configure the router to use High Service Availability (HSA) or Route Processor Redundancy (RPR) mode.

  Further Problem Description: You can verify the occurrence of the symptom in the output of the **show memory | i NV** command. For example, in the following output the router has leaked 8 blocks of memory:

```
Router#show memory | i NV
4357B620 0000126968 00000000 4359A650 001 -- -- 402ADD60 Pre Command NV Buffer
44C81548 0000126968 44C7CE08 44CA0578 001 -- -- 402ADD60 Pre Command NV Buffer
44CA0578 0000126968 44C81548 44CBF5A8 001 -- -- 402ADD60 Pre Command NV Buffer
44CBF5A8 0000126968 44CA0578 44CDE5D8 001 -- -- 402ADD60 Pre Command NV Buffer
```

```
44CDE5D8 0000126968 44CBF5A8 44CFD608 001 -- -- 402ADD60 Pre Command NV Buffer
44CFD608 0000126968 44CDE5D8 44D1C638 001 -- -- 402ADD60 Pre Command NV Buffer
44DF5B70 0000126968 44DF4A98 44E14BA0 001 -- -- 402ADD60 Pre Command NV Buffer
44E742B8 0000126968 44E713A0 44E932E8 001 -- -- 402ADD60 Pre Command NV Buffer
```

- CSCsa58566

  Symptoms: MPLS loadbalancing over multiple paths may not be performed in a balanced way.

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

  Workaround: There is no workaround.

- CSCsa58646

  Symptoms: For all interfaces that have MPLS enabled, except the native Gigabit Ethernet interfaces, the byte counters in the output of the **show mpls forwarding-table** command show 6 bytes more per packet than what is actually sent.

  Conditions: This symptom is observed on a Cisco 7304 that has PXF enabled.

  Workaround: There is no workaround.

- CSCsa58684

  Symptoms: A router may crash when L2TPv3 is configured on an interface.

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

  Workaround: There is no workaround.

- CSCsa60671

  Symptoms: Packets that match some access control entries (ACEs) are denied even though the ACEs are configured to permit these packets. Additionally, packets that match these ACEs are counted as implicit deny drops instead of being counted against the relevant ACEs.

  Conditions: This symptom is observed when you configure more than 16382 ACEs on a Cisco 7304 that has an NSE-100.

  Packets that match the affected ACEs cause the “ACL input deny Drop” and “impli. deny Drop” counters that are shown in the output of the **show pxf accounting** command to increase.

  The limit of 16382 ACEs includes all the ACEs that you have configured in your access control lists (ACLs) and any ACEs in internally-generated ACLs. Internal ACLs are generated when you configure QoS classes by entering the **class-map** command.

  You can see how many ACEs are configured on the router by entering the **test c7300 acl** command if the router runs a Cisco IOS release earlier than Release 12.2(25)S or the **test platform acl** command if the router runs Release 12.2(25)S or a later release. In the output of either command, look for the line with the text “name = ACL_REAL_ACE”. The number shown below this line, next to “allocated”, indicates the number of ACEs that are configured, and “max” indicates the maximum number of ACEs that can be configured. If the value shown next to “alloc_failed” is not zero, you have configured too many ACEs.

  Note that the number of “entries” that are shown as configured in the output of the **show access-lists compiled** command includes additional ACEs that are generated internally to account for fragmented packets when the ACEs match on layer 4 values. These ACEs do not count against the limit of 16382. When you have exceeded this limit, if you unconfigure any ACEs that were configured earlier, it does not cause ACEs that were configured more recently to start functioning correctly.

Workaround: Ensure that all configured ACEs function correctly by changing the ACL configuration to use no more than 16382 ACEs. After you have done so, reload the router to ensure that all configured ACEs function correctly.

- CSCuk55193

  Symptoms: On a router that runs Cisco IOS Release 12.2S and that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), a configuration change that causes one or more LDP sessions to be terminated may cause the router to reload in a manner similar to the following:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x64, pc=0x41285C40,
  ra=0x41285C30, sp=0x44B1C378
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x64, pc=0x41285C40,
  ra=0x41285C30, sp=0x44B1C378
  TLB (store) exception, CPU signal 10, PC = 0x41285C40
  ```

  The symptom may occur with either LDP or Tag Distribution Protocol (TDP).

  Conditions: This symptom is extremely unlikely to occur and requires a very unlikely timing of events between LDP and TCP. The symptom may occur in the following releases and their rebuilds: Release 12.2(18)S, 12.2(20)S, 12.2(22)S, and 12.2(25)S.

  There are many configuration commands that may trigger the symptom, including entering the **no ip vrf** command to remove a VRF that has LDP-enabled interfaces, entering the **no mpls ldp router-id** command to trigger a change to the LDP router ID, or entering the **no mpls ip** interface configuration command to disable LDP on an interface.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCsa49019

  Symptoms: A memory leak may occur in the “Multilink Events” process, which can be seen in the output of the **show memory summary** command:

  ```
  0x60BC47D0 0000000024 0000000157 0000003768    MLP bundle name
  0x60BC47D0 0000000028 0000000003 0000000084    MLP bundle name
  0x60BC47D0 0000000044 0000000001 0000000044    MLP bundle name
  0x60BC47D0 0000000048 0000000001 0000000048    MLP bundle name
  0x60BC47D0 0000000060 0000000001 0000000060    MLP bundle name
  0x60BC47D0 0000000064 0000000013 0000000832    MLP bundle name
  0x60BC47D0 0000000068 0000000008 0000000544    MLP bundle name
  0x60BC47D0 0000000072 0000000001 0000000072    MLP bundle name
  0x60BC47D0 0000000076 0000000001 0000000076    MLP bundle name
  0x60BC47D0 0000000088 0000000018 0000001584    MLP bundle name
  ```

  Conditions: This symptom is observed when two interfaces are configured in the same multilink group or are bound to the same dialer profile.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(25)S2

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(25)S2. All the caveats listed in this section are specific to the Cisco 7304 and are open in Cisco IOS Release 12.2(25)S2. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCee78444

  Symptoms: TDP and OSPF neighborship loss may occur on all interfaces of a Cisco 7304.

  Conditions: This symptom is observed about three to four times per day on a Cisco 7304 is configured with a NSE-100 and that runs Cisco IOS Release 12.2S. However, the neighborships are re-established almost immediately.

  Workaround: There is no workaround.

- CSCef39266

  Symptoms: IP multicast Rendezvous point (RP) discovery messages are not received and RP mappings are not populated on a Cisco 7304.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2S and that is configured for PIM when Auto-RP announcement messages are sent across all the interfaces on a network. The symptom occurs only when the Cisco 7304 is configured with a 4-port or 8-port Ethernet port adapter (PA) that is installed in a PA carrier card and after a multicast configuration command is removed.

  Workaround: To restore the interfaces of the PA to normal operating conditions, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interfaces.

- CSCef67682

  Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

  The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

  ```
  interface Ethernet0/0
    ipv6 traffic-filter nofragments in
  !
  ipv6 access-list nofragments
    deny ipv6 any <my address1> undetermined-transport
    deny ipv6 any <my address2> fragments
    permit ipv6 any any
  ```

  This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

  This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml contain fixes for this issue.

- CSCef97624

  Symptoms: Multicast packets that enter via an Ethernet interface on a port adapter may not be marked correctly when marking is configured on the egress interface or when the multicast packet is decapped to expose the inner payload that is also a multicast packet.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2, that functions as a multicast router or multicast PE router, and that has Parallel eXpress Forwarding (PXF) enabled.

  Workaround: Disable PXF.

- CSCeg09148

  Symptoms: A Cisco 7304 crashes because of a "TLB Modification Exception."

  Conditions: This symptom is observed when you remove the active NSE-100 via an OIR from a Cisco 7304 that is configured for HA and that has VLANs configured on the native GE interfaces. The symptom does not occur on a Cisco 7304 that has an NPE-G100 and that is configured for HA.

  Workaround: There is no workaround.

- CSCeg09902

  Symptoms: A Cisco 7304 may report checksum errors in the output of the **show cef drop** command.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2, that functions as a multicast VPN provider edge (PE) router, and that has Parallel eXpress Forwarding (PXF) enabled.

  Workaround: Disable PXF.

- CSCeg19227

  Symptoms: A Cisco 7304 may not bring up the line protocol on multichannel T1 or E1 ports that are configured for MLP.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and PA-MC-8T1, PA-MC-8E1, and PA-MC-8TE1+ port adapters that are installed in a 7300-CC-PA. The symptom occurs only with a 7300-CC-PA with hardware revision 1.2.

  Attempting to bring up the line protocol on a port by entering the **shutdown** command followed by the **no shutdown** command causes the 7300-CC-PA to reset.

  Workaround: There is no workaround.

- CSCeg26740

  Symptoms: The IGMP State Limit feature is not activated on an interface.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2 and that has the IGMP State Limit feature enabled.

  Workaround: There is no workaround.

- CSCeg30662

  Symptoms: A Cisco 7304 may report the following error message intermittently:

  ```
  %NSE100-3-VA_ERROR: Vanallen ASIC detected an error condition: TIC invalid DMA length.
  ```

Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2, that functions as a multicast VPN provider edge (PE) router, and that has Parallel eXpress Forwarding (PXF) enabled.

Workaround: Disable PXF.

- CSCeg42221

  Symptoms: When you change the MTU for a tunnel interface via the **ip vrf** *vrf-name* command, the PXF MTU value is not immediately changed.

  Conditions: This symptom is observed only on a Cisco 7304 that is configured with an NSE-100, that runs Cisco IOS Release 12.2(25)S2, and that functions in a multicast VPN environment.

  Workaround: Enter the **clear ip mroute vrf** *vrf-name* ***** to re-establish the tunnel interfaces with the right MTU value.

- CSCeg49194

  Symptoms: The NetFlow aggregation cache is not populated with the following NetFlow aggregation schemes:

  - destination-prefix
  - protocol-port
  - source-prefix

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2 and that has Parallel eXpress Forwarding (PXF) enabled.

  Workaround: Disable PXF.

- CSCeg49995

  Symptoms: Pinging a host address through a GRE tunnel may cause a Cisco 7304 to reload.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 when the ping causes a “decapsulation-encapsulation” situation, that is, the route to the host address on the far-end router (on which the GRE tunnel terminates) points back to the GRE tunnel.

  Workaround: There is no workaround.

- CSCeg58740

  Symptoms: Multicast packets that enter through an interface that is not a designated forwarder (DF) for the rendezvous point (RP) of the destination groups are not dropped by the Parallel eXpress Forwarding (PXF) engine. Proper behavior is that these packets are dropped.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2, that is configured for multicast PIM-BIDIR with multiple paths to the multicast group, and that has PXF enabled.

  Workaround: Remove the parallel paths for the multicast group.

Resolved Caveats—Cisco IOS Release 12.2(25)S2

Cisco IOS Release 12.2(25)S2 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S2 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCef00510

  Symptoms: Packets that originate from a Cisco router that is configured with a PA-MC-8TE1+ port adapter may be corrupted and have an invalid FCS. These packets may have the address and control fields compressed even when PFC and ACFC options are explicitly disabled.

  Conditions: This symptom is observed only when traffic is presented simultaneously on several B-channels.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeb19857

  Symptoms: When you reload a router, the router may pause indefinitely with a traceback and bus error exception.

  Conditions: This symptom is observed on a Cisco router that is configured for Open Shortest Path First (OSPF) router and that performs redistribution.

  Workaround: There is no workaround.

- CSCee27479

  Symptoms: Traffic that is processed by a router may be improperly routed to an ESP route.

  Conditions: This symptom is observed when the **ip nat inside source static esp** *local-ip* **interface Loopback0** command is enabled.

  Workaround: There is no workaround.

- CSCee85676

  Symptoms: When VPNv4 route advertisement are received after BGP has converged, the existing path is updated but imported paths from the original path are not updated accordingly.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the **maximum-paths** *number-of-paths* **import** *number-of-paths* command is enabled. The symptom occurs when the path attributes are changed dynamically instead of the path being completely withdrawn and readvertised.

  Workaround: Withdraw the prefix from the remote PE router and then readvertise the prefix.

- CSCef19137

  Symptoms: There are duplicate entries in the flow cache after an interface bounces, causing packet loss. The output of the **show ip cache flow** command may show information similar to the following:

```
SrcIf     SrcIPaddress   DstIf   DstIPaddress   Pr SrcP DstP      Pkts
Gi0/0.1   10.2.0.1       Fa2/0   10.3.0.1       06 2C26 00B3      5
Gi0/0     10.2.0.1       Null    10.3.0.1       06 2C26 00B3<<<<  7
```

Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that runs Cisco IOS Release 12.2(20)S4 when an interface bounces quickly and when the CEF structures are flushed while the ARP cache is not flushed. This situation causes incomplete adjacencies because the CEF process expects a fresh ARP entry to complete its adjacency.

Workaround: Clear the ARP cache or enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCef57022

  Symptoms: OSPF route redistribution in an OSPF VRF process does not function.

  Conditions: This symptom is observed when you associate the OSPF process with a VRF by entering the **router ospf** *process-id* **vrf** *vrf-name* command and configure redistribution under the OSPF VRF process by entering the **redistribute** command.

  Workaround: Do not associate the OSPF process with a VRF; only enter the **router ospf** *process-id* command.

- CSCef91275

  Symptoms: An MPLS TE tunnel stays stuck in the "Path Half Admitting" state, as is shown by the output of the **show mpls traffic-eng tunnel** command, thereby preventing the tunnel from coming up.

  Conditions: This symptom may be observed when a particular third-party router that functions as the headend for the MPLS TE tunnel sends a Path message to a Cisco router that functions as the midpoint for the router MPLS TE tunnel and that does not have the **mpls traffic-eng tunnels** interface configuration command enabled on the outbound interface that would be used to forward the Path message.

  Workaround: Enter the **mpls traffic-eng tunnels** interface configuration command on the outbound interface of the Cisco router. Then, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on this interface, and save the configuration.

- CSCin74330

  Symptoms: The LDP Hello process may not be reinitiated after a TDP ID is received, preventing LDP neighbors from being discovered.

  Conditions: This symptom is observed on a Cisco router that does not have an IP address configured when you first enter the **mpls ip** command and then assign the IP address.

  Workaround: Assign the IP address to an interface of the router before you enable MPLS.

Miscellaneous

- CSCdz84448

  Symptoms: When polling the cbQosREDClassStatsTable of the CISCO-CLASS-BASED- QOS-MIB, spurious memory accesses may occur on a Cisco 2600 series, Cisco 3600 series, or Cisco 7200 series. A Cisco 3640 router may also reboot. The spurious memory accesses may be reproduced when polling the above-mentioned table via Simple Network Management Protocol (SNMP).

  Conditions: This symptom is observed on a Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series that run Cisco IOS Release 12.2(8)T, Release 12.3, or Release 12.3 T.

Workaround: Prevent the router from answering to queries on the cbQosREDClassStatsTable by implementing the following SNMP view in the router configuration:

```
snmp-server view qos internet included
snmp-server view qos 1.3.6.1.4.1.9.9.166.1.20.1 excluded
snmp-server community string view qos ro
```

- CSCed95499

  Symptoms: A Cisco router may crash if a PA driver attempts to convert an uncached iomem address to a cached iomem address.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

  Workaround: There is no workaround.

- CSCee66553

  Symptoms: For traffic that is addressed to certain prefixes, the IP output policy map that is configured for the outgoing interface is not applied to packets that arrive labeled and that are forwarded as IP packets.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S) and that processes MPLS traffic for the following prefixes:

  – prefixes that have a next-hop interface that is not enabled for MPLS forwarding.

  – prefixes that have a next-hop address that is the prefix itself, that is, /32 prefixes that correspond to the IP address on the next-hop router.

  Workaround: There is no workaround.

  Further Problem Description: In certain circumstances, MPLS assigns the implicit-null label as the outgoing label for a prefix path, even if the next-hop router does not advertise the implicit-null label. This behavior, which is referred to as “inferring implicit-null”, makes it possible to support L3 VPNs by means of a mesh of MPLS traffic engineering tunnels between VPN PE routers without enabling LDP in the MPLS core.

  In Cisco IOS software releases that use MFI-based MPLS forwarding (see the Conditions above) as opposed to TFIB-based MPLS forwarding, MPLS may incorrectly infer the implicit-null label for some prefixes whose outgoing interface is not enabled for MPLS forwarding. When this situation occurs, the outgoing label is “Pop” instead of “No Label”.

  If an output policy map is configured for the outgoing interface, the map is not applied to packets that arrive as MPLS packets for such prefixes, have their incoming label popped, and are forwarded as IP packets. The output policy map is applied to incoming MPLS traffic for prefixes whose outgoing label is “No Label” and for all incoming IP traffic that is forwarded on the interface.

- CSCee91386

  Symptoms: A router crashes when you enter the **clear ip route *** command.

  Conditions: This symptom is observed when a FIB entry is marked as deleted but it is not really deleted.

  Workaround: There is no workaround.

- CSCef03049

  Symptoms: A service policy that contains the **bandwidth remaining percent** command along with either the **bandwidth** command or the **bandwidth percent** command does not function as expected.

  Conditions: This symptom is observed on a Cisco 7304 that runs a Cisco IOS interim release for Release 12.2(25)S and that is configured with an NSE-100. However, the symptom may be platform-independent.

Workaround: There is no workaround.

- CSCef13967

  Symptoms: A router that is equipped with ATM interfaces may reload with the following decoded stack trace:

  ```
  adj_il_get_interest_list
  adj_notify
  adj_make_complete
  adj_ios_update_fixup_and_macstr
  adj_ios_mgr_add_and_update
  adj_ios_mgr_add_adj_and_update
  ```

  Conditions: This symptom is observed on a Cisco router when a script unconfigures ATM OAM.

  Workaround: There is no workaround.

- CSCef25960

  Symptoms: End-to-end connectivity (between two CE routers) is lost after an you perform an OIR of the VIP on the PE router.

  Conditions: This symptom is observed when you perform an OIR of the VIP on a Cisco 7500 series that runs Cisco IOS Release 12.2(25)S1, that functions as a PE router, and that is configured for ATM AAL5 over MPLS (AAL5oMPLS).

  Workaround: There is no workaround.

- CSCef29091

  Symptoms: A router may fail to advertise a prefix for which the network portion matches the major net. For example, when 10.0.0.0/8 is the major net, 10.0.0.0/16 is not advertised.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(4) or a later release when the subnet between the two routers is in the same classful range as the advertised prefix of the advertising router.

  Workaround: On the advertising router, enter the **shutdown** command followed by the **no shutdown** command on the interface that is connected to the receiving RIP peer.

- CSCef39466

  Symptoms: A router may fail to advertise a major net route such as 10.0.0.0/8 to a RIP peer.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(3.3) or a later release when the route is redistributed from MP-IBGP into RIP and when the subnet connecting the RIP peer is in the classful range of the advertised major net. The symptom may also occur in other releases.

  Workaround: On the advertising router, enter the **shutdown** command followed by the **no shutdown** command on the interface that is connected to the receiving RIP peer.

- CSCef44438

  Symptoms: A Cisco router may crash when CEF is processing new routing updates while entries are being deleted from the CEF table, for example following a **clear cef table** command or an OIR of a line card.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S or a later release.

  Workaround: There is no workaround.

- CSCef50144

  Symptoms: If XDR multicast groups are deleted and recreated, a very small memory leak may occur.

  Conditions: This symptom is observed when you reboot the standby RP or when you reload a line card, so the symptom occurs rarely.

  Workaround: There is no workaround.

- CSCef51239

  Symptoms: When the MPLS LDP Graceful Restart feature is enabled, when label distribution protocol (LDP)-targeted sessions are configured, and when you globally disable LDP by entering the **no mpls ip** command while a graceful restart-enabled session is recovering, LDP may not be shut down properly.

  When you then re-enable LDP by entering the **mpls ip** command, LDP may not allocate and advertise local labels for certain prefixes. When this situation occurs, MPLS connectivity may be interrupted because the router does not advertise a local label for certain prefixes.

  Conditions: This symptom is observed when targeted sessions are requested to support AToM circuits and when the router runs Cisco IOS Release 12.2S, or a release that is based on Release 12.2S, that contains the fix for CSCed18355.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed18355. Cisco IOS software releases not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: Clear the routes for the affected prefixes from the routing table by entering the **clear ip route** EXEC command. Note that the fix for this caveat is also integrated in Release 12.3 and Release 12.3T.

- CSCef53846

  Symptoms: When fast-switching or MDS is configured in a Multicast VPN (MVPN), packets are punted to the RP instead of switched in the fast path or on the line card.

  Conditions: This symptom is observed when the MAC address of the MDT tunnel is not downloaded onto the line card.

  Workaround: There is no workaround.

- CSCef61721

  Symptoms: CEF may not be updated correctly with a route change.

  Conditions: This symptom is observed when IPv6 BGP is configured and when a route changes from iBGP to eBGP or the other way around.

  Workaround: Repopulate CEF with the correct forwarding information by entering the **clear ipv6 route** *ipv6-address* command.

- CSCef62335

  Symptoms: A "VCID already in use" error message may be generated when you attempt to create an L2TPv3 session.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2S after you first have configured and removed a pseudo-wire configuration and then have removed the xconnect configuration from the PVC.

  Workaround: There is no workaround.

- CSCef63474

  Symptoms: The output of the **show interfaces atm** command is incorrect for the ATM port mode.

Conditions: This symptom is observed when ATM cell-relay functions in port mode. The output of the **show interfaces atm** command shows that the encapsulation is AAL5 PVC mode instead of AAL0 port mode.

Workaround: There is no workaround.

- CSCef67293

  Symptoms: A Cisco 7304 may crash when traffic is switched by the RP.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S, that is configured with an NSE-100, and that functions as a PE router. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCef70242

  Symptoms: Low latency queueing (LLQ) and class-based weighted fair queueing (CBWFQ) may not function for MPLS packets. The MPLS packets that conform to the bandwidth that is allocated to these classes may be dropped.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2S when MPLS packets leave an interface that has an output policy map with **priority** or **bandwidth** commands, or both, configured within its classes. The symptom may also occur in Release 12.3 and Release 12.3T.

  Workaround: There is no workaround.

- CSCef82820

  Symptoms: A provider edge (PE) router in an Any Transport over MPLS (AToM) configuration may crash or the VCs may stay down when you use three or more than three parallel links in the MPLS core.

  Conditions: The symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(25)S and that is configured for AToM. The symptom is specific to the AToM configuration.

  Workaround: Use two parallel links in the MPLS core.

- CSCef89284

  Symptoms: When the **ip verify unicast reverse-path** command is configured on an interface and either the **no ip cef** or the **no ip routing** command is entered, a message such as the following is displayed:

  ```
  % Disabling IP unicast reverse-path check on GigabitEthernet0/2
  ```

  Then, the **ip verify unicast reverse-path** command is removed from the running configuration for each interface for which it is configured, preventing IP traffic from being passed on these interfaces.

  To restore the traffic flow, you must enter the **ip cef** or the **ip routing** command and the **ip verify unicast reverse-path** command on the affected interfaces. However, at this point, entering the **no ip verify unicast reverse-path** command does not have any effect: unicast RPF remains enabled.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2S but may be platform-independent.

  Workaround: There is no workaround.

- CSCef97536

  Symptoms: When Multiprotocol Label Switching (MPLS) label distribution protocol (LDP) is configured and you enter the **clear ip route** EXEC command, the MPLS forwarding entries for some of the cleared routing prefixes may become unlabeled.

Conditions: This symptom is observed for prefixes that are connected (with an unspecified nexthop IP address) and that are not locally recognized. This situation may occur in a configuration in which two LDP peers are connected by a point-to-point link that uses PPP encapsulation, and in which both interfaces are configured to use IP addresses with /32 masks.

A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee12379. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Possible Workaround: Prevent the symptom from occurring by using a shorter network mask when you configure the interfaces or by using another encapsulation such as HDLC.

When the symptom occurs, restore proper operation by forcing the LDP session that is associated with the link to re-establish itself, or by forcing the LDP session to re-advertise labels for the affected prefixes. The LDP session can be reset by entering the **clear mpls ldp neighbor** command, by administratively disabling and then re-enabling one of the interfaces, or by deconfiguring and then reconfiguring LDP on one of the interfaces. The LDP session can be forced to re-advertise labels by modifying the outbound label filtering configuration. However, this method is complicated and should only be attempted if you are already very familiar with the required procedures, and if the routers do not already have a complicated label filtering configuration in place.

- CSCeg10384

  Symptoms: You cannot enable or disable SRP SRR on an SRP port adapter because the **srp srr enable** and **no srp srr enable** commands are not recognized.

  Conditions: This symptom is observed on a Cisco 7200VXR that runs Cisco IOS Release 12.2(14)S7 and that is configured with an SRP port adapter.

  Workaround: There is no workaround. However, this situation does not need to be service-affecting: SRP SRR is enabled by default on the port adapter and SRR kicks in when all nodes on the ring have SRR enabled.

- CSCeg21944

  Symptoms: After an HA switchover while the standby RP comes up, the following error message is generated on the console of the standby RP:

  %HA-4-NOBUF: Failed to allocate buffer for inter-RP IPC message receive

  The configurations of the standby RP and active RP are not synchronized.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that is configured for HA.

  Workaround: There is no workaround.

- CSCeg37358

  The following caveat is closed:

  Symptoms: Multicast packet headers are not cached when PXF is enabled. The cache entries are populated only when PXF is disabled. However, in neither case the packets are dropped and multicast forwarding functions as expected.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2 and that is configured for multicast.

  As of Release 12.2(25)S2, multicast data packets are forwarded by the PXF engine. Multicast control packets are still punted to the RP and are still cached.

  Workaround: If you would like to see all multicast packet headers, disable PXF.

- CSCeg40957

  Symptoms: A router that is equipped with a PA-A3-OC3 ATM port adapter may generate alignment errors.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S1 and that is configured for Xconnect.

  Workaround: There is no workaround.

- CSCeg42817

  Symptoms: A router may crash with a data bus error when you shut down an interface that has RPF check enabled.

  Conditions: This symptom is observed very rarely on a Cisco router when a route change occurs for a prefix that has a path out of an interface with RPF check enabled and when this prefix is recursively resolved in a loop. (For example, prefix A resolves through prefix B, which resolves through prefix A.)

  Workaround: Disable RPF check.

- CSCeg42855

  Symptoms: Multicast flows are not switched in the PXF path when NAT is configured on the multicast traffic input interfaces, on the output interfaces in the outgoing interface list (olist), or on both.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S2 and that has an NSE-100.

  Workaround: There is no workaround. Multicast NAT is not supported in the PXF path.

- CSCeg47382

  Symptoms: After a switchover occurs, the new active RP crashes.

  Conditions: This symptom is observed on a Cisco router that is configured with dual RPs after an FSU to Cisco IOS Release 12.2(25)S is performed.

  Workaround: There is no workaround.

- CSCeg47385

  Symptoms: When Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP), and Nonstop Forwarding (NSF)/Stateful Switchover (SSO) are configured on a router, the CPU utilization may approach 100 percent, and LDP may cease to checkpoint the local label bindings. When this symptom occurs, the output of the **show process cpu sorted** command identifies the "LDP HA" process as the cause of the high CPU utilization.

  Conditions: This symptom is observed on the active RP of a router that is configured with dual RP and that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S. However, the symptom is extremely unlikely to occur.

  Workaround: Reload the active RP.

- CSCeg52128

  Symptoms: A router may reload unexpectedly when you remove a service policy.

  Conditions: This symptom is observed when you remove a service policy that contains one or more classes with the **police** command and when there is traffic for these classes. The symptom may occur in either input or output service policies and on any type of interface, physical interface, subinterface, ATM VC, or Frame Relay VC.

On hardware-accelerated platforms, the symptom occurs only when the service-policy traffic is processed by the main forwarding processor (that is, the RP). The symptom does not occur when the service-policy traffic is hardware-accelerated.

Workaround: There is no workaround.

- CSCeg53716

  Symptoms: An egress QoS service policy does not function when NAT is configured.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when NAT translation and egress QoS are enabled on an output interface.

  Workaround: There is no workaround.

- CSCin75941

  Symptoms: After an RPR+ switchover, pings from one CE router to another CE router via IMA UNI and IMA group interfaces fail.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a PA-A3-8E1 or PA-A3-8T1 port adapter that has the "Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: VP Mode" feature enabled with either Single Cell Relay or Packed Cell Relay and that has IMA UNI and IMA group interfaces.

  Workaround: There is no workaround.

- CSCin84650

  Symptoms: Packets of shaped IP DSCP classes of a policy map may be dropped, causing the output shaping rate to be lower than the configured rate in the policy map.

  Conditions: This symptom is observed on a Cisco 7304 that has a NPE-G100 when an output interface is attached with a policy map that has a shaping configuration for IP DSCP-based classes and when the interface has oversubscribed traffic, including the default class at output.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCef80081

  Symptoms: A Multilink PPP (MLP) bundle that is configured on an ISDN BRI interface may not come up.

  Conditions: This symptom is observed on a Cisco 7200 series when MLP is configured on an ISDN BRI interface. However, the symptom may be platform-independent.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(25)S1

Cisco IOS Release 12.2(25)S1 is a rebuild release for Cisco IOS Release 12.2(25)S. The caveats in this section are resolved in Cisco IOS Release 12.2(25)S1 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCee76965

  Symptoms: The line protocol on serial or POS interfaces with HDLC may become disabled for a few seconds.

Conditions: This symptom is observed after a switchover to a redundant RP on a Cisco 7500 series that is configured for SSO and that has a large number (about 2000) of dot1q interfaces defined.

Workaround: Increase the HDLC keepalive time or disable keepalives. Replacing HDLC with PPP is another workaround.

IP Routing Protocols

- CSCec07636

  Symptoms: When the following Open Shortest Path First (OSPF) MIB tables are queried via snmpwalk, some interfaces may not be displayed:

  - ospfNbrTable
  - ospfIfTable
  - ospfIfMetricTable

  Conditions: This symptom is observed on any Cisco platform that runs OSPF.

  Workaround: There is no workaround.

- CSCec22723

  Symptoms: A router may unexpectedly reload because of a watchdog timeout or bus error in OSPF.

  Conditions: This symptom is observed when iSPF is configured under OSPF.

  Workaround: Remove the iSPF configuration from OSPF by entering the **no ispf** command.

ISO CLNS

- CSCec07636

  Symptom: A CPUHOG condition may occur when there are hundreds of back-to-back point-to-point interfaces that are configured for IS-IS.

  Condition: This symptom is observed when the **router isis** command is enabled and when MPLS traffic engineering is configured.

  Workaround: There is no workaround.

Miscellaneous

- CSCef22949

  Symptoms: The following message is generated when you add a cluster member by using the CLI or via the startup configuration:

  ```
  CMP-NAT-ACL-Cluster-NAT already contains this IP address pair.
  ```

  Conditions: This symptom is observed on a Cisco platform that includes featurette CSCea91540 that enables an ACE to configure up to 10 source ports and up to 10 destination ports. Cisco IOS Release 12.2S and Release 12.3T may be affected by this symptom.

  Workaround: There is no workaround.

- CSCef25939

  Symptoms: A router crashes when you modify the WRED parameters in a policy map.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(25)S. However, the symptom may be platform-independent.

Workaround: There is no workaround.

- CSCef48325

  Symptoms: WRED counters do not function on distributed platforms such as a Cisco 7500 series and a Cisco 7600 series.

  Conditions: This symptom is observed on a distributed Cisco platform that runs Cisco IOS Release 12.0(26)S3, 12.0(29)S, 12.2(25)S, 12.3(10), or 12.3(11)T and that has dWRED configured.

  Workaround: There is no workaround.

- CSCin81343

  Symptoms: During a CPU switchover on a Cisco 15540 extended range transponder, a temporary traffic interruption may occur. When the switchover is complete, traffic resumes. This symptom is intermittent and may not affect all transponders in a chassis.

  The traffic interruption may occur for the following types of encapsulation:

  - ETR/CLO
  - 100-Mbps Fast Ethernet / FDDI
  - ESCON/SBCON
  - 1-Gbps FC/FICON
  - 1-Gbps ISC (ISC1, ISC3-Peer-1gig)
  - 2-Gbps FC/FICON
  - 2-Gbps ISC (ISC3-Peer-2Gig)

  Conditions: This symptom is observed on a Cisco ONS 15540 ESP and Cisco ONS 15540 ESPx in which extended range transponders are installed.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP “source quench” messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Wide-Area Networking

- CSCee44086

  Symptoms: After an RP switchover, a multilink PPP interface cannot forward any traffic.

  Conditions: This symptom is observed on a Cisco 7500 series, Cisco 10000 series, and Cisco 12000 series.

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

Open Caveats—Cisco IOS Release 12.2(25)S

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(25)S. All the caveats listed in this section are open in Cisco IOS Release 12.2(25)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCeb50904

  Symptoms: When you reload a router that is configured with a master Route Processor (RP) and a slave RP by entering the **reload** EXEC command on the master RP, the master RP and the slave RP may change roles. That is, the master RP may become the slave RP, and the slave RP may become the master RP.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with dual RPs.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCuk49939

  Symptoms: On a PA-4E or PA-8E port adapter, the MPLS/Tag MTU does not allow an MTU setting that is greater than the MTU setting of the interface. This situation causes the maximum size of unfragmented packets, transferable across an MPLS network, to be reduced by four bytes for every label that is applied to the packet.

  Conditions: This symptom is observed on a Cisco 7xxx series that runs Cisco IOS Release 12.2(22)S or a later release, that is configured with a PA-4E or PA-8E port adapter, and that is configured for MPLS.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCin74330

  Symptoms: The LDP Hello process may not be reinitiated after a TDP ID is received, preventing LDP neighbors from being discovered.

  Conditions: This symptom is observed on a Cisco router that does not have an IP address configured when you first enter the **mpls ip** command and then assign the IP address.

  Workaround: Assign the IP address to an interface of the router before you enable MPLS.

Miscellaneous

- CSCec45164

  Symptoms: Two interfaces may have the same Cisco Express Forwarding (CEF) interface index when the following configuration sequence occurs:

  1. You create a subinterface.
  2. You delete this subinterface.
  3. You create another subinterface.
  4. You recreate the first subinterface.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S or Release 12.2 S.

  Workaround: There is no workaround. Reload the router to clear the condition.

- CSCee48872

  Symptoms: A router crashes when the watchdog times out.

  Conditions: This symptom is observed on a Cisco router that is configured with thousands of TE tunnels.

  Possible Workaround: Increase the memory to support the configuration.

- CSCin65637

  Symptoms: Latency is higher when priority queueing is configured for an interface of a 2-port Packet-over-SONET OC-3c/STM-1 port adapter (PA-POS-2OC3). Latency is higher even for priority packets.

  Conditions: This symptom is observed when the data rate exceeds the OC-3 line rate and may occur on all types of VIPS on a Cisco 7500 series and on a Cisco 7200 series that is configured with an NPE-300, NPE-400, or NSE-1. The symptom does not occur on a Cisco 7200 series that is configured with an NPE-G1.

  Workaround: To prevent the data rate from exceeding the OC-3 line rate, configure traffic shaping. This also brings the latency for priority packet to tolerable limits.

- CSCin67253

  Symptoms: A Cisco 7500 series may stop forwarding traffic via an Any Transport over Multiprotocol Label Switching (AToM) virtual circuit (VC) that is configured on an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+).

  Conditions: This symptom is observed on a Cisco 7500 series that has a PA-MC-8TE1+ that is configured for frame relay over Multiprotocol Label Switching (FRoMPLS) or frame relay/ATM/Ethernet interworking when you perform an online insertion and removal (OIR) of the Versatile Interface Processor (VIP) in which PA-MC-8TE1+ is installed.

Workaround: Remove and reconfigure the affected AToM VC.

- CSCin75253

  Symptoms: The following traceback and error message may appear when you boot a Cisco ONS 15530 or Cisco ONS 15540:

  ```
  %IPC-5-INVALID: Invalid dest port=0x0
  -Traceback= 600A960C 606C8E90 606D6F88 606D6DD8 606D7230 60252B54 607D8EA0 607C5C6C
  60810894 6080F404 6080EA34 6005CEA8 60073054 60073480 6032BDE8 60326948
  ```

  Conditions: This symptom is observed on a Cisco ONS 15530 and Cisco ONS 15540 that run Cisco IOS Release 12.2(25)S.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCee44086

  Symptoms: After an RP switchover, a multilink PPP interface cannot forward any traffic.

  Conditions: This symptom is observed on a Cisco 7500 series, Cisco 10000 series, and Cisco 12000 series.

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

- CSCef02653

  Symptoms: A Cisco router that is configured for datagram encapsulation over X.25 may fail to respond to pings when X.25 payload compression is enabled.

  Conditions: This symptom is observed on a Cisco router that has the **x25 map ip** command enabled with the **compress** keyword.

  Workaround: Disable X.25 payload compression.

Resolved Caveats—Cisco IOS Release 12.2(25)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(25)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCea87766

  Symptoms: A Cisco platform may generate the following error message:

  ```
  <interface name> is a static pool and cannot be tuned
  ```

  Note that instead of "<interface name>," an actual interface name will be stated in the message.

  Conditions: This symptom is observed when you display the running configuration.

  Workaround: There is no workaround.

- CSCeb20967

  Symptoms: A Route Switch Processor (RSP) may reload unexpectedly when a bus error with an invalid memory address occurs while packets are placed into a hold queue.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S, 12.1(14)E4, or 12.2 S when the following sequence of events occurs:

  1. A packet is switched via Cisco Express Forwarding (CEF).
  2. The egress interface has queueing/shaping configured.
  3. The egress interface is congested, causing the packet to be placed into the hold queue.

  Workaround: There is no workaround.

- CSCeb37423

  Symptoms: A Cisco 7500 series may reload because of a software condition when you enter the **no shutdown** interface configuration command on an interface.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for LAN Emulation (LANE).

  Workaround: There is no workaround.

- CSCeb43981

  Symptoms: When High System Availability (HSA) is configured, the secondary Route Switch Processor (RSP) may not become active when the primary RSP reloads unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S or Release 12.2 S when you configure the primary RSP in slot 2 and the secondary RSP in slot 3.

  Workaround: Configure the secondary RSP in slot 2 by entering the **slave default-slot 2** global configuration command. The symptom does not occur when you configure the secondary RSP in slot 2 and the primary RSP in slot 3.

- CSCed05135

  Symptoms: A Cisco platform that is configured for Kerberos authentication may crash.

  Conditions: This symptom is observed when you attempt to make an encrypted Kerberized Telnet connection.

  Workaround: There is no workaround.

- CSCed64664

  Symptoms: A "%SYS-2-LINKED: Bad enqueue ....." error message may be seen in the syslog of an LNS right after traffic is send through a PPP multilink bundle that is establish via an L2TP session on the LNS. This message is also seen when multilink PPP fragments are switched or when multicast packets are replicated.

  Certain packet buffers (particle clones) are eventually depleted, and multilink fragmentation stops working when all particle clones are exhausted. You can monitor the availability of particle clones by entering the **show buffers | begin Particle Clones:** EXEC command; the command does not produce any output if no more particle clones are available.

  Conditions: This symptom is observed when multilink is configured on a virtual template that is handling the VPDN sessions or when multicast packets are switched.

  Workaround: When L2TP multilink calls are terminated, disable multilink fragmentation by entering the **ppp multilink fragment disable** interface configuration command on the virtual template.

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial-In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

- CSCee35740

  Symptoms: After a VIP crashes, a FIB-3-FIBDISABLE error message due to an IPC timeout may occur for all the slots of the VIP.

  Conditions: This symptom is observed on a Cisco 7500 series after the VIP crashes and before the VIP recovers. The FIB-3-FIBDISABLE error message is generated for all the slots of the VIP, causing dCEF switching to become disabled.

  Workaround: There is no workaround. You can reenable dCEF by entering the **clear cef linecard** command.

- CSCee58426

  Symptoms: A router that is configured for MPLS QoS forwarding crashes.

  Conditions: This symptom is observed on a Cisco router when you use MPLS QoS forwarding over an ATM PVC bundle.

  Workaround: There is no workaround.

- CSCee58479

  Symptoms: When you configure an interface of a PA-MC-8TE1 on a Cisco 7200 series, the router to which the interface of the PA-MC-8TE1 is connected at the other end may crash.

  Conditions: This symptom is observed when the interface of the PA-MC-8TE1 functions in channelization mode and when CDP is enabled.

  Workaround: Disable CDP globally by entering the **no cdp run** global configuration command or by entering the **no cdp enable** interface configuration command on the interface of the router to which the PA-MC-8TE1 interface is connected at the other end.

- CSCee60844

  Symptoms: A software-forced crash may occur on a Cisco 7500 series.

  Conditions: This symptom is observed on a Cisco 7500 series with a PA-T3 or PA-2T3 configured for class-based weighted fair queueing (CBWFQ).

  Workaround: Remove CBWFQ from the interface or policy map.

- CSCee63808

  Symptoms: A router reloads when you enter the **show monitor event-trace merged-list** *component* command and you use a long string for the *component* argument.

  Conditions: This symptom is observed on a Cisco 7200 and Cisco 7500 series that run Cisco IOS Release 12.2 S.

  Workarounds: Enter a short string for the *component* argument.

- CSCee71685

  Symptoms: A Cisco router may crash because of low I/O memory as a result of an IPC storm that is associated with writing the CDP multicast address to an Ethernet MAC filter.

  Conditions: This symptom is observed on Cisco 7304 with an Ethernet, Fast Ethernet, or Gigabit Ethernet port adapter. However, the symptom is platform-independent and could occur on any Cisco platform.

  Workaround: If CDP is not required for SNMP network management, enter the **no cdp run** command in the startup configuration.

  If CDP is required for SNMP network management, enter the **no cdp enable** command on each interface and subinterface in the startup configuration, except for the management interfaces and subinterfaces. (There is a maximum of 10 management interfaces and subinterfaces.)

- CSCee78266

  Symptoms: A Cisco 7500 series may reload in an indefinite loop when you unintentionally enter the **show list** *number* hidden command.

  Conditions: This symptom is observed when you, for example, abbreviate the **show line 2000** command as the **show li 2000** command and actually execute the **show list 2000** hidden command.

  Workaround: Do not abbreviate the **show line** command as the **show li** command but enter the full command.

- CSCee84611

  Symptoms: An NTP broadcast client may fail to synchronize with an NTP broadcast server if the server cannot be reached from the client.

  Conditions: This symptom is observed in Cisco IOS interim Release 12.2(12.11)T or a later release, including Release 12.3. However, the symptom may also occur in other releases.

  Workaround: Ensure that the server can be reached from the client.

- CSCuk50527

  Symptoms: An MPLS/Tag MTU does not allow a setting that is larger than the MTU of the interface. This situation causes the maximum size of unfragmented packets that are transferred across the MPLS network to be reduced by 4 bytes for every label that is applied to the packet.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(22)S and that is configured for MPLS.

  Workaround: There is no workaround.

- CSCuk50643

  Symptoms: A router reloads when the NTP server association is set via SNMP.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(22)S.

  Workaround: Enter the **ntp peer** command.

IBM Connectivity

- CSCec68023

  Symptoms: When you enter the **dlsw bridge-group** *group-number* global configuration command, the following error messages and tracebacks may be generated:

```
%IDBINDEX_SYNC-3-UNKNOWN_TYPE: IDB type is unknown and cannot be synced: "",0
-Traceback= 4021FCAC 40220F58 4021FF10 4022122C 40455C90 40457D4C 41256D8C 412592B0
4125982C 40CC9D04 4125C6C8 4125B83C 4125B6A8 412620AC 41293FD4 4128A660
%IDBINDEX_SYNC-3-IDBINDEX_INITKEY: Cannot initialize IDB index table lookup key: "",0
```

  Conditions: This symptom is observed only on a Cisco platform that is configured for High Availability (HA).

  Workaround: There is no workaround. However, the symptom is of a cosmetic nature. Data-link switching plus (DLSw+) functions properly.

Interfaces and Bridging

- CSCdz89972

  Symptoms: The **media-type mii** interface configuration command cannot be configured on a Fast Ethernet interface on a Cisco router.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCed29590

  Symptoms: An interface on a Cisco 7500 series that is configured for distributed Multilink PPP (dMLP) may stop transmitting data.

  Conditions: This symptom is observed when the links in an MLP bundle flap. When the router detects that the interface does not transmit data, the router automatically resets all Versatile Interface Processors (VIPs) to restore proper functioning.

```
The following log information shows the sequence of events when the symptom occurs:
%LINK-3-UPDOWN: Interface Serial10/1/1/11:23, changed state to down
%LINK-3-UPDOWN: Interface Serial10/1/1/12:23, changed state to down
%LINK-3-UPDOWN: Interface Multilink9, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/1/1/11:23, changed
                     state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/1/1/12:23, changed
                     state to down
%LINK-3-UPDOWN: Line protocol on Interface Multilink9, changed
%LINK-3-UPDOWN: Interface Serial10/1/1/12:23, changed state to up
%LINK-3-UPDOWN: Interface Multilink9, changed state to up
%LINK-3-UPDOWN: Interface Serial10/1/1/11:23, changed state to up
%RSP-3-RESTART: interface Serial10/1/1/11:23, output frozen
%RSP-3-RESTART: cbux complex
```

  Workaround: There is no workaround.

- CSCee02270

  Symptoms: A Cisco router may unexpectedly reload because of a software-forced crash that is due to a watchdog timeout.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(26)S1, Release 12.2 S, or Release 12.3(8)T when you enter the **show list** command.

  Workaround: There is no workaround.

- CSCee22523

  Symptoms: A VIP that contains a PA-A3-OC12 ATM port adapter may unexpectedly reload.

  Condition: This symptom is observed on a Cisco 7500 series that functions in an ATM LANE configuration.

  Workaround: There is no workaround. The traffic on the VIP is disrupted until the VIP comes back up.

- CSCee91408

  Symptoms: Packets may not got through when ATM VP trunking over AToM is configured.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim release of Release 12.2(25)S. However, note that this caveat is resolved in Release 12.2(25)S.

  Workaround: There is no workaround.

- CSCee91605

  Symptoms: A Cisco 2691 or Cisco 3725 may not boot and may generate the following error message:

  ```
  ERR-1-GT64120 (PCI-1): Fatal error, PCI Master abort
  ```

  Conditions: This symptom is observed on a Cisco 2691 and Cisco 3725 that are configured with an NM-1GE network module that is installed in port one. However, this symptom is not platform-dependent.

  Workaround: There is no workaround.

- CSCin58433

  Symptoms: The driver code of a third-party vendor Fast Ethernet controller that is part of a C7200-I/O-FE I/O controller may pause indefinitely or reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7200 series when a packet enters the third-party vendor Fast Ethernet controller, when this packet is forwarded to a Multilink PPP (MLP) interface, and when another packet is forwarded by the third-party vendor Fast Ethernet controller before the first packet has left the MLP interface.

  Workaround: There is no workaround.

- CSCin69944

  Symptoms: AoMPLS VCs may go down or no longer allow data transfers after an OIR and an SSO switchover are performed.

  Conditions: This is symptom is observed on a Cisco 7500 series that functions in SSO redundancy mode.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command after you have performed an OIR of the component on which the AoMPLS VCs are configured. Doing so minimizes the loss when a switchover is performed and enables traffic to continue to be forwarded fine.

- CSCin74070

  Symptoms: Performance degrades when the number of VCs through which traffic is sent is scaled for PCRoMPLS AToM VCs.

  Conditions: This symptom is seen on a Cisco 7500 series with a PCRoMPLS configuration on VCs.

  Workaround: There is no workaround.

- CSCin76595

  Symptoms: A Cisco 7500 series may show a large number of tracebacks of the "64bit read" access type on a VIP.

  Condition: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2 S or Release 12.3 when the VIP contains a PA-POS-OC3, PA-POS-2OC3, or PA-SRP-OC12.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdv57965

  Symptoms: Although you may able to configure more than 4 Gbps of bandwidth for Resource Reservation Protocol (RSVP) or for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, the actual reserved bandwidth that is established for RSVP or the MPLS TE tunnel may be much less than 4 Gbps.

  The output of the **show running-config interface** *type number* privileged EXEC command shows the configured bandwidth. The output of the **show ip rsvp reservation** EXEC command shows the actual reserved bandwidth for RSVP.

  Conditions: This symptom is observed when the interface on which RSVP or the MPLS TE tunnel is configured does have sufficient bandwidth available to satisfy the configured bandwidth but the actual reserved bandwidth is less than the configured bandwidth.

  Workaround: There is no workaround.

  Further Problem Description: This caveat only affects interfaces that can handle more than 4 Gbps. If a router does not have such high-speed interfaces, the symptom does not occur.

- CSCea59206

  Symptoms: When you configure the **distribute-list** router configuration command under the **address-family ipv4 vrf** *vrf name* router configuration command, the **distribute-list** router configuration command may appear under the main routing process as may be displayed in the output of the **show running-config** EXEC command.

  Conditions: This symptom is observed in either a Routing Information Protocol version 2 (RIPv2) or a Border Gateway Protocol (BGP) configuration when you specify the *interface-type* and *interface-number* arguments of the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} [*interface-type interface-number*] router configuration command.

  The symptom does not occur when you do not define the *interface-type* and *interface-number* arguments and only enter the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} router configuration command.

  Workaround: There is no workaround.

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml.

- CSCed39619

  Symptom: When you enter the **passive-interface default** router configuration command in an Open Shortest Path First (OSPF) environment, all interfaces, including a virtual link, become passive interfaces. However, the virtual link may not come up even if the routers that terminate the endpoints of the virtual link have a full neighboring relationship via a nonpassive interface. When you enter the **no passive-interface** *interface-type interface-number* router configuration command and you enter **virtual 0** for the *interface-type interface-number* argument, the command may not function, and the virtual link may remain down.

  Conditions: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.0 S, 12.2 S. or 12.3, that functions in an OSPF environment, and that has the **passive-interface default** router configuration command enabled.

  Workaround: Delete the virtual link and disable the **passive-interface default** router configuration command. Then, reconfigure the virtual link before you reenter the **passive-interface default** router configuration command.

  Alternate Workaround: Do not enter the **passive-interface default** router configuration command. Rather, enter the **passive-interface** *interface-type interface-number* router configuration command for each individual interface that must be configured as a passive interface.

- CSCed55180

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series, the traffic interruption may last longer than you would expect.

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.2(22)S and that is configured with a Route Switch Processor 4 or 8 (RSP4 or RSP8) when the router is configured with a large number (100,000) of Border Gateway Protocol (BGP) routes and Ethernet interfaces that process traffic.

  Workaround: There is no workaround. One way to help reduce the length of the traffic interruption is to add static ARP entries.

- CSCed59978

  Symptoms: A router may crash and reload due to a bus error, and the following error message may appear:

  ```
  Unexpected exception, CPU signal 10
  ```

  Conditions: This symptom is observed on a Cisco router that is running OSPF and that is configured for incremental SPF.

  Workaround: Remove incremental SPF from the router by entering the **router ospf** *process-id* command followed by the **no ospf** command.

- CSCed62479

  Symptoms: The **neighbor next-hop-unchanged** command may not keep the next hop unchanged for internal paths.

  Conditions: This symptom is observed when an internal route is learnt via a confederation eBGP peer.

  Workaround: There is no workaround.

- CSCed75295

  Symptoms: FRR LSPs may fail to provide protection with a Next-next-hop (NNHOP) backup tunnel.

  Conditions: This symptom is observed only when a primary LSP reaches beyond a merge point.

  Workaround: There is no workaround.

- CSCed86069

  Symptoms: A software-forced chunk corruption crash may occur when a MALLOC failure occurs.

  Conditions: This symptom is observed on a Cisco platform that has the **bgp dampening** command enabled.

  Workaround: There is no workaround.

- CSCed93630

  Symptoms: A Cisco router running Cisco IOS Release 12.0 S, 12.2 S, or 12.3 T can reload unexpectedly.

  Conditions: The problem can occur only if a **bgp debug** command is enabled.

  Workaround: There is no workaround.

- CSCee11274

  Symptoms: BGP may fail to reestablish a session when you remove a line card, PA, VIP, or module and replace it with a card of a different type. For example, the problem occurs when you remove a 1-port GE line card and replace it with a 3-port GE line card. However, if you replace the 1-port GE line card with another 1-port GE line card (or you just plug the same 1-port GE line card back in the chassis), the problem does not occur.

  Conditions: This symptom is observed when the router one side of the BGP session is configured with the **neighbor** *ip-address* **transport connection-mode active** command and when a line card, PA, VIP, or module is changed on the router at the other side of the BGP session. Furthermore, the router at the other side of the BGP session is configured with the **neighbor** *ip-address* **update-source** *interface* command, and the *interface* argument refers to the interface on the line card, PA, VIP, or module that is changed.

  Workaround: Disable and reenter the **neighbor** *ip-address* **update-source** command.

- CSCee24899

  Symptom: A router that is configured for multicast routing may reload due to a bus error.

  Condition: This symptom is observed on a Cisco router that runs a Cisco IOS software release that contains the fix for CSCec80252. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec80252. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCee25019

  Symptoms: The OSPF process may still redistribute IPv6 routes that are denied by an access list that is configured on a route map. Alternatively, if a prefix is permitted by the access list, the prefix may not be advertised by OSPF.

  Conditions: This symptom is observed when an access list on a route map is modified after the route map is configured for redistribution.

  Workaround: To flush existing external LSAs and generate correct external LSAs that OSPF can redistribute based on the route map, enter the **clear ipv6 ospf redistribution** command.

- CSCee35125

  Symptoms: A Cisco router may crash when you enter the **clear ip route *** command.

  Conditions: This symptom is observed when the routing table has a default route.

  Workaround: There is no workaround.

- CSCee36721

  Symptoms: An OSPF Designated Router (DR) may fail to regenerate the network LSA when you reload the router.

  Conditions: This symptom is observed on a Cisco router that functions as a DR for an OSPF interface when another interface with the same interface address is present in the area but is in a shut down state.

  Workaround: Remove the duplicate interface address and enter the **clear ip ospf process** command.

- CSCee40207

  Symptoms: The BGP Open processes may hold more and more memory, may cause a memory leak, may finally run out of memory, and may cause a Malloc Failure error.

  Conditions: This symptom is observed when there are BGP neighbors stuck in the active state (that is, a BGP neighbor is configured but the peer address is not reachable) and when some NSF/SSO RP switchovers occur and the standby becomes active.

  Workaround: Shut down the neighbors that are not used.

  Further Problem Description: When the memory leak occurs, it will be a consistent 1k leak for each neighbor that is not up every 2 minutes.

- CSCee49764

  Symptoms: The **redistribute maximum-prefix** command may not take effect.

  Conditions: This symptom is observed when you enter this command while OSPF is processing an SSO switchover.

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

- CSCee59315

  Symptoms: A BGP VPNv4 table may contain paths that may be imported from deleted BGP table entries or from table entries that have a different prefix from the importing prefix.

```
An example of a path from a deleted BGP table entry is as follows:
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 52
Paths: (1 available, best #1, table vpn2)
  Advertised to non peer-group peers:
  10.4.1.2
  2 100, imported path from 2829:2829:185404173:11.13.11.13/-53
```

```
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:3
```

The entry that this path is imported from has been removed from the table and its memory contents contain an incorrect pattern. When the incorrect pattern is displayed as a prefix, it appear as "2829:2829:185404173:11.13.11.13/-53".

A mismatched prefix appears as follows:

```
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 54
Paths: (2 available, best #1, table vpn2)
Flag: 0x820
  Advertised to non peer-group peers:
  10.10.10.10 10.20.20.20
  2
    10.4.1.2 from 10.4.1.2 (10.4.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:2
  2 100, imported path from 200:2:172.16.0.0/24
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external
      Extended Community: RT:1:3
```

This BGP VPNv4 table entry is for prefix 192.168.0.0/32 but it shows that a path is imported from 172.16.0.0/24. This situation occurs when a path has a link to a deleted BGP table entry, and then the memory for the deleted entry is reused for a new table entry of which the prefix may not match with the importing entry.

Conditions: These symptoms are observed when you enter the **maximum-paths import** *number* command in router BGP address-family IPv4 VRF mode. The *number* argument indicates the number of paths to import from one VRF to another.

Workaround: Remove the **maximum-paths import** *number* command from the router BGP address-family IPv4 VRF mode.

- CSCee66936

  Symptoms: A software-forced reload may occur on a router that is configured with a DVMRP tunnel.

  Conditions: This symptom is observed on a Cisco router when the DVMRP tunnel is brought up and routing information is redistributed between DVMRP and MBGP.

  Workaround: There is no workaround.

- CSCee67450

  A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the **bgp log-neighbor-changes** command configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the **show ip bgp neighbors** command or running the **debug ip bgp** *neighbor* **updates** command for a configured BGP neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

- CSCee70798

  Symptoms: You cannot configure **ip igmp ssm-mapping** commands, nor **ip igmp limit** commands.

  Conditions: This symptom is observed a Cisco 7200 series and Cisco 7500 series that runs Cisco IOS Release 12.2 S.

  Workaround: There is no workaround.

- CSCee74586

  Symptoms: A receiver on an NBMA link may be blackholed.

  Conditions: This symptom is observed when (*,G) joins are incorrectly processed and when the source and the receiver of the traffic are on two different routers on the same NBMA link.

  Workaround: There is no workaround.

- CSCee76562

  Symptoms: Spurious memory accesses may occur and tracebacks may be generated.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(9.3)T when NHRP, IPSec, NAT, and EIGRP are configured. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCee83549

  Symptoms: When multipath is configured, one of the paths may have an inconsistent (old) label, causing only one path to be operational.

  Conditions: This symptom is observed when BGP does not update the outlabel information in the TFIB and for CEF.

  Workaround: Clear or readvertise the route that is inoperational.

- CSCee85488

  Symptoms: OSPF does not install routes for which the next hop router is on a broadcast interface in a VRF. A network LSA does not exist for the link, so when the router and the next hop router calculate the SPF tree, they do not detect a path between them.

  Conditions: This symptom is observed when following conditions occur:

  - The OSPF process occurs in a VRF.
  - The router is the designated router (DR) on a broadcast interface.
  - There is only one other OSPF router on the other side of the broadcast interface.
  - The router has a full adjacency with its neighbor.
  - The neighbor's interface goes down, and while it is down the network LSA is deleted (because there are no other neighbors on the link).

  - The neighbor's interface comes back up before it maxages the network LSA from its database, so the network LSA that the router had previously originated for the link is returned to the router.
  - The router flushes the old network LSA but does not originate a new one.

  Workaround: There is no workaround. Clear the symptom by flapping the interface on the DR.

- CSCee89438

  Symptoms: An MSDP enabled RP does not build an (S,G) state from its SA cache when it should do so. Depending on the topology and if an SPT threshold is configured as infinite, this situation may result in a multicast forwarding interruption of up to 2 minutes.

  Conditions: This symptom is observed when the RP for a group fails and an incoming (*,G) join message is received.

  MSDP should create an (S,G) state from its SA cache. However, this is done before the (*,G) olist is populated; because of the (*,G) NULL olist, MSDP does not install an (S,G) state.

  Workaround: Enter the **clear ip mroute *** command on all first-hop routers to the source to enable the FHR to register immediately when the next packet creates an (S,G) state.

- CSCee94787

  Symptoms: A slave RP that functions in SSO mode may reload unexpectedly when IS-IS is implemented on an MPLS LC-ATM interface.

  Conditions: This symptom is observed when a dual-RP router is configured for IS-IS on an MPLS LC-ATM interface for the first time. Once the slave RP has reloaded, the symptom does not reoccur.

  Workaround: There is no workaround.

- CSCef00037

  Symptoms: EIGRP may generate the following error message and a traceback on the peers of a router:

  ```
  DUAL-3-INTERNAL: IP-EIGRP(0) 401: Internal Error
  ```

  Conditions: This symptom is observed when you perform a switchover on the router.

  Workaround: There is no workaround.

- CSCef00535

  Symptoms: An OSPF router may reload unexpectedly.

  Conditions: This symptom is observed after a neighbor has performed a switchover.

  Workaround: Disable LLS under the OSPF process on the router by entering the **no capability LLS** command or disable OSPF NSF under the OSPF process on the neighbor by entering the **no nsf** command.

- CSCef02601

  Symptoms: After a switchover occurs on a router, traffic loss may occur for some VRF traffic.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(22)S or a later release while the BGP Graceful Restart feature is active with some neighbors of the VPNv4 address family.

  Workaround: There is no workaround.

- CSCef11304

  Symptoms: When performing a snmpwalk on OSPF-MIB that supports the ospfExtLsdbTable, a router can crash. In other instances alignment errors are observed when you enter the **show alignment** command.

  Conditions: These symptoms are observed on a Cisco platform that runs Open Shortest Path First (OSPF) and supports the ospfExtLsdbTable in OSPF-MIB.

  Workaround: There is no workaround.

- CSCef25708

  Symptoms: A router may crash when BGP is configured for an IPv6 address family and you enter the **no ipv6 unicast-routing** command.

  Conditions: This symptom is observed on a Cisco 7200 series that runs an interim release of Cisco IOS Release 12.2(25)S. The symptom may be platform-independent.

  Workaround: Enter the **no router bgp** *as-number* command before you enter the **no ipv6 unicast-routing** command.

- CSCin73487

  Symptoms: A BGP advertise map may permit all prefixes, whether or not the prefix exists as defined in the **non-exist-map** keyword.

  Conditions: This symptom is observed when BGP conditional advertisement is configured with the **advertise-map** and **non-exist-map** keywords.

  Workaround: There is no workaround.

- CSCuk49673

  Symptoms: IPv6 multicast forwarding may stop.

  Conditions: This symptom is observed when the **no ipv6 multicast-routing** and **ipv6 multicast-routing** global configuration commands are entered in quick succession.

  Workaround: Enter the commands with some time in between.

ISO CLNS

- CSCed43873

  Symptoms: You may see the following error message and tracebacks on a platform that runs both IS-IS and MPLS traffic engineering:

  ```
  %CLNS-3-LSPLISTERR: ISIS: LSP list traversal incomplete (ISIS)
  -Traceback= 40FCCCE4 40FCD504 40FB99DC 40FD6284 40FD6648 40FD68E8 40FD6988 40FD69F8
  ```

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

  Workaround: There is no workaround.

- CSCee54672

  Symptoms: The redistribution of routes from L1 into L2 or/and from L2 into L1 may not occur properly, and a learned IS-IS prefix may be missing.

  Conditions: This symptom is observed under the following conditions:

  - There are multiple paths to reach the same prefixes.
  - One source LSP removes a prefix and another LSP adds the same prefix, while both paths between the prefix and the LSPs are of equal cost.

Workaround: Enter the **clear isis *** or the **clear ip route *** command to restore the prefix. However, doing so clears all the routes and recalculates them again, which is a disruptive action.

- CSCin57685

  Symptoms: A Cisco 7200 series may reload unexpectedly while sending Connectionless Network Service (CLNS) packets.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(18)S1.

  Workaround: There is no workaround.

Miscellaneous

- CSCdw01772

  Symptoms: A Cisco router or switch that is configured with distributed Network-Based Application Recognition (dNBAR) may reload unexpectedly because of a software-forced crash.

  Conditions: This symptom is observed under rare circumstances when distributed Cisco Express Forwarding (dCEF) is disabled or reset. The symptom may also occur on routers with unsupported configurations; dNBAR is only supported on a Cisco 7500 series that is configured with a VIP2-50 or a later VIP and on a Catalyst 6000 series switch that is configured with a FlexWAN module.

  Workaround: There is no workaround.

- CSCdw65342

  Symptoms: CyBus error 10 and QA zero link errors may occur some time after a switchover.

  Conditions: This symptom is observed on a Cisco 7500 series when a VIP reads an invalid “bufhdr” pointer and attempt to write it to MEMD.

  Workaround: There is no workaround.

- CSCdz54403

  Symptoms: A Cisco router may crash when IPSec IKE SNMP variables are retrieved, and a bus error and a traceback may be logged.

  Conditions: This symptom is observed when at least one SA is established. The symptom does not always occur, but when you retrieve the IPSec IKE SNMP variables once every 10 minutes, the router eventually crashes after a few hours.

  Workaround: There is no workaround.

- CSCea28333

  Symptoms: A Cisco router may display the following error message and traceback:

  ```
  1d13h: %IPC-2-PRECLOSE: IPC port pre-closure overflow : 0x10025 : 0x5F
  -Traceback= 60366B1C 6035B908 6035BBBC
  ```

  Conditions: This bug occurs between distributed IPC clients in a platform, when one IPC client opens and closes too many ports quickly. The problem is triggered by the device opening and closing the IPC port quickly. The problem was specifically seen with clock sync clients in the chassis.

  Workaround: There is no workaround.

- CSCea31672

  Symptoms: Packets that are sent to the Route Processor (RP) from a VIP are dropped when IP is source-bridged on a FDDI port adaptor.

  Conditions: This symptom is observed on a Cisco 7500 series. Note that IP routing works fine.

  Workaround: There is no workaround.

- CSCea79314

  Symptoms: It may take a long time for an Internet Key Exchange (IKE) tunnel to be set up.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a Virtual Private Network (VPN) acceleration module (VAM) or VAM2 for hardware encryption and that has the **authentication rsa-sig** ISAKMP policy configuration command configured.

  Workaround: Use software encryption.

- CSCeb39331

  Symptoms: A Cisco router drops calls intermittently or prevents some calls from connecting.

  Conditions: This symptom is observed on a Cisco router when Cisco Express Forwarding (CEF) with Real-Time Protocol (RTP) header compression is enabled. This symptom occurs because the header compression packets get out of synchronization. If RTP header compression with process switching is used, CPU utilization goes too high.

  Workaround: There is no workaround.

- CSCeb53438

  Symptoms: When you manually set the value of the *ring-limit* argument in the **tx-ring-limit** *ring-limit* interface configuration command, the value is lost when you reload the router, even though the value is properly saved in the running configuration and in the startup configuration.

  Conditions: This symptom is observed only when you manually set the value of the *ring-limit* argument for an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) and you reload the router.

  Workaround: There is no workaround.

- CSCeb54901

  Symptoms: The Channel Interface Processor (CIP) microcode may fail to load, and error messages similar to the following may appear:

  ```
  %UCODE-3-BADCHKSUM: Bad checksum in slot0:cip218-120.hsma_test_kernel_hw5, found
  0xC620 expected 0x0
  %UCODE-3-RDFAIL: Unable to read ucode file slot0:cip218- 120.hsma_test_kernel_hw5
  from flash
  ```

  Conditions: This symptom is observed on a Cisco 7500.

  Workaround: There is no workaround.

- CSCeb55043

  Symptoms: A secondary Route Switch Processor (RSP) may reload when a service policy is detached from an ATM permanent virtual circuit (PVC).

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with two RSPs in a redundant configuration.

  Workaround: First remove the PVC; then, recreate the PVC without the service policy attached to it.

- CSCeb57543

  Symptoms: A virtual circuit (VC) that controls tag switching may pause indefinitely.

  Conditions: This symptom is observed on a Cisco 7500 series when you repeatedly perform a manual redundancy switchover.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the affected VC is configured.

- CSCeb75824

  Symptoms: A Cisco 7200 series router with a Network Processing Engine (NPE-G1) may pause indefinitely on bootup if there is no Compact Flash Card in the disk2: device slot.

  Conditions: This symptom is observed only with an NPE-G1 on a Cisco 7200 series. It does not affect any other Cisco 7200 series NPE.

  Workaround: Insert a Compact Flash Card into the disk2: device slot and power-cycle the router. The Compact Flash Card does not need to contain any particular files; however, a copy of the desired Cisco IOS image is recommended.

- CSCeb84890

  Symptoms: When performing GTP load-balancing of GGSNs, the Cisco IOS Server Load Balancing feature may read corrupted packet data while parsing the GTP payload.

  Conditions: This symptom is observed on a Cisco 7200 series, and on a Cisco Catalyst 6000 series and Cisco 7600 series that are configured with an MSFC1.

  Workaround: There is no workaround for a Cisco 7200 series. For a Cisco Catalyst 6000 series or Cisco 7600 series, install an MSFC2.

- CSCec07487

  Symptoms: An interface may not transmit traffic because the output may be stuck. When this symptom occurs, the console of the Route Switch Processor 4 (RSP4) may display the following error messages:

  ```
  %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se1/0/2:15, TEI0 changed to down
  %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se1/0/1:15, TEI0 changed to down
  %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se1/0/3:15, TEI0 changed to down
  %RSP-3-RESTART: interface Serial1/0/0:15, not transmitting
  Output Stuck on Serial1/0/0:15
  %RSP-3-RESTART: interface Serial1/0/1:15, output frozen
  %RSP-3-RESTART: interface Serial1/0/2:15, not transmitting
  %RSP-3-RESTART: cbus complex
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.1(19)E1 when the **compress stac caim** interface configuration command is configured on the interface. The symptom may also occur in other releases.

  Workaround: Remove the **compress stac caim** interface configuration command from the interface.

- CSCec08434

  Symptoms: The Cisco 7200 series boothelper image for Cisco IOS Release 12.2(14)S2 may reload unexpectedly, and the router may return to the ROM monitor (ROMmon) mode.

  Conditions: This symptom is observed when you install a 2-port Token Ring Inter-Switch Link 100BASE-TX port adapter (PA-2FEISL-TX) or a 1-port ATM Enhanced OC-3 Packet-over-SONET (POS) port adapter in a Cisco 7200 series Network Processing Engine G-1 (NPE-G1) and you reload, reset, or power up the router with the boothelper image.

Workaround: Remove the PA-2FEISL-TX or 1-port ATM Enhanced OC-3 POS port adapter when you reload, reset, or power up the router with the boothelper image. Once the router has booted up, you can reinstall the port adapters.

- CSCec08973

  Symptoms: A 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may report huge numbers of degraded minutes on an E1 controller. For example, after 15 minutes of operation since startup, 35,000,000 degraded minutes may be reported and these values may increase every second. Code violations may also be reported.

  Conditions: These symptoms are observed on a Cisco router in which a PA-MC-STM-1 is installed.

  Workaround: There is no workaround. However, the traffic is not affected, and the symptom is of a cosmetic nature.

- CSCec14039

  Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

  ```
  Last reset from watchdog reset
  ```

  Conditions: This symptom is observed only on a Cisco 7200 series that is configured with an NPE-G1 Network Processing Engine and on a Cisco 7301.

  Workaround: There is no workaround.

- CSCec16666

  Symptoms: Two channel group interfaces on a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may receive the same ifIndex. This can be observed in the following command output:

  ```
  show snmp mib ifmib ifindex serial X/X/X:0 Interface = SerialX/X/X:0, Ifindex = 496
  show snmp mib ifmib ifindex serial Y/Y/Y:0 Interface = SerialY/Y/Y:0, Ifindex = 496
  ```

  Conditions: This symptom is observed when some of the E1 interfaces are deleted and recreated.

  Workaround: Do not delete any of the E1 interfaces.

- CSCec22970

  Symptoms: When the **negotiation auto** command is enabled, the Gigabit Ethernet port link is up and down between the Cisco 7301 router and the network processing engine-G1 (NPE-G1).

  Conditions: This symptom is observed on a Cisco 7301 router but is platform independent.

  Workaround: Enter the **no negotiation auto** command on the interface of each router.

- CSCec31781

  Symptoms: When you enter the **redundancy force-switchover** privileged EXEC command on a Cisco 7500 series, a Versatile Interface Processor (VIP) may reload when the router returns to the Stateful Switchover (SSO) mode.

  Conditions: This symptom is observed on a Cisco 7500 series that runs the rsp-pv-mz image of Cisco IOS Release 12.0(25)S1 but may also occur in other releases.

  Workaround: There is no workaround.

- CSCec36978

  Symptoms: A Cisco 7500 series that is configured with a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may reload unexpectedly.

  Conditions: This symptom is observed when the following steps occur in sequence:

  1. You enter the **shutdown** controller configuration command on the controller of the PA-MC-STM-1.
  2. You enter the **write memory** EXEC command.
  3. You reload the router.
  4. You enter the **no shutdown** controller configuration command on the controller of the PA-MC-STM-1.

  Workaround: There is no workaround.

- CSCec37042

  Symptom: A Cisco 7301 or Cisco 7401ASR may boot up in the boot image rather than in the Cisco IOS image.

  Conditions: This symptom is observed in the following configurations:

  - On a Cisco 7301 that is configured with a Network Processing Engine G1 (NPE-G1) and that runs a c7301-boot-mz image.
  - On a Cisco 7401ASR that is configured with a Cisco Network Service Engine (NSE) and that runs a c7400-kboot-mz image.

  The symptom is observed in Cisco IOS Release 12.2(16)B2 but may also occur in Release 12.2 S, 12.3, 12.3 B, or 12.3 T.

  Workaround: Enable the router to boot the image from a disk by entering the **boot system** global configuration command.

- CSCec37143

  Symptoms: Operation, Administration, and Maintenance (OAM) cells may be dropped from an ATM interface.

  Conditions: This symptom is observed when an input service policy is applied.

  Workaround: Disable OAM.

  Alternate Workaround: Remove the service policy.

- CSCec37930

  Symptoms: The standby Route Switch Processor (RSP) for a Cisco 7500 series may reload unexpectedly.

  Conditions: This symptom is observed on an RSP for a Cisco 7500 series that has a LAN Extender (LEX) interface configured, and that has the Stateful Switchover (SSO) feature enabled.

  Workaround: There is no workaround.

- CSCec49218

  Symptoms: A Cisco router may no longer offer the option to save the configuration.

  Conditions: This symptom is observed on a Cisco router that is configured with redundant Route Processors (RPs) after two high availability (HA) switchovers have occurred and you have initiated the switchovers by entering the **redundancy force-switchover** privileged EXEC command.

When you have completed a configuration on the router, the router should offer the option to save the configuration before you initiate a switchover or reload of the router.

Workaround: Enter the **write memory** EXEC command to save the configuration before you initiate a switchover.

- CSCec61738

  Symptoms: A Cisco 7500 series that functions as a provider edge (PE) router may fail to receive an Internet Control Message Protocol (ICMP) echo message on a Multilink PPP (MLP) ingress interface.

  Conditions: This symptom is observed on a Cisco 7500 series when Virtual Private Network (VPN) routing/forwarding (VRF) is configured on the MLP interface.

  Workaround: There is no workaround.

- CSCec63011

  Symptoms: A router may reload because of an NVRAM corruption.

  Conditions: This symptom is observed when NVRAM is accessed simultaneously by two processes, when one the processes has a file open, and when the second process attempts to open a nonexistent file. The error handling for the second process clears the global NVRAM pointer that is used by the first process. This situation is more likely to occur in a configuration with redundant Route Processors (RPs) but may also occur in a configuration with a single RP when two terminal windows are open.

  Workaround: There is no workaround.

- CSCec67980

  Symptoms: The standby Route Processor may reload shortly after if boots up if the **snmp-server packetsize** *byte-count* global configuration command is included in the configuration.

  Conditions: This symptom is observed on a standby RP if the packet size of the Simple Network Management Protocol (SNMP) server is included in the configuration of the router.

  Workaround: Do not specify the packet size of the SNMP server in the configuration of the router.

- CSCec70301

  Symptoms: The output queue of an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) may be stuck, even though the controller is up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S, 12.1 E, or 12.2 S after you have performed an online insertion and removal (OIR) of the PA-MC-8TE1+.

  Workaround: Reload the router.

- CSCec75189

  Symptoms: Two interfaces may have the same Cisco Express Forwarding (CEF) interface description block (IDB) when the following configuration sequence occurs:

  1. You create a subinterface.
  2. You delete this subinterface.
  3. You create another subinterface.
  4. You recreate the first subinterface.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S or Release 12.2 S.

  Workaround: There is no workaround. Reload the router to clear the condition.

- CSCed00033

  Symptoms: When an ATM PVC bounces, it fails to come back up and remains in the DOWN/UNVERIFIED state.

  Conditions: This symptom occurs when an ATM LC is connected to an ATM switch, when the ATM PVC is managed by OAM, and when the frequency of the OAM F5 loopback cells is set to 0 via the **oam-pvc manage 0** command.

  Workaround: Reactivate the PVC by entering the **shutdown** command followed by the **no shutdown** command on the PVC.

  Alternate Workaround: Disable OAM management.

- CSCed07673

  Symptoms: The copy function from TFTP into the running configuration file may fail even though it appears as though the copy function has succeeded. An error message similar to the following may be displayed:

  ```
  Simultaneous configs not allowed:locked from vty0 (10.1.11.111)
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that has a single Route Switch Processor (RSP) when the following conditions are present:

  - The **service multiple-config-sessions** global configuration command is enabled on the router.
  - There is one vty session that is in configuration mode.
  - You enter the **copy tftp running-config** privileged EXEC command from another vty session.

  Workaround: There is no workaround.

- CSCed09248

  Symptoms: A Cisco 7200 series that is running IPSec may crash with tracebacks pointing to a managed timer.

  Conditions: This symptom is observed when a large number of IPSec tunnels are rekeyed at the same time.

  Workaround: There is no workaround. Increasing the IPSec SA lifetime may help reduce the stress on the router and therefore may avoid the race condition.

- CSCed12659

  Symptoms: A Label Switch Controller (LSC) may reload unexpectedly when there is an invalid address for the “refCount.”

  Conditions: This symptom is observed on a Cisco 7200 series and a Cisco MGX 8850 Route Processor Module (RPM-PR) that function as an LSC.

  Workaround: There is no workaround.

- CSCed20839

  Symptoms: After an interface flaps or when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface that is configured for Hot Standby Router Protocol (HSRP), a virtual HSRP address may not respond to pings.

  Conditions: This symptom is observed on a Cisco router that is configured with a 2-port Fast Ethernet Inter-Switch Link (ISL) port adapter (PA-2FEISL) that has at least one Fast Ethernet interface configured for HSRP.

The symptom occurs because the Fast Ethernet interface that is configured for HSRP is not switched to promiscuous mode when the HSRP group becomes active, preventing packets that are addressed to the HSRP virtual MAC address from being received by the interface. The output of the **show controllers fastethernet** user EXEC or privileged EXEC command displays whether the promiscuous mode is enabled or disabled.

Reboot the router to restore the router to proper operation.

Workaround: To prevent the symptom from occurring, enter the **standby use-bia** interface configuration command on the Fast Ethernet interface that is configured for HSRP.

Further Problem Description: This caveat only effects Fast Ethernet port adapters and network modules that use the AMDP2 chipset (for example, the PA-2FEISL). When you use such a port adapter or network module with HSRP configured and the interface goes down, HSRP does no longer function when the interface comes back up.

- CSCed23828

  Symptoms: L2 fragmentation does not happen for packets greater than the network Maximum Transmission Unit (MTU). Packets are dropped.

  Conditions: This symptom occurs when distributed Cisco Express Forwarding (dCEF) is enabled on an RSP.

  Workaround: Either turn dCEF off or configure the MTU to be equal to the network MTU on the customer edge (CE) routers.

- CSCed32216

  Symptoms: On a Cisco 7500 series, the standby Route Switch Processor (RSP) may reload unexpectedly during a configuration session, and the following messages may be logged on the standby RSP:

  ```
  %HA-3-SYNC_ERROR: Parser no match. %HA-5-SYNC_RETRY: Reloading standby and retrying
  sync operation (retry 1).
  ```

  Conditions: This symptom is observed when the Route Processor Redundancy (RPR), RPR Plus (RPR+), or Stateful Switchover (SSO) redundancy mode is configured on the router and when you perform the following steps:

  1. Configure a multipoint interface.
  2. Delete the interface.
  3. Recreate the interface and configure it.

  Workaround: There is no workaround.

- CSCed34880

  Symptoms: After a Stateful Switchover (SSO) has occurred, the new standby Route Processor (RP) may become stuck in the standby COLD-BULK state and may not progress to the standby HOT state.

  When this situation occurs, all of the following additional symptoms are present:

  – The output of the **show redundancy states** privileged EXEC command shows the message "Reason: Progression in progress."

  – The output of the **show cef linecard** user EXEC or privileged EXEC command shows that the line cards or Versatile Interface Processors (VIPs) are up but also that there is an inactive Virtual Private Network (VPN) routing/forwarding (VRF) table present on the line cards.

  – The output of the **show cef table internal** privileged EXEC command shows that a table is marked as incomplete.

Conditions: This symptom is observed on a Cisco router that functions in an inter-autonomous system (Inter-AS) topology when an incomplete Cisco Express Forwarding (CEF) VRF table is still present as a leftover from a deleted VRF instance and when you enter the **redundancy force-switchover** privileged EXEC command.

Workaround: Remove the incomplete CEF VRF table. If this is not possible, reload the router.

- CSCed35964

  Symptoms: Interoperating problems may occur with a particular third-party vendor 48 MB flash card, and a router may not be able to read the flash card with "bad majic" and "-13 open file" error messages.

  Conditions: This symptom is observed in the following two scenarios:

  - Scenario 1: If the flash card is formatted on one router and then inserted in another router, the boot image and Cisco IOS image can be read from the flash card until you reload the router. After the router is reloaded, "bad majic" and "-13 open file" error messages occur.
  - Scenario 2: When you remove the first large file from the flash card (irrespective of its position on the flash card and irrespective of whether or not the file is a Cisco IOS file) and you reload the router, "bad majic" and "- 13 open file" error messages occur, and the router may enter a continuous loop. The symptom occurs with the removal of a file that is 12 MB or 14 MB but does not occur with the removal of a file of 4 MB.

  Workaround: There is no workaround.

- CSCed37676

  Symptoms: Spurious memory access errors may occur on a Cisco 7200 series.

  Conditions: The symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2 S when you configure or deconfigure Multiprotocol Label Switching (MPLS) traffic engineering (TE) options such as MPLS path options.

  Workaround: There is no workaround.

- CSCed40933

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory, which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml.

- CSCed45698

  Symptoms: Unused ports on a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may flap even when they are not processing any traffic.

  Conditions: This symptom is observed when there is congestion on used ports of the PA-MC-STM-1 and when a committed access rate (CAR) is configured on these used ports.

  Workaround: There is no workaround.

- CSCed45942

  Symptoms: A router with a configuration size that is larger than the NVRAM size reloads because of a bus error and stack overflow or stack corruption when you enter the **show config** command simultaneously with the **write terminal** or **show running-config** command.

  Conditions: This symptom is observed when the **service compress-config** command or **boot config** command is enabled.

Workaround: Do not enter the above-mentioned commands simultaneously, reduce the size of the configuration, or increase the size of the NVRAM.

Further Problem Description: This problem was introduced in Cisco IOS Release 12.1(8a)E1, so most Cisco IOS 12.1 E releases are exposed to this problem. The problem may also occur in Release 12.2 S.

- CSCed46293

  Symptoms: The outgoing label information in the output of the **show mpls forwarding-table** privileged EXEC command may be incorrect for a Versatile Interface Processor (VIP).

  Conditions: The symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(22)S and that is configured for Any Transport over MPLS (AToM). The symptom is specific to the AToM configuration.

  Workaround: Use the outgoing label information in the output of the **show mpls forwarding-table** privileged EXEC command for the Route Switch Processor (RSP).

- CSCed46620

  Symptoms: When Reflexive access control entries (ACEs) are added, CPU utilization may increase to and remain at 100 percent until all the new Reflexive ACEs are formed. The rate at which NetFlow entries are created may become very slow.

  Conditions: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.2 S or Release 12.2(17b)SXA when the global reflexive timeout is reduced while new dynamic ACEs are added to a Reflexive access control list (ACL).

  Workaround: There is no workaround.

- CSCed46797

  Symptoms: A Versatile Interface Processor (VIP) that is installed in a Route Switch Processor (RSP) may drop packets from a Multiprotocol Label Switching (MPLS) forwarding entry for prefixes that are learned via Border Gateway Protocol (BGP) IPv4 routes with MPLS labels.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for high availability (HA) in the period after a HA switchover until BGP reinstalls the prefixes in the routing table of the newly active Route Processor (RP).

  Workaround: There is no workaround.

- CSCed48260

  Symptoms: An automated test for a traceroute check between carrier supporting carrier customer edge (CSC-CE) routers may fail because a hop router that corresponds to a carrier supporting carrier provider edge (CSC-PE) router may be missing from the traceroute output.

  Conditions: This symptom is observed in a carrier supporting carrier (CSC) topology when a traceroute check is performed for a traceroute to the loopback interface address of a remote CSC-CE router.

  Workaround: There is no workaround.

- CSCed54262

  Symptoms: Memory allocation (MALLOC) failures may occur on a VIP, port adapter, or line card.

  Conditions: This symptom is observed on a Cisco router that has a scaled AToM configuration.

  Workaround: There is no workaround.

- CSCed55201

  Symptoms: A serial interface may stop transmitting, and the following error message may be generated:

  ```
  %RSP-3-RESTART: interface Serial1/0/2, not transmitting -Traceback= 403D8D88 403E2830
  4036B72C 4036B718
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an 8-port serial V.35 port adapter (PA-8T-V35).

  Workaround for HDLC interfaces: Disable CDP, the passive interface, and the outbound IP ACL.

  Workaround for Frame Relay interfaces: Disable CDP, the passive interface, the outbound IP ACL, and LMI.

- CSCed56025

  Symptoms: A VIP, port adapter, or line card may reset.

  Conditions: This symptom is observed on a router that has a scaled AToM configuration.

  Workaround: There is no workaround.

- CSCed57551

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series, traffic may fail after a short period of time (5 to 10 minutes).

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.2(22)S and that is configured for SSO/Nonstop Forwarding (NSF).

  Workaround: There is no workaround.

- CSCed57659

  Symptoms: A memory leak may occur in a Multiprotocol Label Switching (MPLS) Virtual Private Network version 4 (VPNv4) Interautonomous System (InterAS) network or in an Any Transport over MPLS (AToM) network.

  Conditions: This symptom is observed on a Cisco 7500 series when memory is not freed when an MPLS VPNv4 forwarding entry flaps or when an MPLS forwarding entry that faces the AToM core flaps. The Route Processor (RP) looses 108 bytes per MPLS VPNv4 or AToM forwarding entry per path on each flap. The symptom may not be platform specific.

  The MPLS VPNv4 forwarding entries are created on an Autonomous System Boundary Router (ASBR) that runs external Border Gateway Protocol (eBGP) VPNv4 for Internet Authentication Server (IAS) deployment. In an MPLS VPNv4 InterAS network, the memory is lost when Border Gateway Protocol (BGP) sessions on the ASBR flap. In an AToM network, the memory is lost when Label Distribution Protocol (LDP) sessions flap.

  Workaround: There is no workaround. The symptom does not occur in a non-VPNv4 IAS environment, or with non-ASBR routers, or with non-AToM provider edge (PE) routers.

- CSCed63357

  This caveat consists, of six separate symptoms, conditions, and workaround, of which the first three apply to all Cisco IOS releases and the last three apply only to Cisco IOS Release 12.3 T:

  1) Symptoms: There are three symptoms:

  - There may be a inconsistent or duplicate display of files between the **show disk***slot-number* and **dir disk***slot-number* commands.
  - When a file is deleted from the CLI, the file may be deleted but a “No such file” message may be printed.

- One cluster may leak. Entering the **fsck** command truncates the original file and creates an orphan file for the leaked cluster.

Conditions: This symptom is observed when an application creates or opens a file without the "O_TRUNC:" mode, as in the following example:

```
show version | append disk#:

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#vtp file new
Setting device to store VLAN database at filename new.
Router(config)#^Z
```

Workaround: There is no workaround.

2) Symptoms: The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information (such as inconsistent file sizes) when multiple images are copied.

Conditions: This symptom is observed when you make two copies of the image file to the disk by using two vtys and by entering the **dir disk***slot-number* command at the same time.

Workaround: Do not enter the **show disk***slot-number* and **dir disk***slot-number* commands when multiple images are being copied.

3) Symptoms: There are two symptoms:

- The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information.
- Entering the **fsck** command may delete or truncate the valid files or create an orphan file for an unused cluster.

Conditions: This symptom is observed when you rename a directory that consists of many subdirectories or files.

Workaround: Reload the router.

4) Symptoms: There are two symptoms:

- There may be a duplicate entry for each file when you enter the **show disk***slot-number* command.
- An snmpGet on a ciscoFlashFileSize object may enter a loop.

Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3 T after the router boots up.

Workaround: There is no workaround.

5) Symptoms: There are two symptoms:

- The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information.
- Entering the **fsck** command may delete or truncate the original file.

Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3 T when an application or a CLI command overwrites a file on the disk.

Workaround: Reload the router.

6) Symptoms: A router that runs Cisco IOS Release 12.3 T crashes.

Conditions: This symptom is observed when an application creates or opens a file without the "O_TRUNC" mode and attempts to delete the file, as in the following example:

```
show version | append disk0:redirect.out" and issuing
delete disk0:disk0:redirect.out
```

Workaround: Reload the router and delete the file.

- CSCed65778

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial-In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

- CSCed68523

  Symptoms: A LAC sends incorrect connection speed information in the L2TP setup message to the LNS, which in turn gets forwarded to the AR RADIUS server for authentication.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3(6.2)T2. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed69858

  Symptoms: A Cisco platform that runs SSH may crash when the **show ssh** command is entered.

  Conditions: This symptom is observed when a number of SSH session negotiations are in progress.

  Workaround: There is no workaround.

- CSCed70198

  Symptom: The line protocol may go down.

  Conditions: This symptom is observed when Frame Relay fragmentation is enabled on the main interface.

  Workaround: There is no workaround.

- CSCed70205

  Symptoms: On an MLPoATM link, an IP Header Compression (IPHC) configuration mismatch may occur between an RSP and a VIP.

  To verify that the symptom occurs, enter the **show ip rtp header-compression** command on the RP and look at the number of seconds since the statistics were last updated. The output of this command may look as follows:

```
RTP/UDP/IP header compression statistics:
  Interface Virtual-Access8 (compression on, IPHC)
  Distributed fast switched:
  976 seconds since line card sent last stats update
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
```

```
          0 dropped, 0 buffer copies, 0 buffer failures
Sent:     0 total, 0 compressed, 0 status msgs, 0 not predicted
          0 bytes saved, 0 bytes sent
Connect: 16 rx slots, 16 tx slots,
          0 misses, 0 collisions, 0 negative cache hits, 0 free contexts
```

If the statistics are not updated within the last 20 seconds, a configuration mismatch has occurred (that is, the line card is not notified of the IPHC update).

Conditions: This problem may occur when an MLPoATM virtual-access link is configured for IP header compression configured on a virtual-template via RSP.

Workaround: There is no workaround.

- CSCed70725

  Symptom: Traffic shaping does not work when it is configured on a tunnel interface.

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

  Workaround: There is no workaround.

- CSCed70886

  Symptoms: All traffic stops after you perform an OIR of a PA-8B.

  Conditions: This symptom is observed on a Cisco 7200 series that functions in an ISDN leased line configuration.

  Workaround: There is no workaround.

- CSCed71490

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series router, traffic destined for the router may fail for about 10 minutes. This could cause routing protocol traffic to fail and routes to be lost. While the routes are still on the router, traffic will flow through the router with no issues.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.0 S or Release 12.2(22)S and that is configured for SSO/Nonstop Forwarding (NSF) with a POS interface with Frame Relay encapsulation.

  Workaround: There is no workaround.

- CSCed72297

  Symptoms: Multiple SYS-3-CPUHOG error messages may be generated in the LDP process, eventually followed by a watchdog timeout crash:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (422/8),process
  = LDP.
  -Traceback= 6101DFC0 6102546C 61016FE4 6101CE24 6101728C 61017A30 ...

  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = LDP.
  -Traceback= 6085658C 6101DE48 6102546C 61016FE4 6101CE24 6101728C 61017A30
  ```

  After the router has reloaded, the output of the **show version** command indicates “Last reset from watchdog reset.”

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S3 or Release 12.2(22)S and that is configured for MPLS LDP. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed74933

  Symptoms: A Cisco 12000 series may exhibit high CPU utilization in the "Per-Second Job" process.

  Conditions: This symptom is observed on a Cisco 12012 router that has a GRP and that is running Cisco IOS Release 12.0(26)S1 with 255 class maps applied to a 4-port ISE Gigabit Ethernet line card. However, the symptom is release- and platform-independent.

  Workaround: Reduce the number of applied class maps.

- CSCed75925

  Symptoms: After configuration of an MPLS Traffic Engineering Tunnel on a Cisco 7500 series router with DCEF enabled, traffic may still be punted to the Route Processor.

  Conditions: This symptom is observed on a Cisco 7500 series router that is configured for MPLS TE Tunnels and DCEF. This problem is not limited to TE tunnels but affects all tunnels.

  Workaround: There is no workaround.

- CSCed82462

  Symptom: The **show optical interface brief** command may not function.

  Conditions: This symptom is observed on a Cisco ONS 15530.

  Workaround: There is no workaround.

- CSCed87468

  Symptoms: A segV exception may occur and the router may crash.

  Conditions: This symptom is observed on a Cisco router when you enter the following command sequence:

  ```
  config t
  archive
  path A
  no path A
  path B
  ```

  Workaround: There is no workaround.

- CSCed88286

  Symptoms: Layer 3 connectivity may be lost after toggling CEF on a provider edge router.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2 S in an ATM/Ethernet VLAN L2 interworking configuration.

  Workaround: There is no workaround.

- CSCed89134

  Symptoms: Rapid enablement and disablement of MPLS via a global configuration command may stop packet forwarding through a router.

  Conditions: This symptom is observed when a router is forwarding MPLS packets and you enter the **no mpls ip** global configuration command followed by the **mpls ip** global configuration command in rapid succession (within approximately 5 seconds).

  Workaround: Wait at least 30 seconds before reenabling MPLS globally. For example, enter the **no mpls ip** global configuration command, wait at least 30 seconds, and enter the **mpls ip** global configuration command.

  If the router has stopped forwarding because MPLS has been rapidly disabled and enabled, use the workaround above to reenable forwarding.

- CSCed91988

  Symptoms: The "Transmitted packets" column in the output of the **show policy interface** command for a particular interface may not be updated for packets that exit via this interface without being random or tail-dropped by WRED.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2 S and that has WRED configured in an output service policy on an interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed92837

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series, the standby Route Switch Processor (RSP) my hang just before downloading the image. This situation may prevent the router from entering the STANDBY-HOT state and from being capable to perform a switchover until the standby RSP is reset.

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.0 S or 12.2 S and that is configured for SSO/Nonstop Forwarding (NSF).

  Workaround: There is no workaround. After the problem occurs, you can recover the router by either waiting for an IPC timer to expire (the default time is 30 minutes) or by entering the **hw-module sec-cpu reset** command.

- CSCee00661

  Symptoms: Changing any IP access control list (ACL) may cause a walk of all LC-ATM prefixes.

  Conditions: This symptom is observed on a router configured with an LC-ATM Multi-VC when the changed ACL is not related to the Multi-VC.

  Workaround: There is no workaround.

- CSCee05729

  Symptoms: dCEF may be disabled on some VIPs that are installed in a Cisco 7500 series.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for Network-Based Application Recognition (NBAR).

  Workaround: Disable NBAR.

- CSCee09533

  Symptoms: Flapping an interface may cause a router that is configured for L2TPv3 to crash.

  Conditions: This symptom is observed on a Cisco router that has many L2TPv3 sessions and tunnels configured. For example, the symptom occurs with 2000 sessions over 2000 tunnels but also with 4000 sessions over one tunnel.

  Workaround: There is no workaround.

- CSCee19487

  Symptoms: The configuration logger may log changes that were made to the running configuration by one user as if they were made by another user.

  Conditions: This symptom is observed when two users are logged in via the same line and from the same IP address and occur when the very first user logs in, makes some changes to the running configuration, and logs out, and then the second user logs in, makes some changes to the running configuration, and logs out.

  Workaround: There is no workaround.

- CSCee21085

  Symptoms: The packet drop for a VRF can be up to a total of 60 seconds, some packet loss occurs during cutover time, and some more packet loss occurs around a 5-minute interval after the cutover or when the routes are refreshed on the new active RP.

  Conditions: This symptom is observed on a Cisco router with dual RPs when there are large numbers of EBGP peers, BGP routes, and VRF routes.

  Workaround: There is no workaround.

- CSCee24349

  Symptoms: A Cisco 7500 series cannot boot when there are more than 256 different policy maps attached as service policies on the router.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 but may also occur in Release 12.2 S.

  Workaround: Do not use more than 256 service policies.

- CSCee28839

  Symptoms: VPNv4 traffic may drop on a Cisco 7500 series.

  Conditions: This symptom is observed when the **ip cef** command is enabled.

  Workaround: Do not enter the **ip cef** command. Rather, enter the **ip cef distributed** command.

- CSCee29138

  Symptoms: The ciscoMemoryPoolType returns the wrong value for all memory types, except processor.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2 S, 12.3, or 12.3 T.

  Workaround: There is no workaround.

- CSCee30574

  Symptoms: Poor performance occurs because packets are forwarded on the RP instead of by a line card, and a larger than normal packet loss occurs during a switchover to the redundant RP.

  Conditions: These symptoms are observed on a distributed platform that supports redundant RPs such as a Cisco 7500 series that runs Cisco IOS Release 12.2 S or a Cisco Catalyst 6000 series or Cisco 7600 series that run a special release that is based on Release 12.2 S.

  The symptoms occur when the following sequence of events occurs:

  1. You enable IP Distributed CEF by entering the **ip cef distributed** command.
  2. You enter the **no ip routing** command.
  3. You enter the **ip routing** command.
  4. The router is configured and operating properly.
  5. A switchover to the redundant RP occurs.

  Workaround: After IP routing is reenabled (see Step 3, above), reenable IP Distributed CEF by entering the **ip cef distributed** command on the active RP.

- CSCee31618

  Symptoms: Buffer leakage could occur when a high load of traffic is sent to an interface that has a service policy enabled. This could result in ping failures or very long packet delay.

  Conditions: The problem is observed with an MC-T3+ interface that is configured in unchannelized mode, and the traffic consists only of small packets such a 64-byte packets.

  Workaround: Manually configure the **tx-ring-limit** command to lower the number of packets that can be placed on the transmission ring.

- CSCee34107

  Symptoms: APS behavior for the **aps clear** command is inconsistent with the standard behavior.

  Conditions: This symptom is observed on a Cisco ONS 15540 and ONS 15530 when the following conditions occur:

  - Traffic runs from the working link (link A) and you perform a manual switch to the protect link (link B), causing traffic to switch to the link B.
  - You enter the **aps clear** command for the aps-group; link A becomes active, regardless of whether the APS group is configured revertively or nonrevertively.

  When you enter the **aps clear** command for the aps-group, the correct behavior should be: in a revertive configuration, a switch occurs to link A, but in a nonrevertive configuration, no switch occurs and link B remains active.

  Workaround: There is no workaround.

- CSCee34939

  Symptoms: A memory leak is seen in SSHv2.

  Conditions: This symptom is observed when the client closes the connection after a key exchange and before user authentication occurs.

  Workaround: Configure SSH1 by entering the **ip ssh version 1** command.

- CSCee35185

  Symptoms: After reloading a Cisco platform, one of the RPs may reload, or the following error message may be displayed:

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file.
  ```

  Conditions: This symptom may be observed on any Cisco platform that is configured with dual RPs and that supports RPR+.

  Workaround: There is no workaround.

- CSCee35331

  Symptoms: A router may reload if removing the L2TP class is followed by removing the pseudowire class.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.0(28)S when both removals are done in a very short time via an auto test script and when the L2TP sessions are already established. This is a timing related issue.

  Workaround: Wait at least 1 second before you remove the pseudowire class.

- CSCee38324

  Symptoms: A VIP may crash.

  Condition: This symptom is observed on a Cisco 7500 series when QoS is configured on the interface of the VIP and traffic is flowing.

  Workaround: There is no workaround.

- CSCee38942

  Symptoms: EoMPLS tunnels do not have labels assigned to them, preventing a virtual circuit from coming up.

  Conditions: This symptom is observed when multiple (for example, 1200) EoMPLS tunnels are configured. Only on a few tunnels the symptom may not occur.

  Workaround: There is no workaround.

- CSCee39028

  Symptoms: Multicast traffic cannot be forwarded. When MPLS multicast is configured, a tunnel between a CE router and a PE router does not come up.

  Conditions: These symptoms are observed when the **ip igmp join group** command is configured on a loopback interface and when the **ip cef** command is enabled.

  Workaround: Enter the **no ip cef** command.

- CSCee41186

  Symptoms: A Cisco 7500 series that is configured with an RSP and that runs Cisco IOS Release 12.2 S may crash when you enter the **set ip next-hop** *ip-address* command for a route map.

  Conditions: This symptom is observed when the route map is referenced by a local policy while the router is intensively generating packets.

  Workaround: There is no workaround.

- CSCee41544

  Symptoms: If there is sequence number enabled on a PVC and you add a service policy to this PVC, the sequence number configuration is lost.

  Conditions: This symptom is observed when you enable the sequence number configuration and then add a service policy to the same PVC.

  Workaround: After the symptom has occurred, re-add the sequence number configuration to the PVC.

- CSCee43569

  Symptoms: The TE DB on a tunnel headend may become corrupted.

  Conditions: This symptom is observed on a Cisco router that has MPLS configured.

  Workaround: There is no workaround.

- CSCee50294

  Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml.

There are multiple workarounds for this issue:

There are four possible workarounds for this vulnerability:

- Disabling the dhcp service
- Control Plane Policing
- Two versions of Access Control Lists

a. Disabling the DHCP Service

This vulnerability can be mitigated by utilizing the command:

no service dhcp

However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

b. Control Plane Policing Feature

The Control Plane Policy feature may be used to mitigate this vulnerability, as in the following example:

```
access-list 140 deny   udp host 192.168.13.1 any eq bootps
access-list 140 deny   udp any host 192.168.13.1 eq bootps
access-list 140 deny   udp any host 255.255.255.255 eq bootps
access-list 140 permit udp any any eq bootps
class-map match-all bootps-class
  match access-group 140
policy-map control-plane-policy
  class bootps-class
police 8000 1500 1500 conform-action drop exceed-action drop
control-plane
 service-policy input control-plane-policy
```

For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afad4.html.

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

c. Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address 192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
access-list 100 remark permit bootps from the DHCP server
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 remark deny bootps from any to router f1/0
```

```
access-list 100 deny   udp any host 10.89.236.147 eq bootps
access-list 100 remark deny bootps from any to router f0/0
access-list 100 deny   udp any host 192.168.13.2 eq bootps
access-list 100 remark deny bootps from any to router loopback1
access-list 100 deny   udp any host 192.168.61.1 eq bootps
access-list 100 remark permit all other traffic
access-list 100 permit ip any any
```

access-list 100 is applied to f0/0 and f1/0 physical interfaces.

```
interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

An alternate configuration for the interface access-list workaround.

This example would also need to be applied to all physical interfaces, but deny statements for all of the IP addresses configured on the router are not necessary in this approach. In this example, the address 192.168.13.1 represents a legitimate DHCP server.

```
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 permit udp any host 192.168.13.1 eq bootps
access-list 100 permit udp any host 255.255.255.255 eq bootps
access-list 100 deny   udp any any eq bootps

interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

- CSCee52486

  Symptoms: When you enter the **show parser dump** privileged EXEC command, loops and duplicated entries may occur.

  Conditions: This symptom is observed on a Cisco router and is platform-independent.

  Workaround: There is no workaround.

- CSCee55297

  Symptoms: When you suspend and resume the event manager scheduler and an applet tries to register, the registration fails with an error from the operating system.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S or Release 12.2 S.

  Workaround: There is no workaround.

- CSCee56209

  Symptoms: Access control list (ACL) counters may display twice as many matches as there are in reality.

  Conditions: This symptom is observed when ACL counters are used in policies in which class maps are nested. These counts propagate into the accounting output of the **show policy interface** command, creating the impression that twice as many packets have entered the network and are matched on these ACLs as there are in reality.

  Workaround: There is no workaround.

- CSCee58083

  Symptoms: A Cisco router that runs a Cisco IOS interim release for Cisco 12.0(29)S or interim release 12.3(9.3) or 12.3(9.2)T may log the following error message and traceback, and IPC services using large RPC messages/replies may fail:

  ```
  %IPC-SP-5-INVALID: Invalid dest port=0x2220000
  -Traceback= 402F3784 403027CC 403025AC 4030A10C 4030A4F8 4030A7B8 402F7E78 402F8244
  40309478 402F8890 4033A0E8 40344284
  ```

  Conditions: This symptom is observed without any external trigger occurring.

  Workaround: There is no workaround.

- CSCee59383

  Symptoms: The entitySensorMIB does not function.

  Conditions: This symptom is observed on a Cisco ONS 15530 that runs Cisco IOS Release 12.2 S.

  Workaround: There is no workaround.

- CSCee60559

  Symptoms: The **ubr** command cannot be configured with a peak cell relay value on a VP.

  Conditions: This symptom is observed when a VP is configured for cell relay.

  Workaround: There is no workaround.

- CSCee60709

  Symptoms: Xconnect configurations are not displayed in the output of the **show running-config interface atm** *number* command.

  Conditions: This symptom is observed when the interface is configured for port mode cell relay and when the interface has an old style PVC configured. Note that the L2 circuit remains up.

  Workaround: There is no workaround.

- CSCee60711

  Symptoms: Packets that are switched via MPLS over a GRE tunnel may be dropped.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(22)S, that has CEF enabled, and that has distributed CEF disabled.

  Workaround: Do not use CEF. Rather, use distributed CEF.

- CSCee62985

  Symptoms: The verification of a configuration synchronization to a redundant RP may fail.

  Conditions: This symptom is observed on a Cisco router that is configured with redundant RPs and that is configured for ISSU.

  Workaround: There is no workaround.

- CSCee64543

  Symptoms: A Cisco 7304 may crash when you enter the **no ip cef** command.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that runs Cisco IOS Release 12.2 S.

  Workaround: There is no workaround.

- CSCee66206

  Symptoms: When you boot a Cisco 7200 series that is configured with an NPE-300 or NPE-400 and that runs a c7200-js-mz image, the router may crash with a traceback.

  Conditions: This symptom is observed when the c7200-kboot-mz image is the bootloader and when the router runs Cisco IOS interim Release 12.1(22.3)E1. The symptom may also occur in other releases such as 12.0 S, 12.2 S, and 12.3.

  Workaround: There is no workaround.

- CSCee69887

  Symptoms: A dual SRP ring fails to become active completely due to an is-type mismatch. The output of the **show clns neighbors** command indicates that a certain system interface remains in the "Init" state indefinitely, although the output of the **show ip interface brief** command shows that this interface is up.

  Conditions: This symptom is observed when a dual SRP ring is configured on three routers that run Cisco IOS Release 12.2 S.

  Workaround: There is no workaround.

- CSCee70024

  Symptoms: LSP-Ping packets may include a Vendor Enterprise Code TLV Type 5 with a length that is greater than 4 and with Vendor Private Extensions. According to the draft-ietf-mpls-lsp-ping-05.txt IETF draft, the Vendor Enterprise Code TLV Length should always be 4, and the vendor extensions should use a TLV Type that is in the range 64512-65535.

  Conditions: This symptom is observed on a Cisco platform that functions in an MPLS OAM environment.

  Workaround: There is no workaround.

- CSCee71793

  Symptoms: Malformed MPLS echo request packets may cause excessive Route Processor (RP) CPU cycles to be consumed during parsing of malformed TLVs.

  Conditions: This symptom is observed when MPLS echo request packet are decoded and incorrectly parse beyond the packet boundary due to improper bounds checking.

  Workaround: There is no workaround.

- CSCee81787

  Symptoms: A VIP crashes with a "DRQ stalled" error message.

  Conditions: This symptom is observed when a switchover occurs on a Cisco 7500 series.

  Workaround: There is no workaround.

- CSCee84496

  Symptoms: An NPE-G1 may displays an erroneous parity error message.

  Conditions: This symptom is observed on a Cisco 7200 series when the NPE-G1 receives an ECC/bus error.

  Workaround: There is no workaround.

- CSCee86567

  Symptoms: A Versatile Interface Processor (VIP) may reload with the following error messages during a switchover:

  ```
  %DMA-1-DRQ_STALLED: DRQ stalled. Dumping DRQ.
  ```

  Conditions: This symptom is observed a Cisco 7500 series that runs Cisco IOS Release 12.2 S.

  Workaround: There is no workaround.

- CSCee88364

  Symptoms: A **set** command may not have any effect on traffic and packets are not marked.

  Conditions: This symptom is observed when a **set** command is enabled in a policy map that is attached to an interface.

  Workaround: There is no workaround.

- CSCee93931

  Symptoms: EEM Tcl policies that are subscribed to application publish events are not triggered when the publish events occur.

  Conditions: This symptom is observed when two EEM Tcl policies are registered. One of these policies publishes an application event every 20 seconds, the other one is subscribed to the application event.

  Workaround: There is no workaround.

- CSCee96231

  Symptom: A Channel Interface Processor (CIP2) and an xCPA port adapter fail to load their microcode. The microcode bundle is expanding such that the files do not have the prefix. For example, the file cip28-17_kernel_hw4 is _kernel_hw4.

  Conditions: This symptom is observed on a Cisco 7200 series and a Cisco 7500 series. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee13801. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCef00171

  Symptoms: A router that is configured for RTP header compression may crash with a bus error.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(4)T or a later release, or Release 12.2 S.

  Workaround: Disable RTP header compression.

- CSCef06857

  Symptoms: CEF adjacencies corresponding to static ARP entries are not deleted when the corresponding interface is shut down.

  Conditions: This symptom is observed during normal operation.

  Workaround: There is no workaround.

- CSCef28539

  Symptoms: A VIP may crash and may cause cycles of extremely slow processing on the router.

  Conditions: This symptom is observed on a Cisco 7500 series when you configure a route map (specifically the "set vrf" clause) on the RSP. However, the symptom is not platform-specific and could occur on any distributed platform.

  Workaround: There is no workaround.

- CSCef32372

  Symptoms: A ping to a virtual IP address may fail after an HA switchover.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(25)S.

  Workaround: There is no workaround.

- CSCin35946

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

  Symptoms 1: When the Rivest, Shamir, and Adleman (RSA) public key of the peer of Cisco router is manually configured on the router, the router may reload and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions 1: This symptom is observed when you enter the following sequence of commands:

  - **crypto key pubkey-chain rsa** global configuration command
  - **addressed-key** *key-address* public key chain configuration command
  - **key-string** *key-string* public key configuration command

  Workaround 1: Do not configure the RSA public key of a peer statically on the router; rather, use certificates. This workaround may not be acceptable in situations in which a certification authority (CA) server is not available or deployed.

  Symptoms 2: When a Cisco router has saved the RSA public key of any peer in its configuration and is booted, the router may reload and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions 2: This symptom is observed when you have configured the RSA public key of the peer by using the following sequence of commands:

  - **crypto keyring** *keyring-name* global configuration command
  - **rsa-pubkey address** address keyring configuration command
  - **key-string** *key-string* public key configuration command

  Workaround 2: Do not configure the RSA public key of a peer statically on the router; rather, use certificates. This workaround may not be acceptable in situations in which a certification authority (CA) server is not available or deployed.

- CSCin41269

  Symptoms: A controller of an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) may fail to come up after the router has booted up.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-8TE1+. The symptom is platform independent and port adapter dependent.

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

Alternate Workaround: Enter the **clear counters** user EXEC or privileged EXEC command on the affected interface of the PA-MC-8TE1+.

- CSCin44386

  Symptoms: When you attempt to bring up a multilink interface, the interface may flap continuously on one side. When the master link of the Multilink PPP (MLP) bundle interface goes down, traffic may stop flowing through the multilink interface.

  Conditions: These symptoms are observed on a Cisco platform that has nonchannelized serial port adaptors, such as a 4-port enhanced serial port adapter (PA-4T+) and an 8-port serial port adapter (PA-8T), and that is configured for distributed MLP.

  Workaround: There is no workaround.

- CSCin51588

  Symptoms: When you reload the microcode onto an enhanced 8-port multichannel T1/E1 port adapter (PA-MC-8TE1+) while traffic is flowing through the port adapter, the following error message may appear:

  ```
  %RSP-3-RESTART: interface Serial0/0/4:0, not transmitting
  ```

  In most cases, the interfaces of the port adapter recover on their own. In very rare cases, the execution of a Cbus Complex occurs.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: If the interfaces of the port adapter do not recover on their own, execute a Cbus Complex.

- CSCin53040

  Symptoms: A secondary Route Switch Processor (RSP) that is configured with 512 MB of RAM may not recognize the 512 MB of RAM.

  Conditions: This symptom is observed on a Cisco 7500 series that has a primary and a secondary RSP and that runs a Cisco IOS image that has a size larger than 20 MB.

  Workaround: Configure the secondary RSP with 256 MB of RAM.

- CSCin62533

  Symptoms: A Cisco 7200 series router may reload unexpectedly when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a Packet-over-SONET (POS) interface of a 2-port POS port adaptor (PA-POS-2OC3).

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2 S, 12.3, or 12.3 T when the POS interface is processing a heavy traffic load. Note that the symptom does not occur on a 1-port POS port adaptor (PA-POS-OC3).

  Workaround: There is no workaround.

- CSCin74155

  Symptoms: A router that functions under a heavy load with SSHv2 clients may crash if any of the SSH clients are terminated.

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

  - The CPU utilization above 70 percent.
  - There are continuous sweep pings from two far-end routers that have the **debug ip packet** command enabled to create continuous logs for the SSH clients.
  - The **no logging console** command is configured.

  - A connection is made from a couple of SSHv2 clients, you enable the **terminal monitor** command, and you terminate the SSHv2 clients while continuous messages are being generated.
  - The TCP window size is reduced.

  Workaround: Avoid using SSHv2 when the router is very stressed.

- CSCin74730

  Symptoms: An IMA-over-L2TPv3 session may get stuck and may not establish itself on a Cisco 7xxx router.

  Conditions: This symptom is observed on a Cisco 7xxx router when you configure an AToM L2TPv3 VP on an IMA interface that is configured for SCR, PCR, and AAL5 and when you enter the **no shutdown** command on the interface.

  Workaround: There is no workaround.

- CSCin77553

  Symptom: A PA-A3-8T1IMA or PA-A3-8E1IMA port adapter that is installed in a Cisco 7xxx series may display an increasing "rx_no_buffer" counter in the output of the **show controllers atm** privileged EXEC command, and some PVCs that are configured on the port adapter may stop receiving traffic.

  Conditions: This symptom is observed when there is a high-traffic load on the PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the PA-A3-8T1IMA or PA-A3-8E1IMA port adapter, or as an alternate workaround, reset the VIP or FlexWAN.

- CSCuk45205

  Symptoms: When you deconfigure IP version 6 (IPv6) or IPv6 unicast Reverse Path Forwarding (uRPF) on a Cisco router that runs IPv6 Cisco Express Forwarding (CEF), the configuration may not be removed from a Versatile Interface Processor (VIP) or line card, although it will be removed from the Route Switch Processor (RPS) or Route Processor (RP). This situation may cause IPv6 or IPv6 uRPF to continue to be applied to packets that are switched via distributed CEF (dCEF).

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 12000 series only when dCEF is enabled.

  Workaround: There is no workaround.

- CSCuk45567

  Symptoms: When you perform a physical online insertion and removal (OIR) of a Route Switch Processor (RSP), the router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series when Routing Information Protocol next generation (RIPng) for IPv6 is configured.

  Workaround: There is no workaround.

- CSCuk45735

  Symptoms: For all IPv6 tunnel modes (that is, 6to4, auto, Intra-Site Automatic Tunnel Addressing Protocol [ISATAP], or manual) connectivity to endpoint destinations that are reachable via the tunnel may fail, preventing any traffic from being forwarded.

  In addition, when packets that exceed the IPv6 maximum transmission unit (MTU) of the tunnel are forwarded to the tunnel headend router, the headend router may fail to send a "packet too big" Internet Control Message Protocol for IPv6 (ICMPv6) message to the source address of the packet.

Conditions: These symptoms are observed on a Cisco router only when Cisco Express Forwarding version 6 (CEFv6) is enabled.

Workaround: Disable CEFv6 on the tunnel endpoint routers.

- CSCuk48092

  Symptoms: External Data Representation (XDR) messages may continue to be sent to a Versatile Interface Processor (VIP) that has been disabled.

  Conditions: This symptom is observed on a Cisco 7500 series that has distributed Cisco Express Forwarding (dCEF) enabled.

  Workaround: There is no workaround.

- CSCuk48398

  Symptoms: Traffic may not be able to pass through a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel between two provider edge (PE) routers.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router in an IPv4 Virtual Private Network (VPN) MPLS environment or as a PE router in an IPv6 VPN MPLS environment (also referred to as a 6PE router).

  Workaround: Create a Tag Distribution Protocol (TDP)/Label Distribution Protocol (LDP) session between the two PE routers by entering the **interface tunnel** *number* global configuration command followed by the **mpls ip** global configuration command on the PE routers.

- CSCuk49694

  Symptoms: When a BGP 6PE peer router send an update with a different label from the previously advertised label, the 6PE router does not update the BGP table nor the forwarding path with the new label.

  Conditions: This symptom is observed in a "1-2-3 cascade" with three 6PE routers when the connection between the second and the third 6PE router goes down long enough for the BGP session between these routers to go down and when the BGP sessions comes up again.

  Workaround: Enter the **clear bgp ipv6** command to clear the old labels.

- CSCuk50878

  Symptoms: After a number of WCCP "cache lost" and "cache found" events have occurred on a Cisco router, spurious memory accesses may occur, and then the addition and deletion of WCCP services may fail. When this situation occurs, the output of the **show ip wccp** *service-number* command does not show the WCCP service, even though the WCCP service does show in the output of the **show ip wccp** command.

  Conditions: This symptom is observed only on Cisco IOS images that contain the fix for CSCec55429 and only with dynamic services (not with web cache service) when all the caches in a service group are lost and then reacquired a number of times. Such a situation may occur by services being manually disabled and reenabled on a cache or by a heavy traffic load between the router and the cache, causing WCCP protocol messages to be dropped.

  Once the symptom has occurred, you must stop all WCCP services on the router, and then restart the WCCP services.

  Workaround: There is no workaround.

- CSCuk51476

  Symptoms: The following error message and traceback may be reported when distributed CEF is disabled:

  ```
  %SYS-2-INTSCHED: 'idle' at level 2
  -Process= "Exec", ipl= 2, pid= 3
  -Traceback= 404C5E88 404AC1C0 406929A0 418C6B0C 418C6BFC 418C6E48 418C6F68 40855440
  4085546C 4077659C 40777458 418C6E7C 418C6F68 40855440 4085546C 4077659C
  ```

  Conditions: This symptom is observed when more than one instance of IP header compression is configured on a Frame Relay interface on a Cisco 7500 series that runs Cisco IOS Release 12.3(4)T, or a later 12.3 T release, or Release 12.2 S.

  Workaround: There is no workaround.

- CSCuk51722

  Symptoms: When a 6PE router learns a prefix from a CE router, the 6PE router does not properly install this prefix in the MPLS forwarding table, causing traffic to be dropped. The prefix shows as “Paths Unkn” in the MPLS forwarding table.

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

  Workaround: There is no workaround. To resume traffic to the prefix, send a ping from the 6PE router to the prefix. However, after traffic has resumed, the prefix still shows as “Paths Unkn” in the MPLS forwarding table.

Wide-Area Networking

- CSCec32738

  Symptoms: When a PPP connection comes up, an IP route should be added to the routing table, but this does not occur. Note that even though there is no entry in the routing table, packets are forwarded on the correct route based on their cached Forwarding Information Base (FIB) headers.

  Conditions: This symptom is observed on a Cisco router that functions as a standby router in a high availability (HA) configuration.

  Workaround: There is no workaround.

- CSCed60338

  Symptoms: The line protocol on serial or POS interfaces with HDLC may become disabled for a few seconds.

  Conditions: This symptom is observed after a switchover to a redundant RP on a Cisco 7500 series that is configured for SSO and that has a large number (about 2000) of dot1q interfaces defined.

  Workaround: Increase the HDLC keepalive time or disable keepalives. Replacing HDLC with PPP is another workaround.

- CSCee53018

  Symptoms: When you enter the **show frame-relay lmi** command on a router, the router may crash, or alignment errors may occur.

  Conditions: This symptom is observed after you first have deleted an MFR interface on the router.

  Workaround: There is no workaround.

- CSCee65997

  Symptoms: A POS (PA-POSSW-SM) interface on a Cisco 7500 series that is configured for MPLS and that functions as a PE router may stop transmitting traffic.

  Conditions: This symptom is observed when either a 3GE-GBIC-SC= or a 4GE-SFP-LC= GE interface is flapped on a connected Cisco 12000 series that is configured for MPLS and that functions as a P router. Note that the interface recovers after approximately 60 seconds.

  Workaround: There is no workaround.

- CSCee70960

  Symptoms: The idle timer does not work properly and is not reset for a Frame Relay (FR) SVC.

  Conditions: This symptom is observed for transit packets that are CEF-switched and forwarded on a FR SVC.

  Workaround: Set a very high timeout value and send periodic pings on the output SVC circuit to keep the circuit alive.

- CSCuk51427

  Symptoms: V6 Frame Relay maps do not work.

  Conditions: This symptom is observed when CEF is enabled.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(22)S2

Cisco IOS Release 12.2(22)S2 is a rebuild release for Cisco IOS Release 12.2(22)S, which supports only the Cisco ONS 15530 and Cisco ONS 15540, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(22)S2 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCee58479

  Symptoms: When you configure an interface of a PA-MC-8TE1 on a Cisco 7200 series, the router to which the interface of the PA-MC-8TE1 is connected at the other end may crash.

  Conditions: This symptom is observed when the interface of the PA-MC-8TE1 functions in channelization mode and when CDP is enabled.

  Workaround: Disable CDP globally by entering the **no cdp run** global configuration command or by entering the **no cdp enable** interface configuration command on the interface of the router to which the PA-MC-8TE1 interface is connected at the other end.

IP Routing Protocols

- CSCee40207

  Symptoms: The BGP Open processes may hold more and more memory, may cause a memory leak, may finally run out of memory, and may cause a Malloc Failure error.

  Conditions: This symptom is observed when there are BGP neighbors stuck in the active state (that is, a BGP neighbor is configured but the peer address is not reachable) and when some NSF/SSO RP switchovers occur and the standby becomes active.

Workaround: Shut down the neighbors that are not used.

Further Problem Description: When the memory leak occurs, 1 Kb of memory leaks every two minutes for each BGP neighbor that is not up.

Miscellaneous

- CSCed24626

  Symptoms: A VoIP connection trunk that is configured between two voice gateways over an IP link with RTP header-compression (cRTP) enabled may flap periodically. Messages similar to the following may appear:

  ```
  %HTSP-5-UPDOWN: Trunk port(channel) [2/0:0(1)] is up
  %HTSP-5-UPDOWN: Trunk port(channel) [2/0:0(1)] is down
  %HTSP-5-UPDOWN: Trunk port(channel) [2/0:0(1)] is up
  %HTSP-5-UPDOWN: Trunk port(channel) [2/0:0(1)] is down
  ```

  Conditions: This symptom is observed when two Cisco IOS voice gateways function in connection trunk mode, when an IP link between the two gateways is configured for cRTP, and when on either side of this IP link the Cisco IOS routers run Cisco IOS Release 12.3 T, such as Release 12.3(2)T or Release 12.3(4)T. However, the symptom could also occur in other releases.

  Workaround: Enter the **ip rtp coalesce** hidden global configuration command on both Cisco IOS routers to stabilize the connection trunk. Note that doing so may increase the CPU utilization. If the implementation of this workaround does not stabilize the trunk, unconfigure cRTP over the affected IP link.

- CSCed45942

  Symptoms: A router with a configuration size that is larger than the NVRAM size reloads because of a bus error and stack overflow or stack corruption when you enter the **show config** command simultaneously with the **write terminal** or **show running-config** command.

  Conditions: This symptom is observed when the **service compress-config** command or **boot config** command is enabled.

  Workaround: Do not enter the above-mentioned commands simultaneously, reduce the size of the configuration, or increase the size of the NVRAM.

  Further Problem Description: This problem was introduced in Cisco IOS Release 12.1(8a)E1, so most Cisco IOS 12.1 E releases are exposed to this problem. The problem may also occur in Release 12.2 S.

- CSCee01637

  Symptoms: A software-forced reload occurs when you remove the header-compression configuration from an interface.

  Conditions: This symptom is observed when the following conditions are present on the interface:

  - The interface is in process-switching mode.
  - Traffic is being sent from the interface.

  Workaround: Shut down the interface during the reconfiguration.

- CSCee12235

  Symptoms: A Cisco platform reloads because of a watchdog timer expiration.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(20)S2 or Release 12.3 under the following conditions:

  – A service policy (“A”) is attached to an ATM PVC.
  – Policy-map “A” is renamed to “B”.
  – Service policy “B” is attached to the ATM PVC.

  Workaround: First detach the service policy from the PVC, then rename it and attach it again.

- CSCee50294

  Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml.

  There are multiple workarounds for this issue:

  There are four possible workarounds for this vulnerability:

  – Disabling the dhcp service
  – Control Plane Policing
  – Two versions of Access Control Lists

  a. Disabling the DHCP Service

     This vulnerability can be mitigated by utilizing the command:

     no service dhcp

     However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

  b. Control Plane Policing Feature

     The Control Plane Policy feature may be used to mitigate this vulnerability, as in the following example:

```
access-list 140 deny   udp host 192.168.13.1 any eq bootps
access-list 140 deny   udp any host 192.168.13.1 eq bootps
access-list 140 deny   udp any host 255.255.255.255 eq bootps
access-list 140 permit udp any any eq bootps
class-map match-all bootps-class
  match access-group 140
policy-map control-plane-policy
  class bootps-class
police 8000 1500 1500 conform-action drop exceed-action drop
control-plane
 service-policy input control-plane-policy
```

     For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afad4.html.

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

c. Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address 192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
access-list 100 remark permit bootps from the DHCP server
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 remark deny bootps from any to router f1/0
access-list 100 deny   udp any host 10.89.236.147 eq bootps
access-list 100 remark deny bootps from any to router f0/0
access-list 100 deny   udp any host 192.168.13.2 eq bootps
access-list 100 remark deny bootps from any to router loopback1
access-list 100 deny   udp any host 192.168.61.1 eq bootps
access-list 100 remark permit all other traffic
access-list 100 permit ip any any
```

access-list 100 is applied to f0/0 and f1/0 physical interfaces.

```
interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

An alternate configuration for the interface access-list workaround.

This example would also need to be applied to all physical interfaces, but deny statements for all of the IP addresses configured on the router are not necessary in this approach. In this example, the address 192.168.13.1 represents a legitimate DHCP server.

```
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 permit udp any host 192.168.13.1 eq bootps
access-list 100 permit udp any host 255.255.255.255 eq bootps
access-list 100 deny   udp any any eq bootps


interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
```

```
ip access-group 100 in
ip helper-address 192.168.13.1
```

- CSCin79420

  This caveat consists of two symptoms, two conditions, and two workarounds in the following configuration:

  A Cisco Catalyst 6000 series connects via a Gigabit Ethernet (GE) interface and a Y cable to a Cisco ONS 15540 that connects to another Cisco ONS 15540. This second Cisco ONS 15540 connects via a Y cable to the GE interface of another Cisco Catalyst 6000 series.

  Symptom 1: The Cisco Catalyst 6000 series at the receiving end does not receive any light.

  Condition 1: This symptom is observed when the portfail notification is received on the working active interface on one of the Cisco ONS 15540 platforms and when auto-failover is disabled, preventing the hardware from switching. However, APS still turns the working laser off, causing the working interface to enter the standby mode. Note that the symptom may also occur when Cisco ONS 15530 platforms are used.

  Workaround 1: There is no workaround.

  Symptom 2: Auto-negotiation between the two Cisco Catalyst 6000 series fails.

  Condition 2: This symptom is observed when auto-failover is disabled and FLC (wave side) is enabled on the Cisco ONS 15540 platforms, causing end-to-end negotiation between the Cisco Catalyst 6000 series to fail. Because the originating Cisco Catalyst 6000 series continues to pulse its light, FLC is triggered and the wave side laser is turned on and off accordingly. Note that the symptom may also occur when Cisco ONS 15530 platforms are used.

  Workaround 2: There is no workaround.

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP “source quench” messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Resolved Caveats—Cisco IOS Release 12.2(22)S1

Cisco IOS Release 12.2(22)S1 is a rebuild release for Cisco IOS Release 12.2(22)S, which supports only the Cisco ONS 15530 and Cisco ONS 15540, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(22)S1 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCin67568

  Symptoms: A Cisco device experiences a memory leak in the CDP process.

  Conditions: The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

  Workaround: Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the global command **no cdp run**.

- CSCuk50643

  Symptoms: A router reloads when the NTP server association is set via SNMP.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(22)S.

  Workaround: Enter the **ntp peer** command.

Miscellaneous

- CSCec20873

  Symptoms: Both the working and the protect interface go into the standby state if sf-lp,1 is followed by sf-lp,0. This situation affects the APS functionality. The correct behavior is that in the presence of both sf-lp,1 and sf-lp,0 the working interface should be active and the protect interface should be standby.

  Conditions: This symptom is observed on a Cisco ONS 15530 and Cisco ONS 15540 when you use y-cable APS.

  Workaround: There is no workaround.

- CSCed40933

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory, which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml.

Open Caveats—Cisco IOS Release 12.2(22)S

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(22)S, which supports only the Cisco ONS 15530 and Cisco ONS 15540. All the caveats listed in this section are open in Cisco IOS Release 12.2(22)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCdz59146

  Symptoms: An ethernetdcc interface may lose connectivity.

  Conditions: This symptom is observed on a Cisco ONS 15530 when you shut down the waveethernetphy interface under the following conditions:

  - Splitter protection is configured.
  - The protection wavepatch interface is active.
  - The working wavepatch interface is down.

  Workaround: Do not shut down the waveethernetphy interface when the working wavepatch interface is down.

- CSCea52092

  Symptom: An Optical Supervisory Channel (OSC) module may not provide any power even though the laser is enabled.

  Conditions: This symptom is observed after you have booted a Cisco ONS 15530.

  Workaround: Perform an online removal and insertion (OIR) of the OSC module.

  Alternate Workaround: Perform and OIR of the carrier motherboard.

- CSCeb18103

  Symptoms: An Optical Supervisory Channel (OSC) wave interface may not come back up after a trunk fiber break is resolved.

  Conditions: This symptom is observed on a Cisco ONS 15530 and Cisco ONS 15540 when you configure laser safety control after the trunk fiber break occurs.

  Workaround: To bring up the OSC wave interface, disable and reenable laser safety control.

- CSCec14447

  Symptoms: A client-side laser of an 8-port GE/FC aggregation card may not be in the proper state.

  Conditions: This symptom is observed on a Cisco ONS 15530 that is configured for Forward Laser Control (FLC) when a cyclic redundancy check (CRC) threshold for outgoing traffic is exceeded.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface of the 8-port GE/FC aggregation card.

- CSCec18408

  Symptoms: A unidirectional or bidirectional y-cable automatic protection switching (APS) switchover of a 10-GE transponder module takes up to 10 seconds.

  Conditions: This symptom is observed on a Cisco ONS 15540 ESPx that runs Cisco IOS Release 12.1(12c)EV or Release 12.2(22)S when a signal failure or fibre break at the client side or trunk side causes a switchover to occur.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(22)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(22)S, which supports only the Cisco ONS 15530 and Cisco ONS 15540. However, many caveats are platform-independent. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdy17802

  Symptoms: The **no cdp run** global configuration command may be deleted from the running configuration file.

  Conditions: This symptom is observed on a Cisco router when you create a subinterface after you have reloaded the router.

  Workaround: Reenter the **no cdp run** global configuration command.

- CSCdy50225

  Symptoms: A Cisco 12000 series may reload when a line card has failed and you perform a Simple Network Management Protocol (SNMP) query to cpmCPUTotalTable from a network management station (NMS).

  Conditions: This symptom is observed under very rare situations on a Cisco 12000 series but may also occur on other Cisco platforms.

  Workaround: When a line card has failed, do not perform an SNMP query to cpmCPUTotalTable from an NMS.

- CSCec87661

  Symptoms: A “SYS-2-CHUNKBOUNDS” error message may be displayed on the router console. This message may be followed by a “NOTQ” error message.

  Conditions: This symptom is observed under rare circumstances during heavy usage of any application that is using chunks. The symptom is platform independent.

  Workaround: There is no workaround.

- CSCin53807

  Symptoms: A warm reboot may fail on a Cisco router because of a decompression failure.

  Conditions: This symptom is platform independent and may occur in Cisco IOS Release 12.2 S or Release 12.3 T.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCea33013

  Symptoms: Traffic that exceeds 1484 bytes may not be passed between two customer edge (CE) routers.

  Conditions: This symptom is observed when one CE router is configured for ATM and the other CE router is configured for Ethernet or VLANs.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdu59038

  Symptoms: A Cisco router or switch may reload unexpectedly when you enter the **show ip eigrp neighbors** EXEC command.

  Conditions: This symptom is platform independent and is observed when you enter the **show ip eigrp neighbors** EXEC command immediately after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command for the interface that connects the router or switch to the neighbor.

  Workaround: Wait for the neighbor list to be completely rebuilt before you enter the **show ip eigrp neighbors** EXEC command.

- CSCdv90022

  Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a Cisco router that has a Route Processor (RP), the RP may stop receiving traffic.

  Conditions: This symptom is observed when a default route is configured for management purposes over the Ethernet 0 interface. This configuration is not recommended because the Ethernet 0 interface is not designed to switch traffic.

  Workaround: Configure the default IP route by entering the **ip route 0.0.0.0 0.0.0.0** *interface-type interface-number* global configuration command, and enter the interface of the next-hop router for the *interface-type* and *interface-number* arguments.

- CSCea58973

  Symptoms: A Border Gateway Protocol (BGP) route to a next-hop address may be purged after a Stateful Switchover (SSO) occurs on a Route Processor (RP).

  Conditions: This symptom is observed on a Cisco router when the next-hop address of the BGP route is also advertised by BGP.

  Workaround: Do not redistribute the next-hop address of the BGP route into the BGP configuration.

- CSCea90941

  Symptoms: The EIGRP Stub Routing feature may be missing from the configuration.

  Conditions: This symptom is observed when a Cisco router on which the EIGRP Stub Routing feature is enabled is reloaded, or when the Enhanced Interior Gateway Routing Protocol (EIGRP) process is restarted.

  Workaround: There is no workaround; you must reenable the EIGRP Stub Routing feature.

- CSCeb32598

  Symptoms: A Cisco router may reload when you enter the **show ip bgp regexp** EXEC command repeatedly. The router may also reload when you enter the **show ip bgp** EXEC command after you enter the **show ip bgp regexp** EXEC command.

  Conditions: This symptom is observed on a Cisco router that is configured with inbound policies that contain prefix lists, autonomous system path filter lists, and so on.

  Workaround: There is no workaround.

- CSCeb77038

  Symptoms: A Cisco router may pause indefinitely because of a bus error, and the following error message may appear:

  ```
  System returned to ROM by bus error at PC 0x60B5F1C0, address 0xEF4321E5
  ```

  Conditions: This symptom is observed on a Multiprotocol Label Switching (MPLS) provider edge (PE) router.

  Workaround: There is no workaround.

- CSCec06466

  Symptoms: A Cisco router may reload unexpectedly when the Designated Forwarder (DF) interface is changed to an interface that is already in the Outgoing Interface list (O-list).

  Conditions: This symptom is observed on a Cisco router that is configured for multicast Bidirectional PIM (Bidir-PIM).

  Workaround: There is no workaround.

- CSCec07592

  Symptoms: The best path is not chosen correctly on a Cisco router.

  Conditions: This symptom is observed when the **bgp deterministic med** router configuration command is configured on a Cisco router. The symptom occurs when different values of Multi Exit Discriminator (MED) are set for peers. In this particular situation, the symptom occurs when different values of MED are set to different peers.

  Workaround: There is no workaround.

- CSCec07636

  Symptoms: When the following Open Shortest Path First (OSPF) MIB tables are queried via snmpwalk, some interfaces may not be displayed:

  - ospfNbrTable
  - ospfIfTable
  - ospfIfMetricTable

  Conditions: This symptom is observed on any Cisco platform that runs OSPF.

  Workaround: There is no workaround.

- CSCec13278

  Symptoms: A Cisco router may generate continual tracebacks when you perform an online insertion and removal (OIR) of a line card.

  Conditions: This symptom is observed when Internet Group Management Protocol (IGMP) and IP Protocol Independent Multicast (PIM) are enabled.

  Workaround: Before you perform the OIR, disable IP PIM.

- CSCec15095

  Symptoms: A network link-state advertisement (LSA) may not be originated for an interface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S, Release 12.2 S, Release 12.3, or Release 12.3 T when an interface that is configured for Open Shortest Path First (OSPF) and that is up has the same address as another interface that is shut down.

  Workaround: There is no workaround.

- CSCec29868

  Symptoms: An Open Shortest Path First version 3 (OSPFv3) adjacency may flap when a standby Route Processor (RP) comes up after a switchover has occurred or after a router has reloaded. The router database may contain duplicate entries of the network link-state advertisement (LSA), or link LSA, or both.

  Conditions: This symptom is observed after a switchover has occurred when the interface number of the interface that is configured for OSPFv3 changes.

  This symptom is also observed after the router has reloaded when the interface number of the interface that is configured for OSPFv3 changes and when the neighbor still has the LSA (that was generated by the router on which the symptom occurs) with the old Link State ID (LSID) in its database. This situation may occur when the router does not clean up its LSA (for example, when the router reloads unexpectedly) or when the interface that connects to the neighbor is shut down before the router reloads and then brought back up after the router has reloaded.

  Workaround: There is no workaround.

- CSCec33773

  Symptoms: When a path is added to or deleted from the transit area between two virtual link routers that function as virtual link endpoints, the routes that are learned from the network backbone may not be updated in the routing table.

  Conditions: This symptom is observed when there are multiple equal-cost paths for virtual links in the transit area.

  Workaround: After the path in transit area has changed, enter the **clear ipv6 ospf force-spf** privileged EXEC command on the virtual link router that functions as a virtual link endpoint and that is not part of the network backbone.

- CSCec40377

  Symptoms: A multicast router may stop sending Protocol Independent Multicast (PIM) join messages.

  Conditions: This symptom is observed on a Cisco router that is configured for multicast routing when buffer allocation failures occur and when the I/O memory is low.

  Workaround: Disable and reenable multicast routing.

- CSCec40548

  Symptoms: A router may no longer be able to reach IP destinations through Open Shortest Path First (OSPF).

  Conditions: This symptom is observed when the **mpls traffic-eng area** *number* router configuration command is removed from the OSPF configuration.

  Workaround: Clear the OSPF process by entering the **clear ip ospf process** privileged EXEC, and wait for the OSPF process to recover. This workaround is not recommended when there is a large routing table.

  Alternate Workaround: Reconfigure the **mpls traffic-eng area** *number* router configuration.

- CSCec43772

  Symptoms: When a large number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets is received, the input-queue counters of an interface may slowly increase, eventually causing the interface to become wedged.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(14)SZ3 or Release 12.2(18)S.

  Workaround: Reload the router.

- CSCec43805

  Symptoms: The **distance bgp** *external-distance internal-distance local-distance* address family or router configuration command may be missing from a Border Gateway Protocol (BGP) IPv4 Virtual Private Network (VPN) configuration in the output of the **show running-config** privileged EXEC command when all of the following keywords in the **address-family ipv4 vrf** *vrf-name* router configuration command are configured with their default values:

```
- aggregate-address    Configure BGP aggregate entries
- auto-summary         Enable automatic network number summarization
- bgp                  BGP specific commands
- default              Set a command to its defaults
- default-information  Control distribution of default information
- default-metric       Set metric of redistributed routes
- distance             Define an administrative distance
- distribute-list      Filter networks in routing updates
- exit-address-family  Exit from Address Family configuration mode
- help                 Description of the interactive help system
- maximum-paths        Forward packets over multiple paths
- neighbor             Specify a neighbor router
- network              Specify a network to announce via BGP
- no                   Negate a command or set its defaults
- redistribute         Redistribute information from another routing protocol
- synchronization      Perform IGP synchronization
- table-map            Map external entry attributes into routing table
```

  However, the **distance bgp** *external-distance internal-distance local-distance* address family or router configuration command functions fine because the BGP administrative distance for the VPN in which the command is configured does get changed.

  Conditions: The symptom is observed after the BGP IPv4 VPN configuration is saved in NVRAM and the router is reloaded.

  Workaround: Change any of the keywords for the **address-family ipv4 vrf** *vrf-name* router configuration command (see the Symptoms section above) to a nondefault value.

- CSCec44271

  Symptoms: The Multiprotocol BGP (MBGP) feature does not function when a router is configured as a Border Gateway Protocol (BGP) route reflector.

  Conditions: This symptom is observed when a BGP peer group has been enabled and then the MBGP feature is added.

  Workaround: Reset the BGP peer group by removing the peer group configuration and adding it back.

- CSCec45770

  Symptoms: A memory leak may occur on a router that runs IPv6 Open Shortest Path First version 3 (OSPFv3), and the following error message that is related to chunks may be generated:

  ```
  SYS-2-CHUNKSIBLINGS: Attempted to destroy chunk with siblings
  ```

  Tracebacks may also be generated.

  Conditions: This symptom is observed when a configuration change occurs in which prefixes are added or deleted or when the router reloads and the same prefix is advertised with a different Link State ID (LSID).

  Workaround: There is no workaround.

- CSCec48816

  Symptoms: A router may reload unexpectedly when you remove a **network** command. There is a small window during which this symptom can occur: when a **network** command that covers an interface that is running OSPF is removed and when there are outstanding packets from this interface in OSPF queue.

  Conditions: This symptom is observed on a Cisco router that has the **router ospf** global configuration command enabled.

  Workaround: There is no workaround.

- CSCec68467

  Symptoms: The memory usage of the Open Shortest Path First version 3 (OSPFv3) process may increase unexpectedly.

  Conditions: This symptom is observed on a Cisco router that runs OSPFv3 when OSPFv3 advertises routes and when you clear OSPFv3 by entering the **clear ipv6 ospf process** privileged EXEC command or when you configure or disable OSPFv3 by entering the **ipv6 router ospf** or **no ipv6 router ospf** router configuration command.

  Workaround: Shut down the interfaces on which OSPFv3 runs before you make changes to the OSPFv3 process by entering the commands stated in the Conditions above.

- CSCec70366

  Symptoms: When the multicast route (mroute) expiration timer is set to a nondefault holdtime value, a router may reload unexpectedly because of a watchdog timeout.

  Conditions: This symptom is observed on a Cisco router when a nondefault holdtime value is received via a Protocol Independent Multicast (PIM) join message in combination with a bursty source. This situation may cause the mroute expiration timer to enter an infinite loop.

  Because the holdtime value is not user configurable on a Cisco router, this situation is caused by a PIM connection with a non-Cisco router or by the modification of the Internet Group Management Protocol (IGMP) query interval on an interface.

  Workaround: Ensure that no nondefault holdtime value can be configured for PIM or IGMP.

- CSCec70664

  Symptoms: Routes on a provider edge (PE) router may take almost 10 minutes to propagate through a network because Border Gateway Protocol (BGP) remains in read-only mode for a long period of time.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that is a BGP peer to other PE routers. A list of the affected releases can be found at http://www.cisco.com/cgi- bin/Support/Bugtool/onebug.pl?bugid=CSCeb54512. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCec72160

  Symptoms: The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature may fail; a not-so-stubby area (NSSA) area border router (ABR) may fail to set the forwarding address of the translated Type-5 link-state advertisements (LSAs) to zero.

  Conditions: This symptom is observed on a Cisco platform that functions as an NSSA ABR when the following sequence of events occurs:

  1. You enter the **area** *area-id* **nssa** router configuration command.
  2. Sufficient time passes for learned Type-7 LSAs to be translated into Type-5 LSAs.
  3. You enter the **area** *area-id* **nssa translate type7 suppress-fa** router configuration command.

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

  Alternate Workaround: Enter the **no area** *area-id* **nssa** router configuration command followed by the **area** *area-id* **nssa translate type7 suppress-fa** router configuration command.

- CSCec82144

  Symptoms: A provider edge (PE) router may reload unexpectedly when you remove a loopback interface.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that is configured for Any Transport over MPLS (AToM) and Fast Reroute (FRR).

  Workaround: Do not remove the loopback interface when AToM and FRR are configured.

- CSCed06329

  Symptoms: The Border Gateway Protocol (BGP) table version may continue to increase, causing continuous updates to occur.

  Conditions: This symptom is observed when multipath is configured for IPv6 BGP and when a path transitions from multipath to nonmultipath.

  Workaround: Disable multipath.

  Alternate Workaround: To prevent BGP from checking for version updates, enter the **address-family ipv4 unicast** router configuration command.

- CSCuk48168

  Symptoms: Enhanced Interior Gateway Routing Protocol (EIGRP) connectivity may not be established.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(22)S.

  Workaround: There is no workaround.

Miscellaneous

- CSCdz15807

  Symptoms: A file that is copied from a remote server to the running configuration file using secure file transfer (SCP) may fail with an error 26 (internal error).

  Conditions: This symptom is observed if the remote server is running the Linux operating system.

  Workaround: Use another file transfer method (for example, FTP).

- CSCea60722

  Symptoms: A Cisco Express Forwarding (CEF) adjacency may not adjust when changes are made to the configuration.

  Conditions: This symptom is observed when you move the IP address from an ATM interface to another interface and when the next-hop router is still mapped in the ATM permanent virtual circuit (PVC). The CEF adjacency continues to point to the ATM interface.

  Workaround: Remove the ATM PVC, and reload the router.

- CSCeb48835

  Symptoms: Boot variables may not be cleared, may not be set, or may become corrupted.

  Conditions: This symptom is observed when you copy a configuration to the startup configuration, for example by entering the **copy system:running-config nvram:startup-config** EXEC command. The old boot variables may not be replaced with the new boot variables; instead, they may be appended incorrectly. The old boot variables should be replaced with the new boot variables.

  Workaround: First, enter the **no boot system** global configuration command and save the configuration. Then, configure the new boot statement.

- CSCeb49834

  Symptoms: If a Cisco platform has the nvram:ifIndex-table file in an incorrect format, difficulties may occur during bootup, and the following error message may be displayed:

  ```
  System init: Insufficient memory to boot the image.
  ```

  Conditions: This symptom is platform independent and is observed in Cisco IOS Release 12.1 E, 12.1(13)EW, 12.1(19)EW, and 12.2 S.

  Workaround: Never create a file that is named ifIndex-table in NVRAM.

  Note: There are no difficulties with the file format when the nvram:ifIndex-table file is created by entering the **snmp-server ifindex persist** global configuration command. There is no need to delete the nvram:ifIndex-table file when you see this file in the configuration and the platform boots up and runs properly.

- CSCec08364

  Symptoms: Ethernet over Multiprotocol Label Switching (EoMPLS) packet forwarding may stop.

  Conditions: This symptom is observed when you configure an IP address on the EoMPLS interface.

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

- CSCec11541

  Symptoms: It may take up to 10 minutes for a Cisco router to read or download a configuration that contains 500 traffic engineering (TE) tunnels. When the configuration has been read or downloaded, the CPU utilization may be very high, even when the TE tunnels are down. The symptom may also occur when a smaller numbers of TE tunnels is configured, but to a lesser extent.

  Conditions: This symptom is observed on a Cisco router that is configured for Multiprotocol Label Switching (MPLS).

  Workaround: There is no workaround.

- CSCec12741

  Symptoms: If an access control list (ACL) is recompiled under heavy load conditions, CPUHOG messages may be generated.

  Conditions: This symptom is observed when compiled ACLs are enabled by entering the **access-list compiled** global configuration command, and the total number of ACL entries is relatively large (over 1500 lines). Random or constantly changing traffic patterns may cause the CPUHOG messages. A side effect of this symptom is that not enough time is provided for other processes, and areas such as keepalives or Cisco Express Forwarding (CEF) management may be impacted.

  Workaround: Disable and then reenable the compiled ACLs by entering the **no access-list compiled** global configuration command followed by the access-list compiled global configuration command.

  Alternate Workaround: Disable the compiled ACLs completely.

- CSCec22912

  Symptoms: When you configure a channelized interface, the following error message and tracebacks may be displayed:

  ```
  %INTERFACE_API-3-NODESTROYSUBBLOCK: The SWIDB subblock named OUNIC was not removed
  -Traceback= 502722FC 50272604 502727DC 5027281C 506A0960 506A57D8 506AA920 506AB788
  506AB91C 506ABD54 5020EC20 5021D5BC 502D011C 502D0108
  ```

  Conditions: This symptom is observed when you first delete and then reconfigure a channelized interface.

  Workaround: There is no workaround.

- CSCec26563

  Symptoms: A Cisco router that is in the process of setting up a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed under unusual circumstances when the following series of events occur:

  – You disable MPLS TE tunnels on the router by entering the **no mpls traffic-eng tunnels** global configuration command.

  – You enter one of the following MPLS TE interface configuration commands on an interface:

    mpls traffic-eng attribute-flags *attributes*

    mpls traffic-eng administrative-weight *weight*

    mpls traffic-eng flooding thresholds

  – The router attempts to set up a TE tunnel over this interface while the interface state changes to "up." (This event causes the router to reload.)

  Workaround: Before you enter any of the above-mentioned MPLS TE interface configuration commands on the interface, ensure that MPLS TE tunnels are enabled on the interface by entering the **mpls traffic-eng tunnels** interface configuration command. Before you disable MPLS TE

tunnels on the interface by entering the **no mpls traffic-eng tunnels** interface configuration command, ensure that any of the above-mentioned MPLS TE interface configuration commands are removed from the interface.

- CSCec29504

  Symptoms: A Cisco router that is configured with redundant Route Processors (RPs) may reload unexpectedly.

  Conditions: This symptom is observed when the RPs use the Checkpoint Facility (CF) with bundled clients.

  Workaround: There is no workaround.

- CSCec35322

  Symptoms: A router may reload unexpectedly when you delete an IPv6 reflexive access control list (ACL) while an ACL that is defined in the *name* argument of the **evaluate** *name* access-list command continues to reference the deleted reflexive ACL.

  Conditions: This symptom occurs when a traffic flow matches the ACL that is defined in the *name* argument of the **evaluate** *name* access-list command.

  Workaround: Disable the **evaluate** *name* access-list command before you delete the reflexive ACL.

- CSCec37783

  Symptoms: Network Time Protocol (NTP) clients may not be able to synchronize to an NTP time server.

  Conditions: This symptom is observed when a Cisco router that functions as an NTP time server has the **ntp source** global configuration command enabled and when the router sends NTP packets via a source (src) port that is set to zero.

  Workaround: Disable the **ntp source** command.

- CSCec56047

  Symptoms: When you configure and deconfigure Multiprotocol Label Switching (MPLS) traffic engineering (TE), stale router ID information may be used in the node structure, causing the path lookup process in the TE label switched path (LSP) topology database to fail.

  Conditions: This symptom is observed when node structures are created and recycled in the TE LSP topology database without proper reinitialization of the router ID.

  Workaround: There is no workaround.

- CSCec64382

  Symptoms: You may not be able to send traffic through an IPv6-to-IPv4 (6to4) tunnel, but you may be able to receive traffic through this tunnel.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2 S or Release 12.3 when the interface on which the tunnel is configured flaps.

  Workaround: There is no workaround.

- CSCec69982

  Symptoms: You may not be able to reestablish a direct label distribution protocol (LDP) session over an Any Transport over MPLS (AToM) virtual circuit (VC).

Conditions: This symptom is observed on a Cisco router when the **mpls ip** interface configuration command is not enabled on any interface and when you delete and reenter the **xconnect** ATM VC configuration command in quick succession.

Workaround: Remove the AToM VC, delete and reenter the **xconnect** interface configuration command, wait until the router returns to the prompt, and recreate the AToM VC.

- CSCec74016

  Symptoms: When you delete an Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel interface by entering the **no interface tunnel** *number* global configuration command, a router may reload unexpectedly.

  Conditions: This symptom is observed when an IPv6 feature such as the Security ACL feature is configured on the ISATAP tunnel interface.

  Workaround: Remove the traffic filter from the interface before you delete the interface.

- CSCec80049

  Symptoms: When a tunnel interface goes down, a new Label Switched Path (LSP) is not signaled until the forwarding adjacency hold timer expires.

  Conditions: This symptom is observed on a Cisco router that is configured with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

  Workaround: There is no workaround.

- CSCec85172

  Symptoms: Control plane policy fails to match Address Resolution Protocol (ARP) packets with the **match protocol arp** class-map configuration command when the ingress interface has Inter-Switch Link (ISL) or Dot1q encapsulation.

  Conditions: This symptom occurs when a service policy is attached to the control plane in input direction.

  Workaround: There is no workaround.

- CSCed12831

  Symptom: A class that matches an access control list (ACL) with a log option may not match packets in a service policy.

  Condition: This symptom is observed in all types of service policies.

  Workaround: Remove the log option from the definition of the ACL.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed33451

  Symptoms: A spurious memory access may occur when you enter the **show connect intermediate** privileged EXEC command.

  Conditions: This symptom is observed on a Cisco ONS 15530 and a Cisco ONS 15540 after you have configured a patch between a Wavepatch interface and a Wdmrelay interface. The symptom does not affect any functionality.

  Workaround: Do not enter the **show connect intermediate** privileged EXEC command.

- CSCed33852

  Symptoms: A Cisco ONS 15530 may reload unexpectedly.

  Conditions: This symptom is observed when a faulty optical add/drop multiplexer (OADM) module is present in the chassis.

  Workaround: Replace the faulty OADM module.

- CSCed37749

  Symptoms: Any Transport over Multiprotocol Label Switching (AToM) virtual circuits (VCs) may fail to come up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2 S and that is configured for AToM and Cisco Express Forwarding (CEF). The symptom may also occur in Release 12.0 S.

  Workaround: Toggle the CEF configuration; that is, remove CEF and reconfigure CEF.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed40585

  Symptoms: CPUHOG messages or tracebacks may be generated when you enter the **no mpls ip** global configuration or interface configuration command or the **no mpls traffic-eng tunnels** global configuration or interface configuration command.

  Conditions: This symptom is observed on a Cisco platform that is configured for Multiprotocol Label Switching, in particular when the platform has a large number of interfaces that are configured for MPLS.

  Workaround: There is no workaround.

- CSCed41108

  Symptoms: A traceback may occur on a Cisco router that runs Border Gateway Protocol (BGP) and Virtual Private Network version 4 (VPNv4).

  Conditions: This symptom is observed after you have configured BGP.

  Workaround: There is no workaround.

- CSCed83998

  Symptoms: All MPLS packets are classified as having the MPLS experimental bit set to 0 on all MPLS outbound interfaces.

  Conditions: This symptom is observed in any MPLS environment.

  Workaround: There is no workaround.

- CSCin64935

  Symptom: A Cisco ONS 15530 may reload unexpectedly.

  Conditions: This symptom is observed when you perform an online insertion and removal (OIR) of a wide-band variable optical attenuator (WB-VOA) module.

  Workaround: Do not perform an OIR of a WB-VOA module.

- CSCin65618

  Symptoms: When you configure the alarm threshold on a waveethernetphy interface of a Cisco ONS 15530 2.5-Gbps ITU trunk card, a Cisco ONS 15530 platform may reload unexpectedly.

  Conditions: This symptom is observed when you perform the following steps:

  1. Configure a code violation running disparity (CVRD) threshold list and apply it to the wave Ethernet interface.
  2. Remove the trunk card, remove the threshold configurations from the threshold list, and reinsert the trunk card.
  3. Remove the trunk card again, configure a CVRD degrade threshold, remove the threshold list, and reinsert the trunk card.

  After you have performed these steps, the Cisco ONS 15530 platform reloads.

  Workaround: There is no workaround.

- CSCin66424

  Symptoms: Automatic protection switching (APS) of a working interface to a protect interface may not occur for the following modules:

  - 10 Gigabit Ethernet Transponder downlink module in a Cisco ONS 15540
  - 10 Gigabit Ethernet uplink module in a Cisco ONS 15530

  - 10 Gigabit Ethernet Trunk module in a Cisco ONS 15530
  - 2.5 Gigabit Ethernet Trunk module in a Cisco ONS 15530

  Conditions: This symptom is observed on the above-mentioned modules that are installed in a Cisco ONS 15530 or Cisco ONS 15540 and occurs under the following circumstances:

  - The module is installed in a Cisco ONS 15530 and configured for switch fabric based line card protection or the module is installed in a Cisco ONS 15540 and configured for y-cable APS.
  - The interfaces of the module have thresholds groups that are configured for Converged Data Link (CDL) header error checksum (HEC) errors, cyclic redundancy check (CRC) errors, or both.
  - The CDL HEC error thresholds, CRC error thresholds, or both, are exceeded.

  Workaround: Do not configure CDL HEC error thresholds, CRC error thresholds, or both. Rather, configure code violation running disparity (CVRD) error thresholds. In a configuration in which an APS switchover of a working interface to a protect interface is based on CDL HEC error thresholds, CRC error thresholds, or both, there is no workaround.

- CSCin67971

  Symptoms: When a unidirectional patch configuration is removed between a thru interface and a wdm interface, the system hangs for a long time, and it eventually crashes.

  Conditions: This symptom is observed on the Cisco ONS 15540 and Cisco ONS 15530 platforms.

  Workaround: Configure bidirectional patches between the thru and wdm interfaces.

- CSCuk47482

  Symptoms: A router may reload unexpectedly while you disable label distribution protocol (LDP) on an interface.

  Conditions: This symptom is observed on a router that has several interfaces that are configured for LDP when you disable LDP on all interfaces and when there is still one open TCP connection that is passively used by LDP while you disable LDP on the last interface.

  Workaround: There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCec26432

  Symptoms: A router may reload unexpectedly when you enter the **show ipx access-list** EXEC command or the **show access-list** privileged EXEC command.

  Conditions: The symptom is observed on a Cisco router that runs Cisco IOS Release 12.2 S.

  Workaround: Do not use the above-mentioned commands. To display information about the access control lists (ACLs) in the configuration, enter the **show running-config** EXEC command.

TCP/IP Host-Mode Services

- CSCeb21552

  Symptoms: The following error message may be displayed when a router receives a connection request on command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports:

  ```
  %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.2.2
  ```

Conditions: This symptom is observed on a Cisco router that has the remote shell (rsh) disabled.

Workaround: Filter the traffic that is destined for command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports.

First, enter the **show ip interface brief** EXEC command to display the usability status of interfaces that are configured for IP. The output may look like the following:

```
Interface      IP-Address      OK? Method Status                Protocol
Ethernet0/0    172.16.1.1      YES NVRAM  up                        up
Ethernet1/0    unassigned      YES NVRAM  administratively down    down
Serial2/0      192.168.2.1     YES NVRAM  up                        up
Serial3/0      192.168.3.1     YES NVRAM  up                        up
Loopback0      10.1.1.1        YES NVRAM  up                        up
```

Then, create the following access control list (ACL) for the router and apply this ACL to all interfaces that are enabled with the **ip access-group 177 in** router configuration command:

```
access-list 177 deny tcp any host 172.16.1.1 eq 514
access-list 177 deny tcp any host 172.16.1.1 eq 544
access-list 177 deny tcp any host 192.168.2.1 eq 514
access-list 177 deny tcp any host 192.168.2.1 eq 544
access-list 177 deny tcp any host 192.168.3.1 eq 514
access-list 177 deny tcp any host 192.168.3.1 eq 544
access-list 177 deny tcp any host 10.1.1.1 eq 514
access-list 177 deny tcp any host 10.1.1.1 eq 544
access-list 177 permit ip any any
```

- CSCec29952

  Symptoms: A Cisco router will not form a Border Gateway Protocol neighbor under the **address-family ipv4** [**vrf** *vrf-name*] router configuration command if Message Digest 5 (MD5) authentication is configured.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(18)S.

  Workaround: There is no workaround.

- CSCed21865

  Symptoms: A router may reload unexpectedly when a TCP watchdog timer expires.

  Conditions: This symptom is observed when the router has hundreds of Border Gateway Protocol (BGP) peers.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCec32738

  Symptoms: When a PPP connection comes up, an IP route should be added to the routing table, but this does not occur. Note that even though there is no entry in the routing table, packets are forwarded on the correct route based on their cached Forwarding Information Base (FIB) headers.

  Conditions: This symptom is observed on a Cisco router that functions as a standby router in a high availability (HA) configuration.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(20)S14

Cisco IOS Release 12.2(20)S14 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S14 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsb11698

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

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

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

- CSCsj44081

  Cisco IOS software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message when it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

  ```
  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

  Recommended Action: Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORR UPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

IP Routing Protocols

- CSCin95836

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

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

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

NHRP is not enabled by default for Cisco IOS.

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

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Miscellaneous

- CSCdz55178

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

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

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                          00000000011111111112222222222333^
                          12345678901234567890123456789012|
                                                           |
                                                        PROBLEM
                                                       (Variable Overflowed).
```

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

- CSCeb21064

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

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

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

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

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

- CSCef77013

  Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also result in a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

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

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml.

- CSCsc72722

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

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

  Workaround: There is no workaround.

- CSCse56501

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

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml.

- CSCsg40567

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

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

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

- CSCsg70474

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

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

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

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

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

- CSCsi01470

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

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

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

- CSCsi58871

  Symptoms: For a Gigabit Ethernet interface, the ifOutNUcastPkts may decrement rather than increment.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB but could also occur in Release 12.2S.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(20)S13

Cisco IOS Release 12.2(20)S13 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S13 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml.

EXEC and Configuration Parser

- CSCec40348

  Symptoms: A Cisco router that functions in high availability (HA) Stateful Switchover (SSO) mode may unexpectedly reload because of a software-forced crash when the Multilink PPP configuration is changed.

  Conditions: This symptom is observed when a multilink interface is deleted.

  Workaround: Do not delete a multilink interface when the router functions in HA SSO mode.

IBM Connectivity

- CSCec68023

  Symptoms: When you enter the **dlsw bridge-group** *group-number* global configuration command, the following error messages and tracebacks may be generated:

  ```
  %IDBINDEX_SYNC-3-UNKNOWN_TYPE: IDB type is unknown and cannot be synced: "",0
  -Traceback= 4021FCAC 40220F58 4021FF10 4022122C 40455C90 40457D4C 41256D8C 412592B0
  4125982C 40CC9D04 4125C6C8 4125B83C 4125B6A8 412620AC 41293FD4 4128A660
  %IDBINDEX_SYNC-3-IDBINDEX_INITKEY: Cannot initialize IDB index table lookup key: "",0
  ```

  Conditions: This symptom is observed only on a Cisco platform that is configured for High Availability (HA).

  Workaround: There is no workaround. However, the symptom is of a cosmetic nature. Data-link switching plus (DLSw+) functions properly.

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

IP Routing Protocols

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml.

- 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 Bug resolves a symptom of CSCec71950. Cisco IOS software images with this specific bug are not at risk of a 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

- CSCed68723

  Symptoms: Packets that are destined for an MPLS VPN may not reach their destination. The output of the **show ip cef vrf** *vrf name* **detail** command may show the following tag information:

```
10.0.0.0/16, version 437, epoch 0, cached adjacency to POS4/0
0 packets, 0 bytes
  Flow: AS 0, mask 16
  tag information set, all rewrites inherited  <---------
    local tag: assigned-when-resolved-later    <---------
  via 10.1.1.1, 0, 0 dependencies, recursive
    next hop 10.2.2.2, POS4/0 via 10.1.1.1/32
    valid cached adjacency
```

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN forwarding and CEF.

  Workaround: Clear the affected route by entering the **clear ip route vrf** *vrf name network mask* command.

- CSCee78444

  Symptoms: TDP and OSPF neighborship loss may occur on all interfaces of a Cisco 7304.

  Conditions: This symptom is observed about three to four times per day on a Cisco 7304 is configured with a NSE-100 and that runs Cisco IOS Release 12.2S. However, the neighborships are re-established almost immediately.

  Workaround: There is no workaround.

- CSCek47252

  Symptoms: A Cisco 7304 may reload unexpectedly when you enter the **show diag** *slot-number* command for a Port Adapter Carrier Card (7300-CC-PA).

  Conditions: This symptom is observed rarely on a Cisco 7304 and occurs only when the **show diag** *slot-number* command causes the 7300-CC-PA to reset unexpectedly.

  Workaround: To prevent the symptom from occurring, do not enter the **show diag** *slot-number* command or the **show tech-support** command, which includes the **show diag** *slot-number* command.

- CSCin99753

  Symptoms: When you enter the **test pppoe** command on the PPPoE client, the PPPoE client or PPPoE server crashes.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that functions as a PPPoE client or PPPoE server. When the Cisco 7304 functions as a server and you enter the **test pppoe** command on another Cisco 7304 that functions as a PPPoE client, the PPPoE server crashes. When another router functions as the PPPoE server and a Cisco 7304 functions as the PPPoE client, the PPPoE client crashes.

  Workaround: There is no workaround.

- CSCir00106

  Symptoms: IPC timeout messages may be generated on a Cisco 7304 that has an NSE-100.

  Conditions: This symptom is observed when the CPU usage of the router is at 100 percent, when the PXF engine is switched off, and when there is a heavy traffic that is punted to the RP.

Workaround: Enable PXF switching by entering the **ip pxf** command.

- CSCsb12598

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

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

  Cisco IOS is affected by the following vulnerabilities:

  – Processing ClientHello messages, documented as Cisco bug ID CSCsb12598

  – Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304

  – Processing Finished messages, documented as Cisco bug ID CSCsd92405

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

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

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

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

- CSCsb40304

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

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

  Cisco IOS is affected by the following vulnerabilities:

  – Processing ClientHello messages, documented as Cisco bug ID CSCsb12598

  – Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304

  – Processing Finished messages, documented as Cisco bug ID CSCsd92405

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

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

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

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

- CSCsd34855

  Symptoms: The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

  Conditions: The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

  Further Information: On the 13th September 2006, the Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759 – VTP version field DoS
  - CSCse40078/CSCse47765 – Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611 – Buffer Overflow in VTP VLAN name

  Cisco's statement and further information are available on the Cisco public website at http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml.

- 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.

- CSCsd80937

  Symptoms: A Cisco 7304 crashes when you enter the **show diag** command for the slot in which a de-activated PA-CC is installed. Later, when you enter the **hw-module slot** *slot-number* **start** command, the command is not accepted for the slot in which the de-activated PA-CC is installed.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB after you have selected the "No upgrade now" option from the ROMmon Upgrade menu, causing the PA-CC to become de-activated. The symptom may also occur in Release 12.2S.

Workaround: There is no workaround.

- CSCsd81407

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

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

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

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

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

- CSCsd92405

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- CSCsd95616

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

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

- CSCse39760

  Symptoms: A PA-CC does not recover when you perform a soft or hard OIR of the standby RP.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with dual RPs after a switchover has occurred that causes the standby RP to become the active RP. In this situation, when you perform a soft or hard OIR of the standby RP, the PA-CC does not recover because the PA-CC fails to initialize.

  Workaround: There is no workaround.

- CSCse68138

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

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

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

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

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

- CSCse98421

  Symptoms: When a Cisco 7304 that functions in an MPLS environment as a P router receives MPLS traffic that is forwarded as pure IP traffic, the router may incorrectly apply an MPLS string rather than an IP string, causing the next PE router to drop packets that have a size larger than 1496 bytes.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that runs Cisco IOS Release 12.2(28)SB1 or Release 12.2(28)SB2, that has PXF enabled, and that has MPLS configured on the connecting interfaces. The symptom could also occur in Release 12.2S.

  Workaround: Disable PXF, downgrade to Cisco IOS Release 12.2(25)S8, or disable MPLS. However, if none of these solutions are an option, there is no workaround.

  Further Problem Description: The same symptom is observed irrespective of the FPGA microcode that is used. The connecting interfaces have the **mtu 1512** and **ip mtu 1500** commands enabled so the MPLS MTU is the same as the interface MTU and the IP MTU is a bit less than the interface MTU to accommodate for two labels.

- CSCsf04754

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

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

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

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

- CSCsf17521

  Symptoms: When there is a hierarchical policy with a Class of Service (CoS), traffic shaping that is applied on the parent policy does not function properly for speeds that are slower than 2000 kbps because the throughput is reduced.

  Conditions: This symptom is observed on a Cisco 7304 when there is a priority class configured in a policy that is attached to an interface. The larger the packets, the more the throughput is reduced.

  Workaround: There is no workaround.

- CSCsg31202

  Symptoms: A Cisco 7304 with an NSE-100 may crash and generate the following error message:

  ```
  Unexpected exception, CPU signal 10, PC = 0x4008B2EC
  ```

  Conditions: This symptom is observed very rarely when the router is configured with an input policy that marks incoming IP traffic on one interface and then uses this information for classification on an output policy on another interface.

  Workaround: There is no workaround.

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.

- CSCse05736

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

Conditions: This symptom is seen under the following conditions:

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

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

Resolved Caveats—Cisco IOS Release 12.2(20)S12

Cisco IOS Release 12.2(20)S12 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S12 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCsc60249

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

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

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

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

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

- CSCsd46274

  Symptoms: A Cisco 7304 may hangs when the Cisco IOS software image is loaded during cleaning.

  Conditions: This symptom is observed on Cisco 7304 that has an NSE-100 but rarely on a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

  Further Problem Description: Cleaning comprises of the following steps:

  4. Erase all configurations from the router.
  5. Load the boot image, load the minimum configuration, and save the configurations.
  6. Reload the router with the proper image, and load the proper configurations.

- CSCsd49081

  Symptoms: A Cisco 7304 may hang when an HA switchover occurs.

  Conditions: This symptom is observed when you have entered the **hw-module stop** command followed by the **hw-module start** command for a port adapter before the HA switchover occurs.

  Workaround: Do not enter **hw-module stop** command followed by the **hw-module start** command for a port adapter.

  Further Problem Description: The symptom occurs only for port adapters, not for SPAs and native line cards.

- CSCsd87217

  Symptoms: For both DSCP-based and precedence-based WRED statistics counters, the output of the **show policy-map interface** command may show zero, or data for the wrong class.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCse37573

  Symptoms: The NPE-G100 in a Cisco 7304 crashes after the PA-CC has crashed.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S10 and that is configured with a PA-CC in which an 8-port ATM IMA port adapter is installed.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(20)S11

Cisco IOS Release 12.2(20)S11 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S11 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCdz41069

  Symptoms: On a Cisco 7500 series that has channelized T1/E1/T3/E3 port adapters, two different interfaces on these port adapters can have the same “hw_if_index” value, which can be seen in the output of the **show idb** command on the RSP. The output of the **show idb** command may show a line in the following format:

  ```
  HWIDB#x    y    z  <Interface Name String> u v (<string>)
  ```

  In this line, x,y,z,u, and v are numbers, and the “hw_if_index” value is presented by the number z.

  This situation may cause “CBUS-4-FIXBADTXVC” error messages to be generated.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(22)S when interfaces are created, deleted, and recreated by entering the **channel-group** and **no channel-group** controller configuration commands. The symptom may also occur in other releases.

  Workaround: Do not delete an interface, that is, do no enter the **no channel-group** controller configuration command.

- CSCec87736

  Symptoms: TX Simple Network Management Protocol (SNMP) counters do not update on Fast Ethernet subinterfaces for distributed Cisco Express Forwarding (dCEF) traffic.

Conditions: This symptom is observed on Cisco IOS Release 12.0(26)S and Release 12.3. The hardware is DEC21140A, and the interface receiving the traffic is not located on the same Versatile Interface Processor (VIP). The symptom may also occur in other releases.

Workaround: There is no workaround.

IP Routing Protocols

- CSCed67358

  Symptoms: An IPv6 PIM neighbor may be down after changing the PIM configuration.

  Conditions: This symptom is observed when the **no ipv6 pim** command is entered on some subinterfaces of a physical Ethernet interface and when PIM is enabled on several subinterfaces of the same physical Ethernet interface. The symptom affects both IPv4 and IPv6, and configurations with multicast and OSPF Hello messages.

  Workaround: There is no workaround.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Miscellaneous

- CSCdz84963

  Symptoms: A VIP that is installed in a Cisco 7500 series runs out of memory after some time of operation. The output of the **show processes memory** command shows that the CEF IPC background process holds a lot of memory, and the output of the **show buffers** command on the VIP shows that many buffers are used by IPC.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(18)S8 after dCEF is enabled.

Workaround: Disable dCEF. Note that the symptom does not occur in Release 12.2(14)S13.

- CSCeb63310

  Symptoms: A Cisco router that has an interface with an output service policy attached may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router when the **bandwidth** interface configuration command or the **fair-queue** interface configuration command is configured in the policy map that is attached via the **service-policy** router configuration command and when traffic is flowing through the interface at a fast rate. The router reloads under any of the following conditions:

  – The interface has the **ip rsvp bandwidth** interface configuration command configured, and the router reloads when you enter the **no ip rsvp bandwidth** interface configuration command.

  – The interface does not have the **ip rsvp bandwidth** interface configuration command configured, and you enter the **ip rsvp bandwidth** interface configuration command.

  – You enter the **ip rtp reserve** *lowest-udp-port range-of-ports* interface configuration command.

  In all three situations, a service policy that is configured with the **bandwidth** or **fair-queue** command is attached to the interface.

  Workaround: Shut down the interface before entering the above commands. Enable the interface again after you have entered the commands.

- CSCec06146

  Symptoms: A serial interface of a channelized port adapter may fail to enter the "up/up" state when you initially configure the interface or after a number of reconfigurations.

  Conditions: This symptom is observed on a channelized port adapter that is installed in a Cisco 7500 series or Cisco 7600 series when the following sequence of events occurs:

  1. You configure an interface by entering the **controller e3** *slot/port* global configuration command followed by the **e1** *line-number* **channel-group** *channel* **timeslots** *range* controller configuration command.
  2. You delete the interface by entering the **controller e3** *slot/port* global configuration command followed by the **no e1** *line-number* **channel-group** *channel* controller configuration command.
  3. You reconfigure the interface by entering the commands listed in Step 1.

  Although the symptom may occur when you initially configure the interface, it is more likely to occur when you configure, delete, and reconfigure the interface several times. In addition, the symptom may also occur after a link flap of an interface of one of the channelized cards.

  The symptom may occur on any of the following channelized port adapters: PA-MC-T3, PA-MC-2T3, PA-MC-xT1 (x = 2,4,8), PA-MC-xE1 (x = 2,4,8), and PA-MCX-xTE1 (x = 2,4,8).

  Workaround: When the interface does not enter the "up/up" state, configure the interface again.

- CSCec37783

  Symptoms: Network Time Protocol (NTP) clients may not be able to synchronize to an NTP time server.

  Conditions: This symptom is observed when a Cisco router that functions as an NTP time server has the **ntp source** global configuration command enabled and when the router sends NTP packets via a source (src) port that is set to zero.

  Workaround: Disable the **ntp source** command.

- CSCec80902

  Symptoms: A Cisco 7500 series that is configured for Hierarchical Queuing Framework (HQF) may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed when you attempt to print queue statistics for priority classes within the same layer of a policy map.

  Workaround: There is no workaround.

- CSCed48156

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

  Conditions: 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.

- CSCed76109

  Symptoms: On a Cisco 7500 series that is equipped with Versatile Interface Processors (VIPs) with ATM port adapters, the ATM PVCs may not come back up after the ATM interface flaps. This occurs because the interfaces in the VIP do not transmit any packets but still process incoming traffic.

  Conditions: This symptom is observed in a dLFIoATM environment in which distributed Class Based Weighted Fair Queueing (dCBWFQ) is configured on PPPoATM virtual templates.

  Workaround: Apply any kind of distributed queueing on any interface or subinterface of the affected VIP. Doing so triggers all interfaces to start transmitting again, enabling the ATM PVCs to come back up.

- 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.

- CSCin31767

  Symptoms: A Cisco router may reload when you enter the **show atm map** privileged EXEC command.

  Conditions: This symptom is observed on all Cisco routers after you have first deleted a subinterface on which a static map bundle was configured.

  Workaround: First remove the static map bundle; then, delete the subinterface.

- 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.

- CSCsc49455

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

  1. Symptom 1: A Cisco 7304 stops transmitting traffic on an interface for 16 seconds.

     Condition 1: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 processor that has PXF enabled and occurs in a rare situation when the router functions under a heavy load.

     Workaround 1: There is no workaround.

  2. Symptom 2: A Cisco 7304 stops processing incoming network messages for 16 seconds.

     Condition 2: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 processor that has PXF enabled and occurs when the interface functions as the internal path from the PXF engine to the main processor.

     Workaround 2: There is no workaround.

- CSCsd11646

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

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

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

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

- 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.

- 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 card.

- 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.

TCP/IP Host-Mode Services

- CSCeb21552

  Symptoms: The following error message may be displayed when a router receives a connection request on command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports:

  ```
  %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.2.2
  ```

  Conditions: This symptom is observed on a Cisco router that has the remote shell (rsh) disabled.

  Workaround: Filter the traffic that is destined for command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports.

  First, enter the **show ip interface brief** EXEC command to display the usability status of interfaces that are configured for IP. The output may look like the following:

  ```
  Interface      IP-Address      OK? Method Status                Protocol
  Ethernet0/0    172.16.1.1      YES NVRAM  up                    up
  Ethernet1/0    unassigned      YES NVRAM  administratively down down
  Serial2/0      192.168.2.1     YES NVRAM  up                    up
  Serial3/0      192.168.3.1     YES NVRAM  up                    up
  Loopback0      10.1.1.1        YES NVRAM  up                    up
  ```

  Then, create the following access control list (ACL) for the router and apply this ACL to all interfaces that are enabled with the **ip access-group 177 in** router configuration command:

  ```
  access-list 177 deny tcp any host 172.16.1.1 eq 514
  access-list 177 deny tcp any host 172.16.1.1 eq 544
  access-list 177 deny tcp any host 192.168.2.1 eq 514
  access-list 177 deny tcp any host 192.168.2.1 eq 544
  access-list 177 deny tcp any host 192.168.3.1 eq 514
  access-list 177 deny tcp any host 192.168.3.1 eq 544
  access-list 177 deny tcp any host 10.1.1.1 eq 514
  ```

```
access-list 177 deny tcp any host 10.1.1.1 eq 544
access-list 177 permit ip any any
```

Wide-Area Networking

- CSCec83030

  Symptoms: A parity error on a Versatile Interface Processor (VIP) card may cause other VIPs to go to a wedged state.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(20)S10

Cisco IOS Release 12.2(20)S10 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S10 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeg64124

  Symptoms: The operation result of an IP SLA jitter probe shows a high packet MIA that is equal to the jitter's number of packets minus one. In the responder router, the responder debug message shows many error packets.

  Conditions: This symptom is observed when multiple jitter probes (either from the same router or from different routers) are configured to send packets to the same destination IP address and the same destination port number and when the responder is turned off for a short time and turned on again.

  Workaround: To prevent the symptom from occurring, configure the jitter probe to use a unique destination port number.

  Alternate Workaround: If the symptom has occurred, turn off the responder by entering the **no rtr responder** global configuration command, wait until all jitter probes report "No connection," and then turn on the responder by entering the **rtr responder** global configuration command.

IP Routing Protocols

- CSCei13040

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

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

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

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

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

- CSCsc07467

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

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

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

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

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

Miscellaneous

- 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.

- 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.

- 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.

- CSCej62850

  Symptoms: When you remove the first link member of an IMA group from a PA-A3-8T1IMA port adapter, the link remains down.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 7300-CC-PA in which a PA-A3-8T1IMA port adapter is installed.

  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.

  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.

- CSCsc14859

  Symptoms: A Cisco 7304 may reload because the PXF engine reloads unexpectedly.

  Conditions: This symptom is observed rarely on a Cisco 7304 that is configured with an NSE-100 and is not associated with any specific configuration or traffic type.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(20)S9

Cisco IOS Release 12.2(20)S9 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S9 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCei61732

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

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

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

Interfaces and Bridging

- CSCin86455

  Symptoms: Auto-provisioning may be disabled on a Cisco router that is configured with a PA-A3 port adapter.

  Conditions: This symptom is observed when a VC class that is configured for create on-demand is attached to the main ATM interface and then the create on-demand configuration is removed and re-applied to the VC class.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface of the PA-A3 port adapter.

ISO CLNS

- CSCeh61778

  Symptom: A Cisco device running IOS and enabled for Intermediate System-to- Intermediate System (IS-IS) routing protocol may reset with a SYS-2-WATCHDOG error from a specifically crafted malformed IS-IS packet. The IS-IS protocol is not enabled by default.

  Conditions: The IS-IS crafted malformed IS-IS Packet that requires processing will not be forwarded across a Level 1/Level 2 boundary. The specifically crafted malformed IS-IS packet would require local attachment to either a Level 1 or Level 2 router. A Cisco device receiving the malformed IS-IS packet will forward the malformed packet to its neighbors, and may reset.

  Workaround: There is no workaround. Enabling IS-IS Authentication is seen as a best practice, and can be leveraged as a mitigation technique.

IP Routing Protocols

- CSCeb77038

  Symptoms: A Cisco router may pause indefinitely because of a bus error, and the following error message may appear:

  ```
  System returned to ROM by bus error at PC 0x60B5F1C0, address 0xEF4321E5
  ```

  Conditions: This symptom is observed on a Multiprotocol Label Switching (MPLS) provider edge (PE) router.

  Workaround: There is no workaround.

- CSCec40377

  Symptoms: A multicast router may stop sending Protocol Independent Multicast (PIM) join messages.

  Conditions: This symptom is observed on a Cisco router that is configured for multicast routing when buffer allocation failures occur and when the I/O memory is low.

  Workaround: Disable and reenable multicast routing.

- CSCee41172

  Symptoms: The **maximum-paths import** *number-of-paths* command enables a VRF to import additional paths in addition to the bestpath. If the original path of the import path is withdrawn, wrong import paths may be purged. This situation may cause traffic disruption up to 15 seconds.

Conditions: This symptom is observed when the original path of the best import path is withdrawn and the import path is at the end of the path list (that is, the one learned the very first). In this situation, all import paths that are derived from other paths may be purged as well. If the imported net has only import paths, the net may not be reachable until other paths are reimported.

Workaround: Ensure that the import path is at the top of the path list or use the same route descriptor (RD) for all import paths.

- CSCee85676

  Symptoms: When VPNv4 route advertisement are received after BGP has converged, the existing path is updated but imported paths from the original path are not updated accordingly.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the **maximum-paths** *number-of-paths* **import** *number-of-paths* command is enabled. The symptom occurs when the path attributes are changed dynamically instead of the path being completely withdrawn and readvertised.

  Workaround: Withdraw the prefix from the remote PE router and then readvertise the prefix.

- CSCef57803

  Symptoms: In a VPNv4 network in which a multi-homed CE router advertises multiple paths for a prefix, a PE router may fail to withdraw the prefix previously advertised to another PE router when its best path changes from a non-imported path to an imported path because of a change in the import route map of the VRF.

  Conditions: This symptom is observed in a topology in which a CE router connects to a PE router via two different VRFs.

  Workaround: Remove the imported path either by unconfiguring the import route map of the VRF or by changing the import route target, withdraw the non-imported prefix from the CE router, and restore the import route map or import route target.

- CSCef60452

  Symptoms: A router may stop receiving multicast traffic.

  Conditions: This symptom is observed rarely during convergence when a router receives a Join message on an RPF interface and when a downstream router converges faster than the first router that receives the Join message.

  In this situation, the router does not populate the RPF interface into the OIL (that is, the OIL remains null) because the old SP-tree has already been pruned by the downstream router. When the RPF interface of the router changes to the new path later, it does not trigger a Join message toward the multicast source until the router receives a next periodic Join message from the downstream router and populates the OIL. As a result, multicast traffic stops temporarily but no longer than the periodic Join message interval.

  Workaround: There is no workaround.

- CSCef97738

  Symptoms: BGP may pass an incorrect loopback address to a multicast distribution tree (MDT) component for use as the source of an MDT tunnel.

  Conditions: This symptom is observed when you reload a Cisco router that runs Cisco IOS Release 12.0(28)S1 and when there is more than one source address that is used in BGP, such as Lo0 for IPv4 and Lo10 for VPN. If the IPv4 peer is the last entry in the configuration, the MDT tunnel interface uses lo0 as the source address instead of lo10. The symptom may also occur in other releases.

  Workaround: Remove and add the MDT statement in the VRF.

- CSCeh53906

  Symptoms: A stale non-bestpath multipath remains in the RIB after the path information changes, and BGP does not consider the stale path part of the multipath.

  Conditions: This symptom is observed on a Cisco router that has the **soft-reconfiguration inbound** command enabled and occurs only when the BGP Multipath Loadsharing feature is enabled for three or more paths, that is, the *number-of-paths* argument of the **maximum-paths** *number-of-paths* command has a value of three or more.

  Workaround: Disable the **soft-reconfiguration inbound** command for the neighbor sessions for which the BGP Multipath Loadsharing feature is enabled or reduce the maximum number of paths for the BGP Multipath Loadsharing feature to two.

- CSCuk54787

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for redistributed route maps.

ISO CLNS

- CSCin57685

  Symptoms: A Cisco 7200 series may reload unexpectedly while sending Connectionless Network Service (CLNS) packets.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(18)S1 but may also occur on other platforms and in other releases of Release 12.2S.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb56457

  Symptoms: An 8-port ATM Inverse MUX T1 port adapter (PA-A3-8T1IMA) may drop packets with a certain unknown pattern.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(16). The symptom may also occur on other platforms and in other releases.

  Workaround: There is no workaround.

- CSCec31162

  Symptoms: Incorrect tags may be imposed after a route has flapped.

  Conditions: This symptom is observed on a Cisco router that functions in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment.

  Workaround: There is no workaround.

- CSCec75189

  Symptoms: Two interfaces may have the same Cisco Express Forwarding (CEF) interface description block (IDB) when the following configuration sequence occurs:

  1. You create a subinterface.
  2. You delete this subinterface.
  3. You create another subinterface.
  4. You recreate the first subinterface.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S or Release 12.2S but may also occur on other platforms.

  Workaround: There is no workaround. Reload the router to clear the condition.

- CSCed08172

  Symptoms: When you enter the **write memory** privileged EXEC command on a Cisco 7206VXR, a long delay may occur during the transfer of packets.

  Conditions: This symptom is observed on a Cisco 7206VXR that is configured with a Network Processing Engine G-1 (NPE-G1), that runs Cisco IOS Release 12.2(18)S or a later release, and that functions as a Multiprotocol Label Switching (MPLS) provider edge (PE) router. The symptom may also occur on other platforms and in other releases.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(14)S3.

- CSCed72297

  Symptoms: Multiple SYS-3-CPUHOG error messages may be generated in the LDP process, eventually followed by a watchdog timeout crash:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (422/8),process
  = LDP.
  -Traceback= 6101DFC0 6102546C 61016FE4 6101CE24 6101728C 61017A30

  ...

  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = LDP.
  -Traceback= 6085658C 6101DE48 6102546C 61016FE4 6101CE24 6101728C 61017A30
  ```

  After the router has reloaded, the output of the **show version** command indicates “Last reset from watchdog reset.”

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S3 or Release 12.2(22)S and that is configured for MPLS LDP. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCef56327

  Symptoms: You may not be able to configure the **clock source line** command during the configuration of the SONET controller on a Cisco router in which a PA-MC-STM1 port adapter is installed.

  When you enter the **clock source line** command during the configuration of the SONET controller, the output of the **show running-config** command indicates that the clock source is set to line. However, the output of the **show controllers sonet** command indicates that the clock is set to internal, and when you enter the **show running-config** command again, the output indicates this time that the clock source is set to internal.

  Conditions: This symptom is observed when the PA-MC-STM1 port adapter is connected back-to-back via dark fiber to another PA-MC-STM1 port adapter.

Workaround: Enter the **overhead s1byte ignore** command on the SONET controller before you configure the clock source.

- CSCeg20374

  Symptoms: If a configuration file that contains a large number (4096) of virtual circuits is downloaded or copied to the running configuration, the standby RP may reload.

  Conditions: This symptom is observed on a Cisco 7304 that functions in HA SSO mode with two NSE-100 RPs or two NPE-G100 RPs and that is configured with an OC-3 ATM or OC-12 ATM line card.

  Workaround: There is no workaround.

  Further Problem Description: To prevent the symptom form occurring again, configure the standby RP to autoboot. Doing so enables the configuration to be synchronized to the standby RP via bulk synchronization.

- CSCeg38482

  Symptoms: AutoRP packets are dropped because of an RPF failure.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when both the Candidate RP and Mapping Agent (MA) are configured in a VRF context and when the interface is not specified in the **ip pim vrf** *vrf-name* **send-rp-discovery** *interface-type interface-number* command. This situation may cause the MDT update source address (an address that belongs to the global table) for the MVPN to be chosen and, in turn, the AutoRP flow to be created in the downstream route with a global address as the source.

  Workaround: Configure the interface that has the highest IP address in the VPN as the Candidate RP and MA.

  Alternate Workaround: Configure the interface that is defined in the Candidate RP as the interface in the **ip pim vrf** *vrf-name* **send-rp-discovery** *interface-type interface-number* command.

- CSCeg62979

  Symptoms: A PA carrier card that is installed in a Cisco 7304 that is configured with an NSE-100 may become deactivated and reloads, and the router generates the following error message:

  ```
  %PACC-3-HEARTBEAT_LOSS: PA Carrier Card Loss of heartbeat from linecard in slot
  <slot_number>
  ```

  Conditions: This symptom is observed when the router functions under stress and when a large number of packets are punted to the Route Processor (RP).

  Workaround: Reduce the stress by reducing the number of packets that are punted to the RP or by disabling some features on the router.

  Further Problem Description: When a large number of packets are punted to the RP and/or a high CPU load occurs on the router, heartbeat packets from the PA carrier card to the RP may be lost, causing the PA carrier card to become deactivated and reload.

- CSCeg67788

  Symptoms: The 5-minute output rate in the output of the **show interfaces** command is incorrect for serial interfaces that are configured on a PA-MC-8TE1+ port adapter.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-8TE1+ port adapter.

  Workaround: There is no workaround.

- CSCeh27709

  Symptoms: The link line rate cannot be achieved, and more than the expected number of packets drop.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a policy-map that contains traffic shaping classes is attached to an egress interface, and when configured average shape rate is larger than link bandwidth.

  Workaround: Do not configure traffic shaping rate over link bandwidth.

- CSCeh52460

  Symptoms: A standby RP of a Cisco 7304 that is configured for high availability (HA) may crash.

  Conditions: This symptom is observed when a link flap (originating on the remote end) occurs while ATM VCs are being created on a PA-A3 that is installed in a PA-CC. The symptom does not occur during the boot process of the router but only when the router is already up and running.

  Workaround: Prevent link flaps from occurring when you configure ATM VCs on a PA-A3 that is installed in a PA-CC.

  Alternate Workaround: Copy the configuration to the startup configuration and reload the router.

- CSCeh76459

  Symptoms: The output of the **show policy-map interface** *interface* command does not show a configured policy map for an IMA interface, although the output of the **show running-config** command does show the policy map for the same IMA interface.

  When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the IMA interface and you reload the router, the policy map is removed.

  Conditions: These symptoms are observed on a Cisco 7304 that is configured with an IMA port adapter.

  Workaround: Attach the policy map as part of a PVC and reload the router. Note that the symptom does not occur on a Cisco 7200 series that functions in the same configuration.

- CSCei17357

  Symptoms: A Cisco 7304 may not perform eBGP multihop loadbalancing for traffic that passes from a CE router to a PE router. VPN traffic is not affected.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(20)S8.

  Workaround: Reload the router.

- CSCin78324

  Symptoms: A Cisco router that is configured with a PA-MC-8TE1 port adapter may hang.

  Conditions: This symptom is observed on a Cisco 7200 VXR router that has a PA-MC-8TE1 port adapter and that is configured for IPSec encryption, either via tunnel protection or via a crypto map. The symptom may also occur on other platforms and in other releases.

  Workaround: Disable IPSec encryption.

- CSCin78325

  Symptoms: A serial interface of a PA-MC-8TE1+ continues to process packets even after the interface is placed in the "ADMINDOWN" state. The counters in the output of the **show interfaces serial** command may continue to increment even if the serial interface is shut down.

Conditions: This symptom is observed on a serial interface of a PA-MC-8TE1+ when there is a channel-group configuration for the interface.

Workaround: Remove the channel-group configuration for the interface.

- CSCin95530

  Symptoms: A Cisco 7304 may reload unexpectedly when you attach or detach a QoS policy to an ATM IMA PVC.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100 when you attach or detach the QoS policy while traffic passes through the router.

  Workaround: There is no workaround.

- CSCsa50971

  Symptoms: A Cisco platform may unexpectedly reload while attempting to resequence an access list.

  Conditions: This symptom is observed when you delete a few ACEs and then immediately enter the **ip access-list resequence** *access-list-name starting-sequence-number* **increment** command.

  Workaround: There is no workaround.

- 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.

  Workaround: There is no workaround.

- CSCsb19585

  Symptoms: A router may reload unexpectedly when you enter a **no match** Modular QoS CLI (MQC) command in a class map and when the parameters that are entered do not exactly match an existing **match** command that is configured for the same class map.

  Conditions: This symptom is observed on a Cisco 7304 that has one or more NSE-100 or NPE-G100 forwarding engines when the **aaa accounting** command is enabled. The symptom could occur on other routers or with other configurations.

  Workaround: When you enter a **no match** command, ensure that the parameters match an existing **match** command in the class map. A good way to do this is by copying and pasting the existing **match** command and by adding the **no** keyword to the command. If you wish to modify an existing **match** command, remove the command completely by entering the **no match** command, and then add back the parts that you want to use by entering the **match** command. For example, to remove IP precedence value 2 from the **match ip precedence 1 2** command, rather than entering the **no match ip precedence 2** command, first enter the **no match ip precedence 1 2** command, and then enter the **match ip precedence 1** command.

- CSCsb25109

  Symptoms: The PXF engine on a Cisco 7304 that is configured with an NSE-100 may punt many packets to the Route Processor (RP) because of null adjacencies.

  The output of the **show pxf accounting** command indicates that the Null Adjacency counter increases steadily. There are also some inconsistencies between the PXF table in the output of the **show pxf cef** command and the routing table on the RP in the output of the **show ip route** or **show ip cef** command.

  Conditions: This symptom is observed when the Cisco 7304 switches only IP traffic.

  Workaround: There is no workaround.

- CSCsb26828

  Symptoms: A Cisco 7304 may generate an "%NSE100-3-VA_ERROR: Vanallen ASIC detected" error message, traffic stops flowing, and adjacencies go down.

  Conditions: These symptoms are observed on a Cisco 7304 that is configured with an NSE-100, that runs Cisco IOS Release 12.2(20)S7 or Release 12.2(20)S8, and that has NetFlow enabled.

  Workaround: Disable NetFlow.

- CSCsb48482

  Symptoms: When an ATM PVC is congested, prioritized packets are delayed.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100. Note that the symptom does not occur on a Cisco 7304 that is configured with an NSE-100.

  Workaround: There is no workaround.

- CSCsb48489

  Symptoms: A Cisco 7304 that processes Frame Relay traffic crashes because of a bus error and generates the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x40, pc=0x40540BC0,
  ra=0x40540ACC, sp=0x4684DE18
  ```

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100 and that runs Cisco IOS Release 12.2(25)S5.

  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.

- CSCsb69080

  Symptoms: A Cisco 7304 may generate the following error message:

  ```
  %NSE100-3-VA_ERROR: Vanallen ASIC detected an error condition: TIC invalid DMA length
  ```

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100), that is configured for PXF hardware switching, and that has a GRE tunnel configured when the GRE traffic proceeds over a physical interface that is configured for dot1q VLAN encapsulation.

  Workaround: Do not use PXF hardware switching for GRE traffic. Rather, use software switching such as CEF, fast-switching, or process-switching.

Resolved Caveats—Cisco IOS Release 12.2(20)S8

Cisco IOS Release 12.2(20)S8 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S8 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCdy50225

  Symptoms: A Cisco 12000 series may reload when a line card has failed and you perform a Simple Network Management Protocol (SNMP) query to cpmCPUTotalTable from a network management station (NMS).

  Conditions: This symptom is observed under very rare situations on a Cisco 12000 series but may also occur on other Cisco platforms.

  Workaround: When a line card has failed, do not perform an SNMP query to cpmCPUTotalTable from an NMS.

- CSCec85347

  Symptoms: A router may reload unexpectedly because of memory corruption.

  Conditions: This symptom is observed when connection accounting is enabled and when the router is handling a high volume of connections.

  Workaround: Disable connection accounting.

  Further Problem Description: The high-volume condition may occur when there are many users that log into the router (typically via a script) through vty lines and when a race condition occurs in which the router attempts to perform accounting after the connection structures have been freed.

- CSCed88768

  Symptoms: Certain type-7 encrypted forms of passwords may no longer work after a Cisco IOS software upgrade.

  Conditions: This symptom is observed when you upgrade a Cisco router to Cisco IOS Release 12.2(18)S, a later release of Release 12.2S, or a release that is based on Release 12.2(18)S or a later release of Release 12.2S. The symptom occurs when you save a type-7 password that consists of more than four characters.

  Workaround for enable passwords: Configure an “enable” secret in place of the enable password, or in addition to it. An enable secret uses a different encryption mechanism and is not affected by this caveat. When both an enable password and an enable secret are configured, the enable secret takes precedence. You may remove the enable secret after the software upgrade has occurred and when the enable password has been validated or reconfigured.

  Workaround for other passwords than enable: When the software upgrade has occurred, reconfigure the same password as you used before the software upgrade.

  Further Problem Description: If you have a router that runs Cisco IOS Release 12.2(18)S, a later release of Release 12.2S, or a release that is based on Release 12.2(18)S or a later release of Release 12.2S and you upgrade to a release that integrates the fix for this caveat (CSCed88768), copy and paste the corresponding “password 7” cypher lines in configuration mode to the router before you proceed with the software upgrade.

IP Routing Protocols

- CSCec06466

  Symptoms: A Cisco router may reload unexpectedly when the Designated Forwarder (DF) interface is changed to an interface that is already in the Outgoing Interface list (O-list).

  Conditions: This symptom is observed on a Cisco router that is configured for multicast Bidirectional PIM (Bidir-PIM).

  Workaround: There is no workaround.

- CSCec29868

  Symptoms: An Open Shortest Path First version 3 (OSPFv3) adjacency may flap when a standby Route Processor (RP) comes up after a switchover has occurred or after a router has reloaded. The router database may contain duplicate entries of the network link-state advertisement (LSA), or link LSA, or both.

  Conditions: This symptom is observed after a switchover has occurred when the interface number of the interface that is configured for OSPFv3 changes.

  This symptom is also observed after the router has reloaded when the interface number of the interface that is configured for OSPFv3 changes and when the neighbor still has the LSA (that was generated by the router on which the symptom occurs) with the old Link State ID (LSID) in its database. This situation may occur when the router does not clean up its LSA (for example, when the router reloads unexpectedly) or when the interface that connects to the neighbor is shut down before the router reloads and then brought back up after the router has reloaded.

  Workaround: There is no workaround.

- CSCed60800

  Symptoms: The withdraw message of a multipath (not bestpath) from a BGP neighbor deletes the path from the BGP table but it does not uninstall the route from the IP routing table.

  Conditions: This symptom is observed when the **maximum-paths eibgp** command or **maximum-paths ibgp** command is configured along with **soft-reconfiguration inbound**.

  Workaround: Enter the **clear ip bgp *** or disable the **soft-reconfiguration inbound** or disable the **maximum-paths eibgp** command or **maximum-paths ibgp** command.

  Alternate Workaround: Ensure that the number of possible EBGP peers is less or equal to two. In this situation, the symptom is transient and not obviously noticeable.

- CSCsa57101

  Symptoms: A Cisco router may reload when the RSVP MIB object is polled via SNMP.

  Conditions: The symptom is platform- and release-independent.

  Workaround: Disable SNMP by entering the **no snmp-server host** command.

Miscellaneous

- CSCdt51547

  Symptoms: The **ip verify unicast reverse-path** interface configuration command may incorrectly drop a fraction of incoming traffic.

  Conditions: This symptom is observed when packets are received on multiple subinterfaces of an interface and when these subinterfaces are in different VRFs. The symptom is release-independent.

  Workaround: There is no workaround.

Further Problem Description: For Cisco IOS Release 12.2T, there are two parts to the fix and you need to run interim Release 12.2(12.14)T or a later release for the fix to work properly.

- CSCee31450

  Symptoms: IPv6 packets may not be switched via CEFv6 but may be blackholed.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S4 when the packets are switched from an FE interface to a POS interface.

  Workaround: There is no workaround.

- CSCef16022

  Symptoms: A memory block overrun or bus error may occur on a Cisco 7304 when you perform an OIR or change the encapsulation.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S and that is configured with an NPE-G100 under the following conditions:

  – You perform an OIR or change the encapsulation of a native line card that has an interface that is processing traffic.

  – You perform an OIR or change the encapsulation of a carrier card in which a port adapter or SPA is installed that has an interface that is processing traffic.

  – You perform an OIR or change the encapsulation of an SPA that has an interface that is processing traffic.

  Workaround: Stop the traffic before you perform an OIR or change the encapsulation by entering the **shutdown** or the **hw-module slot** *slot-number* **stop** command. When you have performed the OIR or changed the encapsulation, restart the traffic by entering the **no shutdown** or the **hw-module slot** *slot-number* **start** command.

- CSCeg89677

  Symptoms: A Cisco 7304 router may crash when you enter the **clear counters** command.

  Conditions: This symptom is observed when an ATM line card has fatal hardware errors early during its initialization and may occur when the line card is programmed with an incorrect ATM FPGA image, for example, an ATM FPGA image that is not bundled in a Cisco IOS software image.

  Workaround: Ensure that the ATM line card runs an ATM FPGA image that is bundled in a Cisco IOS software image.

- CSCeh14324

  Symptoms: A Cisco 7304 may report assertion failures on the console when its routing peers inject and withdraw overlapped routes. Traffic that is forwarded is not affected in any way.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S and that is configured with an NSE-100 route processor.

  Workaround: Disable the console logging. If this is not an option, there is no workaround.

- CSCeh22026

  Symptoms: The standby RP of a Cisco 7304 that functions in a high-availability mode may reload unexpectedly.

  Conditions: This symptom is observed under various circumstances, one of which is the following:

  The Cisco 7304 is configured with a port adapter carrier card in which a PA-MC-2T3+ port adapter is installed and you enter the **no channelized** command for one of the ports of the port adapter.

Workaround: Do not enter the **no channelized** command for a port of the PA-MC-2T3+ port adapter. Rather, configure the startup configuration to include the **no channelized** command for the port of the PA-MC-2T3+ port adapter.

- CSCeh34645

  Symptoms: When you enter the **match qos-group** *qos-group-value* command on a class that is used by an output policy map may cause a Cisco 7304 router to reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7304 router is configured with an NSE-100 forwarding engine and that runs Cisco IOS Releases 12.2(20)S7 or Releases 12.2(25)S3 when the QoS group is set during input processing (through either the **set qos-group** *qos-group-value* command or the **set-qos-transmit** *qos-group-value* police action).

  Workaround: There is no workaround.

- CSCeh39794

  Symptoms: A QoS service policy does not function.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when you remove a child policy map from a hierarchical policy that is attached to an interface.

  Workaround: Detach the service policy from the interface and re-attach it again.

- CSCeh53449

  Symptoms: A router may seem to hang after you enter the **no shutdown** interface configuration command followed by the **shutdown** interface configuration command on an ATM interface that was previously a member of an IMA group. The router does not really hang and is still capable of routing packets but the EXEC process hangs.

  Conditions: This symptom is observed on a Cisco 7304 that has a PA-CC in which a PA-A3-8E1IMA or PA-A3-8T1IMA port adapter is installed.

  Workaround: There is no workaround.

- CSCeh55923

  Symptoms: A router may crash and generate an assertion-failure error message.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when you apply an hierarchical police map on an interface while traffic is being processed.

  Workaround: Stop traffic before you apply the hierarchical police map.

- CSCsa59126

  Symptoms: CPU-HOG messages may be generated and a router may crash when a large number of entries is configured on a single access control list (ACL).

  Conditions: This symptom is observed on a Cisco router that has IP ACL enabled.

  Workaround: Reduce the number of entries on the ACL.

- CSCsa64426

  Symptoms: A Cisco 7304 may crash and generate an error message that is similar to the following:

  ```
  %NSE100-3-ERRORINTR: Fatal error interrupt. IOFPGA error interrupt statuses:
  Asic/FPGA 0001, Line card 0000, OIR 0000, Envm. 0000
  ```

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

  Workaround: There is no workaround.

- CSCsa72313

  Symptoms: The following error messages may be generated on a router that has IP ACL enabled:

  ```
  %SYS-2-INSCHED: suspend within scheduler
  -Process= "<interrupt level>", ipl= 3 -Traceback= 40525388 40628848 4060AED4 403F15BC
  403F34F8 403F37EC 400901C8 4008E730 406A0EEC 40621120
  ```

  Conditions: This symptom is observed on a Cisco router such as a Cisco 7304, Cisco 7200 series, and Cisco 7500 series when a Turbo ACL compilation is configured along with an ACL on an ingress interface and when traffic passes through the ingress interface. The symptom does not affect the Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsa91159

  Symptoms: A Cisco 7304 series carrier card may run out of memory, may reload, and the following error message may be generated:

  ```
  %PACC-3-HEARTBEAT_LOSS: PA Carrier Card Loss of heartbeat from linecard in slot
  <slot_number>
  ```

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 7300-CC-PA port adapter carrier card in which a PA-2POS-OC3 port adapter is installed when a high rate of egress traffic is processed by the interfaces of the port adapter.

  Workaround: Reduce the rate of egress traffic.

- CSCuk45567

  Symptoms: When you perform a physical online insertion and removal (OIR) of a Route Switch Processor (RSP), the router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series when Routing Information Protocol next generation (RIPng) for IPv6 is configured.

  Workaround: There is no workaround.

- CSCuk47482

  Symptoms: A router may reload unexpectedly while you disable label distribution protocol (LDP) on an interface.

  Conditions: This symptom is observed on a router that has several interfaces that are configured for LDP when you disable LDP on all interfaces and when there is still one open TCP connection that is passively used by LDP while you disable LDP on the last interface.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCea61281

  Symptoms: An HTTP server hangs and returns only a partial page.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(20)S when you configure an HTTP server and request the server page from the browser.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(20)S7

Cisco IOS Release 12.2(20)S7 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S7 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCdz27562

  Symptoms: Executing an snmpwalk command on a loopback interface causes a response that is sourced from the IP address of the physical interface.

  Conditions: This symptom is observed on a Cisco 12000 series but also affects other platforms.

  Workaround: Execute the snmpwalk command on the physical interface.

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial-In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

- CSCed86286

  Symptoms: A router may reload due to a software-forced crash.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.2(13)T5 and that has SSH configured. However, the symptom may occur on other platforms that run other releases and that do not have SSH configured when there are many process messages.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCeb64384

  Symptoms: ATM subinterfaces that are created on an 1-port ATM enhanced OC-3c/STM-1 single mode port adapter (PA-A3-OC3SMI) cause the SNMP agent to malfunction, in turn causing an SNMP getmany command to hang in the ifTable.

  Conditions: This symptom is observed on a Cisco router in which a PA-A3-OC3SMI is installed when you enter an SNMP getmany command in the ifTable.

  Workaround: There is no workaround.

- CSCef00510

  Symptoms: Packets that originate from a Cisco router that is configured with a PA-MC-8TE1+ port adapter may be corrupted and have an invalid FCS. These packets may have the address and control fields compressed even when PFC and ACFC options are explicitly disabled.

  Conditions: This symptom is observed only when traffic is presented simultaneously on several B-channels.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCee59315

  Symptoms: A BGP VPNv4 table may contain paths that may be imported from deleted BGP table entries or from table entries that have a different prefix from the importing prefix.

  An example of a path from a deleted BGP table entry is as follows:

```
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 52
Paths: (1 available, best #1, table vpn2)
  Advertised to non peer-group peers:
  10.4.1.2
  2 100, imported path from 2829:2829:185404173:11.13.11.13/-53
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:3
```

  The entry that this path is imported from has been removed from the table and its memory contents contain an incorrect pattern. When the incorrect pattern is displayed as a prefix, it appear as “2829:2829:185404173:11.13.11.13/-53”.

  A mismatched prefix appears as follows:

```
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 54
Paths: (2 available, best #1, table vpn2)
Flag: 0x820
  Advertised to non peer-group peers:
  10.10.10.10 10.20.20.20
  2
    10.4.1.2 from 10.4.1.2 (10.4.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:2
  2 100, imported path from 200:2:172.16.0.0/24
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external
      Extended Community: RT:1:3
```

  This BGP VPNv4 table entry is for prefix 192.168.0.0/32 but it shows that a path is imported from 172.16.0.0/24. This situation occurs when a path has a link to a deleted BGP table entry, and then the memory for the deleted entry is reused for a new table entry of which the prefix may not match with the importing entry.

Conditions: These symptoms are observed when you enter the **maximum-paths import** *number* command in router BGP address-family IPv4 VRF mode. The *number* argument indicates the number of paths to import from one VRF to another.

Workaround: Remove the **maximum-paths import** *number* command from the router BGP address-family IPv4 VRF mode.

- CSCee89438

  Symptoms: An MSDP enabled RP does not build an (S,G) state from its SA cache when it should do so. Depending on the topology and if an SPT threshold is configured as infinite, this situation may result in a multicast forwarding interruption of up to 2 minutes.

  Conditions: This symptom is observed when the RP for a group fails and an incoming (*,G) join message is received.

  MSDP should create an (S,G) state from its SA cache. However, this is done before the (*,G) olist is populated; because of the (*,G) NULL olist, MSDP does not install an (S,G) state.

  Workaround: Enter the **clear ip mroute *** command on all first-hop routers to the source to enable the FHR to register immediately when the next packet creates an (S,G) state.

- CSCeg54375

  Symptoms: Routing inconsistencies may occur in the RIB: routes may be missing from the RIB but may be present in the BGP table.

  Conditions: This symptom is observed on a Cisco RPM-XF when the toaster processor crashes. However, the symptom may occur on any platform that has a toaster processor.

  Workaround: Enter the **clear ip route vrf** *vrf-name* ***** command.

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP “source quench” messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

ISO CLNS

- CSCec39973

  Symptoms: A router that runs Intermediate System-to-Intermediate System (IS-IS) may reload unexpectedly when there are a lot of adjacencies that continue to flap.

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

  In Release 12.0S, the symptom may occur when you enter the **router isis** global configuration command followed by the **fast-flood** router configuration command.

  In Release 12.3, the symptom may occur when you enter the **router isis** global configuration command followed by the **ip fast-convergence** router configuration command.

  Workarounds: Prevent IS-IS adjacencies from flapping. There is no other workaround for Release 12.2S.

  For Release 12.0S, do not enter the **router isis** global configuration command followed by the **fast-flood** router configuration command.

  For Release 12.3, do not enter the **router isis** global configuration command followed by the **ip fast-convergence** router configuration command.

Miscellaneous

- CSCdz33630

  Symptoms: A standby RP that is in the “Standby HOT” state before a switchover in SSO mode crashes right after the switchover.

  Conditions: This symptom is observed on a Cisco router that has dual RPs and that is configured for SSO, MPLS, and IS-IS as the IGP routing protocol. The symptom occurs only when the router is configured for Layer 2 SSO support and functions in an MPLS network but runs a Cisco IOS image that supports only MPLS SSO coexistence.

  Workaround: There is no workaround.

- CSCdz84448

  Symptoms: Spurious memory accesses may occur on a router, and the router may reboot.

  Conditions: This symptom is observed on a Cisco router when you poll the cbQosREDClassStatsTable of the CISCO-CLASS-BASED-QOS-MIB. The symptom is platform-independent. The spurious memory accesses may be reproduced when polling the above-mentioned table via Simple Network Management Protocol (SNMP).

  Workaround: Prevent the router from answering to queries on the cbQosREDClassStatsTable by implementing the following SNMP view in the router configuration:

  ```
  snmp-server view qos internet included
  snmp-server view qos 1.3.6.1.4.1.9.9.166.1.20.1 excluded
  snmp-server community string view qos ro
  ```

- CSCea76134

  Symptoms: External Border Gateway Protocol (eBGP) multipath load sharing may not use all of the available BGP paths.

  Conditions: This symptom is observed when all of the eBGP routes for the prefix that are affected are locally imported from another VPN routing/forwarding (VRF). As a result, a local label is not associated with the prefix in the imported VRF. This behavior prevents all BGP paths from being used.

Workaround: Have at least one eBGP route for the prefix learned directly from an eBGP peer, instead of importing the route from another VRF. This forces the creation of a local label, and as a result, all BGP paths are used.

- CSCeb52181

  Symptoms: A Cisco platform that accesses the "system:/vfiles/tmstats_ascii" virtual file (for example, via "more system:/vfiles/tmstats_ascii") may crash because of bus error.

  Conditions: This symptom is observed under normal working conditions when no configuration changes are made on a Cisco platform that runs Cisco IOS Release 12.0S, 12.1E, 12.2, 12.2.S or 12.3. When the "system:/vfiles/tmstats_ascii" virtual file is not used, the symptom does not occur.

  Workaround: There is no workaround.

- CSCec07579

  Symptoms: Interface bit-rate counters may not be cleared when they should be cleared.

  Conditions: This symptom is observed on a Cisco router that is configured for quality of service (QoS) when you enter the **clear counters** user EXEC or privileged EXEC command. The QoS bit-rate counters are cleared, but the interface bit-rate counters are not.

  Workaround: There is no workaround. Wait for the next update interval for the bit-rate counters.

- CSCed45698

  Symptoms: Unused ports on a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may flap even when they are not processing any traffic.

  Conditions: This symptom is observed when there is congestion on used ports of the PA-MC-STM-1 and when a committed access rate (CAR) is configured on these used ports.

  Workaround: There is no workaround.

- CSCed52578

  Symptoms: The MPLS packets are forwarded with a bogus label when they are sent out on a loadshared non-VRF MPLS enabled "Internet" interface from a VRF.

  Condition: A static route for the VRF should be configured to reach the Internet, which would in turn be configured to recurse over 2 static routes to reach the next hop for the global Internet.

  Workaround: Shut down one of the interfaces to remove the load-sharing condition.

- CSCed81317

  Symptoms: When an import map is configured on a VPN Routing/Forwarding (VRF) instance, the CE-learned routes are filtered out, preventing them from appearing in the VRF routing table.

  Conditions: This symptom is observed when the **import map** *word* command is configured as part of the VRF configuration. Note that eBGP routes are not filtered out.

  Workaround: There is no workaround.

- CSCee56209

  Symptoms: Access control list (ACL) counters may display twice as many matches as there are in reality.

  Conditions: This symptom is observed when ACL counters are used in policies in which class maps are nested. These counts propagate into the accounting output of the **show policy interface** command, creating the impression that twice as many packets have entered the network and are matched on these ACLs as there are in reality.

  Workaround: There is no workaround.

- CSCee58323

  Symptoms: In a back-to-back MPLS configuration, a Cisco router that functions as a provider edge (PE) router may show the wrong value of the next hop in the NetFlow table and the Parallel Express Forwarding routing table.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S.

  Workarounds: There is no workaround.

- CSCee67207

  Symptoms: A public recursive route is not labeled.

  Conditions: This symptom is observed on a Cisco router that functions as a BGP peer and that has the **neighbor** *name* **send-label** command enabled as part of an IPv4 address family, which is required for Inter-AS configurations. The symptom affects routers that perform MPLS forwarding using ASICs such as some Cisco 7200 series routers, the Cisco 7304, the Cisco 10000 series, the Cisco 12000 series, and the Cisco RPM-XF. (This list may not be exhaustive.)

  Workaround: There is no workaround. Note that the symptom does not occur if the **neighbor** *name* **send-label** command is enabled as part of an IPv4 address family VRF.

- CSCee78118

  Symptoms: A line card or port adapter may crash on an MPLS VPN PE router when the customer-facing interfaces are flapped.

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

  – eBGP is used as the routing protocol between the PE and CE router, the CE router has the **redistribute connected** command enabled in the BGP configuration, and there are multiple eBGP sessions between the PE and CE router.

  – The connected route for the link between the CE and PE router is learned from another PE router via MP-iBGP. For example, the CE router may be dual-homed and may advertise the connected routes to both PE routers.

  The symptom affects routers that perform MPLS forwarding using ASICs such as some Cisco 7200 series routers, the Cisco 7304, the Cisco 10000 series, the Cisco 12000 series, and the Cisco RPM-XF. (This list may not be exhaustive.)

  Workaround: Avoid the above-mentioned conditions. For example, avoid the **redistribute connected** command in the BGP configuration of the CE router.

- CSCee80649

  Symptoms: A Cisco 7304 does not function as a 6PE router.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 only when PXF processing is enabled.

  Workaround: Disable PXF processing by entering the **no ip pxf** global configuration command.

- CSCef29119

  Symptoms: IP fragmentation does not function on an ATM OC-3 interface.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 2-port OC-3 ATM line card when the native ATM OC-3 interface of the line card and the VC are configured with any encapsulation type other than AAL5MUX IP encapsulation.

  Workaround: Use a 7300-PA-CC with a PA-A3 ATM port adapter.

Alternate Workaround: Use the native ATM OC-3 interface of the 2-port OC-3 ATM line card with AAL5MUX IP encapsulation.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef47225

  Symptoms: The output of the **show pxf interfaces** command may show "acl not ready" for subinterfaces on which a service policy is configured.

  Conditions: This symptom is observed on a Cisco 7304 when there are more than 200 subinterfaces on an ATM interface and when a service policy is defined on some of the subinterfaces.

  Workaround: Remove the service policies from the ATM subinterfaces and reapply the service policies. Do this each time after you have reloaded the router.

- CSCef60395

  Symptoms: A TFTP upload or download and a Telnet connection to a Cisco 7304 fail.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for SSO or RPR+ when the router is connected to a device that autonegotiates the speed.

  Workaround: Do not use speed autonegotiation. Rather, configure the native Fast Ethernet port 0 of the router to half duplex and the speed to 100 Mbps.

- CSCef61610

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef67682

  Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

  The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

  This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

  This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

  We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml contain fixes for this issue.

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

- CSCef75735

  Symptoms: An ingress police may not properly mark an exceed or violate action, and double accounting may occur for punted packets in a policy map.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a policy map that contains a **police** command is attached to an ingress interface and when an exceed or violate action is marked.

  Workaround: Disable PXF for a while by entering the **no ip pxf** command until traffic exceeds the configured police rate.

- CSCef87051

  Symptoms: A broadcast or network address ping to a VRF interface via an interface may return the broadcast or network address in an ICMP echo reply packet.

  Conditions: This symptom is observed on a Cisco 7304 that is equipped with an NSE-100, that has PXF enabled, and that has a VPN configured on an interface. The symptom may be platform-independent.

  Workaround: Disable PXF.

- CSCef97142

  Symptoms: The packet rate to a high speed interface is limited to 620 Kpps.

  Conditions: This symptom is observed on a Cisco 7304 when traffic in reverse direction is distributed over thousands of egress VCs.

  Workaround: There is no workaround.

- CSCeg09148

  Symptoms: A Cisco 7304 crashes because of a “TLB Modification Exception.”

  Conditions: This symptom is observed when you remove the active NSE-100 via an OIR from a Cisco 7304 that is configured for HA and that has VLANs configured on the native GE interfaces. The symptom does not occur on a Cisco 7304 that has an NPE-G100 and that is configured for HA.

  Workaround: There is no workaround.

- CSCeg11046

  Symptoms: A Cisco 7304 may fail to pass traffic across dot1q Gigabit Ethernet subinterfaces.

  Conditions: This symptom is observed on a Cisco 7304 with an NSE-100 when the native dot1q subinterface is shut down.

  Workaround: Configure static ARP entries for the remote interfaces that connect to the dot1q subinterfaces on the Cisco 7304.

- CSCeg11281

  Symptoms: A spurious memory access message is displayed when you remove an ATM line card via an OIR.

  Conditions: This symptom is observed on a Cisco 7304 when you perform an OIR of an ATM line card and when there is traffic running on a large number of PVCs on the line card.

  Workaround: Perform a graceful OIR by entering the **hw-module slot** *slot-number* **stop** command before removing the line card.

- CSCeg11358

  Symptoms: A Cisco 7304 crashes when you perform an OIR of a line card or SPA.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when the router receives an "XON" flow control message from the line card or SPA during the OIR.

  Workaround: Enter the **hw-module slot** *slot-number* **stop** command before you perform an OIR of the line card or SPA.

- CSCeg21944

  Symptoms: After an HA switchover while the standby RP comes up, the following error message is generated on the console of the standby RP:

  ```
  %HA-4-NOBUF: Failed to allocate buffer for inter-RP IPC message receive
  ```

  The configurations of the standby RP and active RP are not synchronized.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that is configured for HA.

  Workaround: There is no workaround.

- CSCeg37309

  Symptoms: A Cisco 7304 reloads on receipt of a ping to a local interface.

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

  Workarounds: There is no workaround.

- CSCeg52128

  Symptoms: A router may reload unexpectedly when you remove a service policy.

  Conditions: This symptom is observed when you remove a service policy that contains one or more classes with the **police** command and when there is traffic for these classes. The symptom may occur in either input or output service policies and on any type of interface, physical interface, subinterface, ATM VC, or Frame Relay VC.

  On hardware-accelerated platforms, the symptom occurs only when the service-policy traffic is processed by the main forwarding processor (that is, the RP). The symptom does not occur when the service-policy traffic is hardware-accelerated.

  Workaround: There is no workaround.

- CSCeg53716

  Symptoms: An egress QoS service policy does not function when NAT is configured.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when NAT translation and egress QoS are enabled on an output interface.

  Workaround: There is no workaround.

- CSCeg66023

  Symptoms: A PPPoA virtual-access interface does not come up.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S6 and that is configured with an OC-3 ATM line card or a 7300-PA-CC in which a PA-A3 ATM port adapter is installed.

  Workaround: There is no workaround.

- CSCeg78990

  Symptoms: QoS **match not ip** commands match incorrectly.

Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a class-map configuration contains **match not ip** commands such as the following:

match not ip dscp *dscp*

match not ip precedence *precedence*

match not ip rtp *port*

Workaround: There is no workaround.

- CSCeg86909

  Symptom: A Cisco 7304 reloads unexpectedly when it receives an ICMP packet through a tunnel.

  Condition: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S5 and that has an NSE-100 when the ICMP source address is unknown to the router, that is, the source address is not in the FIB table.

  Workaround: There is no workaround

- CSCeg87041

  Symptoms: A Cisco 7304 may reload continuously during a high-availability switchover or may become unusable when any port of a PA-MC-2T3+ port adapter is configured to operate in the non-channelized mode.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S6 or Release 12.2(25)S2 and that is configured with a port adapter carrier card (7300-CC-PA) in which a PA-MC-2T3+ port adapter is installed. The symptom occurs in both high-availability and non-high-availability configurations.

  Workaround: Do not configure any port of the PA-MC-2T3+ port adapter to operate in the non-channelized mode or enter the **no cdp run** global configuration command on the router.

  Further Problem Description: When CDP is configured globally or on an interface of the PA-MC-2T3+ port adapter that is configured to operate in non-channelized mode, the router stops processing packets.

- CSCeh02678

  Symptoms: Turbo ACL tables may grow so large that the memory they require is larger than the available PXF memory, causing traffic that requires ACL classification to be punted to the RP. If this situation occurs, an error message similar to the following is generated:

  ```
  toaster_acl_init_node: failed index=[dec] type=[dec] table_size=[dec]
  ```

  This message has a logging severity level of 7 (debugging). The output of the **show pxf interfaces** command for any interface with an ACL configured on it shows the "Punting to RP - acl not ready" message.

  If you subsequently enter the **no access-list** *access-list-number* command, the **no ip access-list standard** command, or the **no ip access-list extended** command to delete an ACL from the running configuration, regardless of whether or not the ACL is attached to an interface, and then add one or more ACEs to the ACL that was deleted, any interface that you subsequently attach the ACL to (or that the ACL was already attached to) incorrectly processes this ACL in PXF instead of on the RP. In this case, the ACL processing in PXF occurs by using old Turbo ACL tables that are based on the configuration at the time when the memory that the Turbo ACL tables require first exceeded the available PXF memory.

  Any incoming packets that do not have entries in the Turbo ACL tables because similar packets have not been received previously are punted to the RP, and new entries for these packets are not added to the tables. Such packets continue to be punted to the RP and are processed correctly. Only packets for which entries already exist in the tables in PXF are processed incorrectly in PXF.

Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, ACLs configured, and traffic being switched in PXF.

Workaround: Ensure that all ACLs always contain at least one ACE. If you wish to replace the contents of an ACL with a new set of ACEs, follow these steps:

1. Add a dummy ACE to the ACL; this ACE must differ from all the ACEs in both the existing and the new configurations of the ACL.
2. Remove all ACEs and remarks except the dummy ACE from the ACL. You can do this by loading the configuration of the ACL without the dummy ACE in it into a text editor, placing the **no** keyword before every **permit**, **deny**, or **remark** keyword, and then entering the **copy** *source-url* **system:running-config** command to apply the configuration. For the *source-url* argument, enter the location of the configuration file.
3. Load the new ACL configuration onto the router, possibly by entering the **copy** command again.
4. Remove the dummy ACE from the ACL. Enter the **show pxf interfaces** command to verify that the "Punting to RP - acl not ready" message is shown in the output for the interface in question, indicating that traffic is punted to the RP for correct ACL processing.

- CSCeh17832

  Symptoms: A Cisco 7304 may reload unexpectedly because of a "Fatal Error Interrupt."

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a NSE-100, that runs Cisco IOS Release 12.2(20)S6, that is configured for MPLS, and that has PXF processing enabled. The symptom occurs in a two-way loadbalancing scenario in which one link is a tunnel interface.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(20)S2.

- CSCin84650

  Symptoms: Packets of shaped IP DSCP classes of a policy map may be dropped, causing the output shaping rate to be lower than the configured rate in the policy map.

  Conditions: This symptom is observed on a Cisco 7304 that has a NPE-G100 when an output interface is attached with a policy map that has a shaping configuration for IP DSCP-based classes and when the interface has oversubscribed traffic, including the default class at output.

  Workaround: There is no workaround.

- CSCsa41345

  Symptoms: Packets greater than 4470 bytes are dropped from an ATM OC-3 line card after you have performed an OIR of the line card.

  Conditions: This symptom is observed on a Cisco 7304 when the MTU for the ATM interface of the line card is not the default MTU.

  Workaround: Configure the MTU after you have performed an OIR of the line card.

- CSCsa43143

  Symptoms: A system exception may occur and the router may reload when you apply a service policy for which the aggregate allocated bandwidth exceeds the bandwidth that is available to the policy. The bandwidth that is available to the policy is either the maximum reserved bandwidth value of the interface (the default is 75 percent of interface bandwidth) or the shape rate of a hierarchical policy.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100. The symptom may also occur when any of the following actions occur:

  – You increase the bandwidth of the class.
  – You decrease the maximum reserved bandwidth value of the interface.

  - You decrease the shape rate of the hierarchical policy.
  - You remove the **max-reserved-bandwidth** command such that the aggregate allocated bandwidth exceeds the bandwidth that is available to the policy.

  Note that a service policy for which the aggregate allocated bandwidth exceeds the bandwidth that is available to the policy is an invalid service policy.

  Workaround: There is no workaround.

- CSCsa46132

  Symptoms: A Cisco 7304 router may stop forwarding VPN traffic. IPv4 traffic is not affected.

  Conditions: This symptom is observed on a Cisco 7304 that has a NSE-100 and that runs Cisco IOS Release 12.2(20)S4.

  Workaround: Reload the router.

- CSCsa58566

  Symptoms: MPLS loadbalancing over multiple paths may not be performed in a balanced way.

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

  Workaround: There is no workaround.

- CSCsa58646

  Symptoms: For all interfaces that have MPLS enabled, except the native Gigabit Ethernet interfaces, the byte counters in the output of the **show mpls forwarding-table** command show 6 bytes more per packet than what is actually sent.

  Conditions: This symptom is observed on a Cisco 7304 that has PXF enabled.

  Workaround: There is no workaround.

- CSCsa60671

  Symptoms: Packets that match some access control entries (ACEs) are denied even though the ACEs are configured to permit these packets. Additionally, packets that match these ACEs are counted as implicit deny drops instead of being counted against the relevant ACEs.

  Conditions: This symptom is observed when you configure more than 16382 ACEs on a Cisco 7304 that has an NSE-100.

  Packets that match the affected ACEs cause the “ACL input deny Drop” and “impli. deny Drop” counters that are shown in the output of the **show pxf accounting** command to increase.

  The limit of 16382 ACEs includes all the ACEs that you have configured in your access control lists (ACLs) and any ACEs in internally-generated ACLs. Internal ACLs are generated when you configure QoS classes by entering the **class-map** command.

  You can see how many ACEs are configured on the router by entering the **test c7300 acl** command if the router runs a Cisco IOS release earlier than Release 12.2(25)S or the **test platform acl** command if the router runs Release 12.2(25)S or a later release. In the output of either command, look for the line with the text “name = ACL_REAL_ACE”. The number shown below this line, next to “allocated”, indicates the number of ACEs that are configured, and “max” indicates the maximum number of ACEs that can be configured. If the value shown next to “alloc_failed” is not zero, you have configured too many ACEs.

  Note that the number of “entries” that are shown as configured in the output of the **show access-lists compiled** command includes additional ACEs that are generated internally to account for fragmented packets when the ACEs match on layer 4 values. These ACEs do not count against the

limit of 16382. When you have exceeded this limit, if you unconfigure any ACEs that were configured earlier, it does not cause ACEs that were configured more recently to start functioning correctly.

Workaround: Ensure that all configured ACEs function correctly by changing the ACL configuration to use no more than 16382 ACEs. After you have done so, reload the router to ensure that all configured ACEs function correctly.

- CSCuk51673

  Symptoms: Distributed Cisco Express Forwarding (DCEF) may become disabled and the following error message may appear on the console:

  ```
  %FIB-3-NOMEM: Malloc Failure, disabling DCEF
  %FIB-2-FIBDOWN: CEF has been disabled due to a low memory condition.
  ```

  Conditions: This symptom is observed on a Cisco platform that is configured for DCEF. The occurrence of the symptom depends on how much memory is allocated at runtime.

  Workaround: There is no workaround. After the symptom has occurred, re-enable DCEF by entering the **ip cef distributed** command.

- CSCuk55193

  Symptoms: On a router that runs Cisco IOS Release 12.2S and that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), a configuration change that causes one or more LDP sessions to be terminated may cause the router to reload in a manner similar to the following:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x64, pc=0x41285C40,
  ra=0x41285C30, sp=0x44B1C378
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x64, pc=0x41285C40,
  ra=0x41285C30, sp=0x44B1C378
  TLB (store) exception, CPU signal 10, PC = 0x41285C40
  ```

  The symptom may occur with either LDP or Tag Distribution Protocol (TDP).

  Conditions: This symptom is extremely unlikely to occur and requires a very unlikely timing of events between LDP and TCP. The symptom may occur in the following releases and their rebuilds: Release 12.2(18)S, 12.2(20)S, 12.2(22)S, and 12.2(25)S.

  There are many configuration commands that may trigger the symptom, including entering the **no ip vrf** command to remove a VRF that has LDP-enabled interfaces, entering the **no mpls ldp router-id** command to trigger a change to the LDP router ID, or entering the **no mpls ip** interface configuration command to disable LDP on an interface.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(20)S6

Cisco IOS Release 12.2(20)S6 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S6 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCea36491

  Symptoms: When a Telnet session is made to a router after a VTY session pauses indefinitely, the user in the Telnet session may not be able to enter the configuration mode. When these symptoms occur, interfaces may enter the wedged state with Simple Network Management Protocol (SNMP) traffic.

  Conditions: This behavior is observed on ATM and Packet over SONET (POS) interfaces. This behavior is not platform-specific.

  Workaround: Disable Simple Network Management Protocol (SNMP) configuration traps by entering the **no snmp-server enable traps** config global configuration command.

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

  Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml.

IP Routing Protocols

- CSCeb53542

  Symptoms: An inconsistency between the Cisco Express Forwarding (CEF) table and the Address Resolution Protocol (ARP) table may cause CEF entries to be removed and then recreated at random times. This situation, in turn, may cause unicast packet loss for the affected entry or entries.

  Condition: This symptom is observed only when ARP requests are not answered. ARP and adjacency tables are periodically refreshed independently; this may cause tables to be out of synch until this situation ages out.

  Possible Workaround: Configure the ARP timeout to be 60 seconds or a multiple of 60 seconds. For example, when you enter the **arp timeout 270** interface configuration command, the symptom occurs, but when you enter the **arp timeout 300** interface configuration command, the symptom does not occur.

- CSCec22723

  Symptoms: A router may unexpectedly reload because of a watchdog timeout or bus error in OSPF.

  Conditions: This symptom is observed when iSPF is configured under OSPF.

Workaround: Remove the iSPF configuration from OSPF by entering the **no ispf** command.

- CSCed62901

  Symptoms: This symptom occurs in an OSPF network topology in which a CE router (CE-1) connect to a PE router (PE-1) that connects to two other PE routers (PE- 2 and PE-3), each of which connect to another CE router (CE-2 and CE-3). In turn, both of these CE routers are connected to each other (that is, CE-2 and CE-3 connect to each other).

  When the link between the PE-3 and the CE-3 flaps, the OSPF route in the VRF fails to switch back from BGP to OSPF on the PE-1.

  Conditions: This symptom is observed in Cisco IOS Release 12.0 S, 12.2 S, and 12.3 T.

  Workaround: Clear the ip route, clear the OSPF process, or enter the **clear ip bgp *** command on the PE-1 to bring the route back from BGP to OSPF.

- CSCef19137

  Symptoms: There are duplicate entries in the flow cache after an interface bounces, causing packet loss. The output of the **show ip cache flow** command may show information similar to the following:

```
SrcIf      SrcIPaddress    DstIf    DstIPaddress    Pr SrcP DstP      Pkts
Gi0/0.1    10.2.0.1        Fa2/0    10.3.0.1        06 2C26 00B3      5
Gi0/0      10.2.0.1        Null     10.3.0.1        06 2C26 00B3<<<<  7
```

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that runs Cisco IOS Release 12.2(20)S4 when an interface bounces quickly and when the CEF structures are flushed while the ARP cache is not flushed. This situation causes incomplete adjacencies because the CEF process expects a fresh ARP entry to complete its adjacency.

  Workaround: Clear the ARP cache or enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

ISO CLNS

- CSCed96062

  Symptoms: A router that runs IPv6 on IS-IS may reload.

  Conditions: This symptom is observed when you enable and disable the **ipv6 router isis** command.

  Workaround: There is no workaround.

Miscellaneous

- CSCea65827

  Symptoms: A Cisco router performing MPLS label imposition on IPv4 traffic may reload.

  Conditions: This symptom is observed when the router attempts to forward traffic to a destination via a route that is newly learned, when the router forwards traffic via Cisco IOS software (that is, not via hardware acceleration), and when one of the following conditions is present:

  - There are multiple routes to the destination.
  - The **ip cef accounting non-recursive** command is enabled.
  - CEF does not install a “cached adjacency” (as seen in the output of the **show ip cef** *prefix* command.)

The symptom affects the following Cisco IOS releases:

- Releases later than Release 12.0(22)S.
- Release 12.1T and a special XT-release that is based on 12.1T.
- Release earlier than Release 12.2S.
- Releases later than Release 12.2(2)T.
- Release 12.3.

The symptom does not affect the following Cisco IOS releases:

- Release 12.1E
- Release 12.2M

Possible Workaround: Avoid conditions that prevent a "valid cached adjacency" from being installed.

- CSCeb88239

  Symptoms: A router that runs RIPng may crash after receiving a malformed RIPng packet, causing a Denial of Service (DoS) on the device.

  Conditions: This symptom is observed when the **ipv6 debug rip** command is enabled on the router. Malformed packets can normally be sent locally. However, when the **ipv6 debug rip** command is enabled, the crash can also be triggered remotely. Note that RIP for IPv4 is not affected by this vulnerability.

  Workaround: There is no workaround.

- CSCec10116

  Symptoms: An MPLS VPN PE router uses a source address from its global routing table for some packets that originate in one of its VRF interfaces.

  Conditions: This symptom is observed when an MPLS VPN PE router replies to an ICMP Echo Request that was sent from a VRF interface of another router via the MPLS backbone to the network or broadcast address of the VRF interface on the MPLS VPN PE router.

  Workaround: There is no workaround.

- CSCec81075

  Symptoms: You may be unable to pass traffic between an E3 interface on a Cisco 7304 router and an E3/T3 interface on a Cisco 10000 series router.

  Conditions: This problem is seen when using the default DSU mode and the minimum bandwidth.

  Workaround: Use another DSU mode, or set the bandwidth to something other than the minimum allowed.

- CSCed77033

  Symptoms: A router may reload when you enter the **show glbp** privileged EXEC command.

  Conditions: This symptom is observed when routers are added or removed from the Gateway Load Balancing Protocol (GLBP) group membership while you enter the **show glbp** privileged EXEC command.

  Workaround: Do not enter the **show glbp** privileged EXEC command while routers are added or removed from the GLBP group membership.

- CSCee52430

  Symptoms: The Parallel Express Forwarding (PXF) processor of a Network Service Engine (NSE-100) may not store the proper interface number value in its special routing table when the route is learned via a port adapter that is installed in a 7300-CC-PA.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S, that functions as a provider edge (PE) router, and that has Parallel Express Forwarding (PXF) enabled.

  Workaround: Thee is no workaround.

- CSCee81907

  Symptoms: When OAM traffic is received from a pseudowire, the traffic is not properly fast-switched to the attachment circuit (AC) and is instead dropped, potentially causing spurious memory accesses or crashes.

  Conditions: This symptom is observed when you configure ATM over MPLS on a Cisco 7304 that functions as a provider edge (PE) router with the AC on an ATM line card or an IMA port adapter that is installed in a 7300-CC-PA.

  Workaround: Enable the **oam-ac emulation-enable** command on the Cisco 7304 and the other PE router. With OAM emulation enabled, OAM packets are no longer fast-switched through the router but are processed and generated locally. Alternatively, OAM can be disabled on the customer edge (CE) routers.

- CSCee89877

  Symptom: A Cisco 7304 with a Network Services Engine 100 (NSE-100) may drop MPLS packets.

  Conditions: This symptom is observed when the **mpls ldp explict-null** command is configured on the NSE-100.

  Workaround: Enter the **no mpls ldp explict-null** command on the NSE-100.

- CSCef11032

  Symptoms: When a Cisco 7304 is configured with a port adapter carrier card (7300-CC-PA) with hardware revision 1.2 or 1.3, packet loss and delays may occur. Specifically, when a packet with a size that is larger than about 200 bytes is received by a port adapter that is installed in the 7300-CC-PA, the packet may not be detected and received immediately. In this situation, the packet is not processed until another packet is received. Egress traffic from the Cisco 7304 is not affected. The symptom occurs for any traffic stream that enters on an affected port adapter, regardless of whether or not the traffic stream terminates on the Cisco 7304.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a PA-POS-OC3, PA-A3-E3, PA-A3-T3, or PA-A3-OC3 port adapter. The symptom is not observed with other port adapters. You can check the hardware revision of a 7300-CC-PA by entering the **show diag** *slot-number* command.

  Workaround: There is no workaround.

- CSCef17600

  Symptoms: Labeled packets that arrive on Gigabit Ethernet port 1, 2, or 3 of a Cisco 7304 may be process-switched.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a NPE-G100 and that functions as an MPLS PE router.

  Workaround: There is no workaround.

- CSCef21562

  Symptoms: VC-based queuing via Frame Relay traffic shaping with a service policy that is attached in a map class does not function as expected.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100 and that runs Cisco IOS Release 12.2(20)S1 or a later rebuild.

  Workaround: There is no workaround.

- CSCef26774

  Symptoms: When OAM traffic is received from a pseudowire, the traffic is not properly fast-switched to the attachment circuit (AC) and is instead dropped, potentially causing spurious memory accesses or crashes.

  Conditions: This symptom is observed when you configure ATM over MPLS on a Cisco 7304 that functions as a provider edge (PE) router with the AC on a non-IMA port adapter that is installed in a 7300-CC-PA.

  Workaround: Enable the **oam-ac emulation-enable** command on the Cisco 7304 and the other PE router. With OAM emulation enabled, OAM packets are no longer fast-switched through the router but are processed and generated locally. Alternatively, OAM can be disabled on the customer edge (CE) routers.

- CSCef30174

  Symptoms: An FPGA error (%Error: CI TX FPGA, status: 0x00000010) may occur on a Cisco 7304 that is configured with an NSE-100, causing packets to be black- holed when they pass through a traffic engineering tunnel.

  Conditions: This symptom is observed when you attempt to engineer traffic within the core, that is, when an MPLS TE tunnel originates and terminates on provider (P) routers.

  Workaround: There is no workaround.

- CSCef32253

  Symptoms: Route updates to the PXF shadow structures may cause a CPU hog condition when load-balancing is enabled.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that has PXF enabled.

  Workaround: Remove the load-balancing paths.

- CSCef34844

  Symptoms: There may be a flood of assertion messages on the RP console when links flap in an MPLS VPN network.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that has PXF enabled.

  Workaround: Turn off console logging.

- CSCef35906

  Symptoms: Some QoS configuration commands may not be accepted by a router.

  Conditions: This symptom is observed on a Cisco 7304 when high availability is configured with RPR+ or SSO and when the active RP sends QoS configuration changes to the standby RP.

  Workaround: Load only one RP, configure the QoS parameters, write the configuration to the startup configuration, and bring up the standby RP.

- CSCef36850

  Symptoms: A service policy stops working on 2-port GE SPA.

  Conditions: This symptom is observed on a Cisco 7304 after a graceful OIR has occurred.

  Workaround: Reapply the service policy.

- CSCef37186

  Symptoms: The Simple Network Management Protocol (SNMP) agent may use 99 percent of the CPU bandwidth of a Route Processor (RP) for an arbitrarily long time, possibly generating CPUHOG errors and causing a watchdog crash. Other processes on the router may fail because these processes do not receive the CPU bandwidth that they require. Consequently, the following difficulties may occur:

  - Routes may time out.
  - Tunnels may go down.
  - Accessing the router via a Telnet connection to a network port may become impossible.
  - The command-line interface (CLI) via the console line may become quite slow to respond.

  The output of the **show snmp summary** EXEC command may indicate that the number of requests is "N" while the number of replies that were sent is "N-1." The output of the **show processes cpu | include SN** EXEC command may indicate that the SNMP process uses 99 percent of the CPU bandwidth of the RP.

  Conditions: These symptoms are observed on a Cisco 7300 series when the MPLS-LSR-MIB MIB is enabled, when you query the object mplsXCIndexNext, and when there are more than 1,000 Multiprotocol Label Switching (MPLS) labels active. However, the symptoms are platform-independent.

  Workaround: Perform the following steps:

  1. Shut down interfaces to bring the total count of active MPLS labels down to far below 1,000.
  2. Disable the MPLS-LSR-MIB MIB by entering the following sequence of commands:

     ```
     snmp-server view nolsrmib mplsLsrMIB exclude
     snmp-server view nolsrmib iso include
     ```

  3. Modify each defined community string to include the **view nolsrmib** keywords. For example, define the "public" community string by entering the following command:

     ```
     snmp-server community public view nolsrmib ro
     ```

  4. Enter the **no shutdown** interface configuration command on all the interfaces that you shut down in Step 1.

- CSCef38300

  Symptoms: A %SYS-2-CHUNKBOUNDSIB error message and a traceback may be generated.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a misconfigured policy-map is attached to an interface and is rejected. The error message and traceback are generated at the next QoS configuration change.

  Workaround: There is no workaround.

- CSCef38488

  Symptoms: The standby RP may crash when you unconfigure a service policy and other IP parameters on an ATM main interface.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for HA.

Workaround: There is no workaround. However, the only impact is a short interruption in HA. The active RP remains up; wait for the standby RP to come up again.

- CSCef46605

  Symptoms: Traffic is corrupted when a Gigabit Ethernet (GE) subinterface is configured for native dot1Q encapsulation via the **encapsulation dot1q** *vlan-id* **native**.

  Conditions: This symptom is observed on a Cisco 7304.

  Workaround: Remove the **native** keyword from the GE subinterface configuration on the Cisco 7304.

- CSCef47219

  Symptoms: A Cisco 7304 may reload unexpectedly during a stateful switchover.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a port adapter carrier card (7300-CC-PA) in which a PA-2T3+ port adapter is installed when both T3 controllers are configured to operate in the non-channelized mode.

  Workaround: Use only port 0 or do not use port 1 in non-channelized mode.

- CSCef47725

  Symptoms: When you add or modify a large ACL, a CPU hog condition may occur:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
  (0/0),process = TurboACL.
  -Traceback= 405BD480 4035AFA0 4035C89C 4035D558
  %SYS-5-CONFIG_I: Configured from console by console
  ```

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

  Workaround: There is no workaround.

- CSCef55698

  Symptoms: Loadbalancing between IP and MPLS VPN does not function on a Cisco 7304.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that has PXF switching enabled.

  Workaround: Disable PXF switching.

- CSCef62475

  Symptoms: QoS does not function.

  Conditions: This symptom is observed on a Cisco 7304 that runs a Cisco IOS Release that includes the fix for CSCee84307. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl? bugid=CSCee84307. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCef65426

  Symptoms: A memory leak may occur in the "Per-second Jobs" process on an interface that is configured for QoS.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine (NSE-100) when QoS is configured. The memory leak occurs during the graceful OIR of a line card while QoS traffic is running.

  Workaround: There is no workaround.

- CSCef73591

  Symptoms: When a VLAN with dot1q encapsulation is switched to a native VLAN, the connectivity fails.

  Conditions: This symptom is observed when the VLAN was previously configured for dot1q and then switched to native.

  Workaround: Remove the subinterface on which the VLAN is configured and reapply the configuration.

- CSCef80425

  Symptoms: A Cisco 7304 that reboots may crash.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 when there is an input service policy and traffic continues to run during the reboot.

  Workaround: There is no workaround.

- CSCef80583

  Symptoms: A bus error may occur on a Cisco 7304 that is configured with a carrier card in which a PA-MC-STM-1SMI is installed.

  Conditions: This symptom is observed when a FIB entry is updated in a network that is enabled for load-balancing and occurs because of a timing issue.

  Workaround: There is no workaround.

- CSCef83911

  Symptoms: The QoS statistic are not updated.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when any of the following actions occur:

  - You attach a policy map to a Frame Relay encapsulation subinterface and reload the router.
  - You attach a policy map to a newly-created Frame Relay encapsulation subinterface.
  - You attach a policy map to a newly created VLAN subinterface before encapsulation is configured on this VLAN subinterface.

  The following is a configuration example for a VLAN subinterface:

  ```
  Router(config)# interface GigabitEthernet 0/0.1
  Router(config-subif)# service-policy output aaa
  Router(config-subif)# encapsulation dot1Q 100
  ```

  Workaround: Detach and reattach the service policy to the subinterface.

- CSCef84453

  Symptoms: When traffic passes through an MPLS TE tunnel, PXF sends packets with incorrect tags, causing communication problems.

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

  Workaround: Disable PXF by entering the **no ip pxf** command. Ensure that you understand the impact of this command prior to applying it: the command causes all traffic to be switched by the RP and, depending on the traffic load on the router, may cause high CPU utilization.

- CSCef88153

  Symptoms: A carrier card in which a PA-MC-STM1 is installed may crash.

Conditions: This symptom is observed on a Cisco 7304 after the carrier card has functioned for about one hour.

Workaround: There is no workaround.

- CSCef89230

  Symptoms: An ATM OC-3 line card crashes when you perform a soft OIR.

  Conditions: This symptom is observed on a Cisco 7304 when the ATM OC-3 line card has an active SVC.

  Workaround: There is no workaround.

- CSCef93083

  Symptoms: A CPU hog condition may occur on a Cisco 7304 after BGP adjacency changes:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
  (3/3),process = Per-Second Jobs.
  -Traceback= 40029318 4002BB44 411654CC 41164028 411640BC 410627AC 41164120
  405935C8 40539A4C 405937A0 405588A8 405594D8 404D8DD4 404501AC
  ```

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S5, that is configured with an NSE-100, that functions as a PE router, and that has PXF enabled.

  Workaround: There is no workaround.

- CSCef93104

  Symptoms: After OSPF flaps, a CPU hog condition may occur on a Cisco 7304 that is subjected to stress traffic.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S5, that is configured with an NSE-100, that functions as a PE router, and that has PXF enabled.

  Workaround: There is no workaround.

- CSCef94319

  Symptoms: After links flap, a Cisco 7304 that is subjected to stress traffic may crash.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S5, that is configured with an NSE-100, that functions as a PE router, and that has PXF enabled.

  Workaround: There is no workaround.

- CSCef96635

  Symptoms: A Cisco 7304 may crash with a Redzone corruption.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100 board when you enter multiple times the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a dot1q VLAN subinterface that receives MPLS packets.

  Workaround: There is no workaround.

- CSCeg14930

  Symptoms: After GRE decapsulation, an FIB lookup of an inner packet mail fail, the PXF engine may punt the packet to the RP, and the router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7304 when the route for the inner packet does not exist.

  Workaround: There is no workaround.

- CSCin83244

  Symptoms: VC-based queuing via Frame Relay traffic shaping with a service policy that is attached in a map class does not function as expected.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NPE-G100 and that runs Cisco IOS Release 12.2(20)S1 or a later release when the map class is applied to the PA-CC interface.

  Workaround: There is no workaround.

- CSCuk45501

  Symptoms: A route reflector (RR) may fail to change the nexthop for all iBGP prefixes that are advertised to the RR clients.

  Conditions: This symptom is observed when an outbound route map is used to change the nexthop of prefixes that are advertised to RR clients.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Resolved Caveats—Cisco IOS Release 12.2(20)S5

Cisco IOS Release 12.2(20)S5 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S5 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCds33629

  Symptoms: Closing an existing Telnet session may cause a router to crash.

  Conditions: This symptom is platform-independent.

  Workaround: There is no workaround.

- CSCee58479

  Symptoms: When you configure an interface of a PA-MC-8TE1 on a Cisco 7200 series, the router to which the interface of the PA-MC-8TE1 is connected at the other end may crash.

  Conditions: This symptom is observed when the interface of the PA-MC-8TE1 functions in channelization mode and when CDP is enabled.

  Workaround: Disable CDP globally by entering the **no cdp run** global configuration command or by entering the **no cdp enable** interface configuration command on the interface of the router to which the PA-MC-8TE1 interface is connected at the other end.

IP Routing Protocols

- CSCea59206

  Symptoms: When you configure the **distribute-list** router configuration command under the **address-family ipv4 vrf** *vrf name* router configuration command, the **distribute-list** router configuration command may appear under the main routing process as may be displayed in the output of the **show running-config** EXEC command.

  Conditions: This symptom is observed in either a Routing Information Protocol version 2 (RIPv2) or a Border Gateway Protocol (BGP) configuration when you specify the *interface-type* and *interface-number* arguments of the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} [*interface-type interface-number*] router configuration command.

  The symptom does not occur when you do not define the *interface-type* and *interface-number* arguments and only enter the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} router configuration command.

  Workaround: There is no workaround.

Miscellaneous

- CSCec64382

  Symptoms: You may not be able to send traffic through an IPv6-to-IPv4 (6to4) tunnel, but you may be able to receive traffic through this tunnel.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2 S or Release 12.3 when the interface on which the tunnel is configured flaps.

  Workaround: There is no workaround.

- CSCed37615

  Symptoms: A router may reload unexpectedly after renaming a policy-map the second time.

  Conditions: This defect may be observed if there are at least two policies configured.

  Workaround: Avoid renaming the policy-map.

- CSCed40526

  Symptoms: Open Shortest Path First (OSPF) flood reduction may not function correctly. The DoNotAge (DNA) bit may be set even though the content of the OSPF summary link-state advertisement (LSA) does not change.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(22)S but may also occur in other 12.2 S releases.

  Workaround: There is no workaround.

- CSCed45942

  Symptoms: A router with a configuration size that is larger than the NVRAM size reloads because of a bus error and stack overflow or stack corruption when you enter the **show config** command simultaneously with the **write terminal** or **show running-config** command.

  Conditions: This symptom is observed when the **service compress-config** command or **boot config** command is enabled.

  Workaround: Do not enter the above-mentioned commands simultaneously, reduce the size of the configuration, or increase the size of the NVRAM.

  Further Problem Description: This problem was introduced in Cisco IOS Release 12.1(8a)E1, so most Cisco IOS 12.1 E releases are exposed to this problem. The problem may also occur in Release 12.2 S.

- CSCed54639

  Symptoms: A Cisco 7304 that has a Network Services Engine 100 (NSE-100) and that is configured for VLAN over MPLS may not have basic connectivity.

  Conditions: This symptom is observed when the VLAN over MPLS configuration runs in a back-to-back scenario. The symptom does not occur on a router that is connected through a core router.

  Workaround: There is no workaround.

- CSCed93286

  Symptoms: A Cisco 7304 that has a Network Services Engine-100 (NSE-100) may punt packets to the Route Processor (RP) even though PXF is enabled.

  Conditions: This symptom is observed when the output features are changed on the RP but not updated for interfaces that are configured for either MPLS or AToM. Then, when the router is booted with PXF disabled and you enable PXF, the router continues to punt MPLS and AToM packets to the RP.

  Workaround: Boot the router with PXF enabled.

- CSCee12235

  Symptoms: A Cisco platform reloads because of a watchdog timer expiration.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(20)S2 or Release 12.3 under the following conditions:

- A service policy (“A”) is attached to an ATM PVC.
- Policy-map “A” is renamed to “B”.
- Service policy “B” is attached to the ATM PVC.

Workaround: First detach the service policy from the PVC, then rename it and attach it again.

- CSCee45154

  Symptoms: Class queues do not receive their expected bandwidths.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a policy map is attached to the subrate E3 or T3 interface of a clear-channel port adaptor. The symptom is not observed on native line cards, nor on PA-MC-E3 or PA-MC-T3 port adapters.

  Workaround: There is no workaround.

- CSCee49465

  Symptoms: A PA-MC-2T3+ in a PA-CC on a Cisco 7304 that is configured with an NSE-100 may fail to switch traffic via PXF and may switch all traffic via process switching.

  Conditions: This symptom is observed when the PA-MC-2T3+ has the **no channelized** command enabled.

  Workaround: There is no workaround.

- CSCee61519

  Symptoms: A NetFlow entry may disappear when there are WRED drop packets.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 when NetFlow is configured on the input interface and WRED is configured on the output interface.

  Workaround: There is no workaround.

- CSCee77410

  Symptoms: The following symptoms may occur on a Cisco 7304:

  - The router may reload when the tunnel source is specified by an interface name instead of an IP address.
  - The router may reload when PXF successively switches through a GRE tunnel.
  - VRF-aware GRE does not function for some ingress or egress interfaces.
  - PXF fails to forward packets after the packets have been encapsulated for GRE.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100 and that is configured for GRE.

  Workaround: There is no workaround.

- CSCee86997

  Symptoms: A Cisco 7304 may generate memory alignment errors, which can be observed in the output of the **show align** command in which the “Initial Address” is in the range of 0x0D0D0D0D to 0x0D0DFFFF. These alignment errors indicate that the router attempts to utilize free memory and may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 with 512 MB of memory when a process attempts to read from or write to freed memory. A list of the affected releases can be found at

http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb12116. Cisco IOS software releases not listed in the "First Fixed-in Version" field at this location are not affected. The symptom may also occur on a Cisco 7304 that has an NPE-G100 with 512 MB of memory.

Workaround: Use a NSE-100 or NPE-G100 with less than 512 MB of memory.

- CSCee95041

  Symptoms: A Cisco 7304 may crash when you send traffic over an EoMPLS VC.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 when traffic flows over an EoMPLS VC using the PXF processor on the NSE-100.

  Workaround: There is no workaround.

- CSCef08376

  Symptoms: When OSPF is configured on POS interfaces that are connected back-to-back, the adjacency does not come up and remains in the "EXSTART" or "DOWN" state. Debugs show many retransmissions from both sides.

  Conditions: This symptom is observed on POS interfaces of a 2-port OC-12 POS port adapter that is installed in a Cisco 7304 that runs Cisco IOS Release 12.2(20)S4.

  Workaround: Either apply or remove the bandwidth statement on both interfaces.

- CSCef11954

  Symptoms: A Turbo ACL may misclassify packets, impacting ACL security and QoS.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(20)S3 or Release 12.2(20)S4.

  Workaround: There is no workaround.

- CSCef13257

  Symptoms: When a policy map is attached to multiple interfaces and you attempt to attach the same policy map to an additional interface that rejects the policy map, the QoS functionality may stop working properly on some of the other interfaces that use the same policy map.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when PXF is enabled.

  Workaround: Detach the policy map from all interfaces and reattach the policy map to all interfaces.

- CSCef16070

  Symptoms: ACL functionality and WRED counters do not function together.

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

  Workaround: There is no workaround.

- CSCef16529

  Symptoms: A Gigabit Ethernet subinterface that is configured for EoMPLS in VLAN mode does not forward traffic when another Gigabit Ethernet subinterface has a native VLAN configuration.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(20)S4.

  Workaround: There is no workaround.

- CSCef25723

  Symptoms: When the **ip pxf qos-statistics** command is enabled and an egress service policy is configured, the following error message may be generated and the QoS statistics may be incorrect:

  ```
  %NSE100-3-VA_ERROR: Vanallen ASIC detected an error condition: TIC invalid DMA length.
  ```

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

  Workaround: There is no workaround.

- CSCef31151

  Symptoms: After you reload a router, a service policy on an interface that is configured for Frame Relay encapsulation fails to function correctly.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 forwarding engine and that has PXF enabled when the service policy is configured on the main interface. (The symptom does not occur when a service policy is configured on a subinterface.)

  Workaround: After the router has reloaded, detach and reattach the service policy.

- CSCef34636

  Symptoms: Hierarchical policing does not function.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when you attach a two-level policy map and when policing is enabled on both the parent policy map and the child policy map. A configuration example follows:

  ```
  policy-map child
     class c1
       (other actions)
       police action
     (other class)
  policy-map parent
     class p1
       (other actions)
       service-policy child
     class p2(or class-default)
       (other actions)
       police action
  ```

  Workaround: There is no workaround.

- CSCef34847

  Symptoms: When you enter the **shutdown** command followed by the **no shutdown** command on an interface that has a service policy with WRED, WRED stops functioning and egress packets are dropped.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 forwarding engine.

  Workaround: Reapply the service policy to the interface.

- CSCef37313

  Symptoms: After a router reloads, a service policy that is enabled on an interface that is configured for PPP encapsulation may fail to function correctly.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that has PXF enabled.

  Workaround: Detach and reattach the service policy.

Resolved Caveats—Cisco IOS Release 12.2(20)S4

Cisco IOS Release 12.2(20)S4 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S4 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCin67568

  Symptoms: A Cisco device experiences a memory leak in the CDP process.

  Conditions: The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

  Workaround: Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the global command **no cdp run**.

Miscellaneous

- CSCed22837

  Symptoms: A router may reload unexpectedly when packets are tag switched.

  Conditions: This symptom is observed when a Bridge-Group Virtual Interface (BVI) is created after the router has booted up, when IP packets are received through the BVI, and when these IP packets are forwarded as Multiprotocol Label Switching (MPLS) packets through another interface.

  Workaround: Disable tag switching on the BVI interface by entering the **tag-switching ip** interface configuration command followed by the **no tag-switching ip** interface configuration command.

- CSCed45746

  Symptoms: Several prefixes for nonredistributed and connected interfaces in different VRFs may be partially bound to the same MPLS VPN label, causing traffic that is bound for one or more of these VRFs to be disrupted.

  Conditions: This symptom is observed on a Cisco router after the VRF interfaces have flapped.

  Workaround: Clear the routes in the VRFs in sequence.

- CSCed70694

  Symptoms: When you enter the **address-family** subcommand under the **router bgp** command, spurious error messages may be generated by the parser. However, when this situation occurs, the command is processed correctly, is "nvgened" correctly, and the output of the **show running-config** command shows that the commands were entered correctly.

  The symptom may also occur with commands for other protocols such as IS-IS and OSPF.

  However, when the symptom occurs, the functionality of the system is not affected.

  Conditions: This symptom is observed on a Cisco platform with redundant route processors.

  Workaround: There is no workaround.

- CSCee08880

  Symptoms: EoMPLS configured on a 3-port Gigabit Ethernet line card may fail when CEF is disabled.

  Conditions: This symptom is observed on Cisco 12000 series that runs Cisco IOS Release 12.0(23)S6. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCee09083

  Symptoms: Artificially crafted, very short packets may be punted continuously to the RP due to a "classify-miss" reason, even if all the packets are identical.

  Conditions: This symptom is observed on a Cisco 7304.

  Workaround: There is no workaround.

- CSCee15798

  Symptoms: After an SSO switchover or when a line card reloads, routes may be deleted from the CEF forwarding tables on the line cards.

  Conditions: This symptom is observed when a large number of recursive routes is configured and when an SSO switchover occurs. NDB updates from the routing protocols may not be downloaded to the line cards if they are received while a line card is downloading.

  Workaround: Clear the line cards and reload the full CEF forwarding database by entering the **clear cef linecard** command after the routing protocols have converged.

- CSCee23517

  Symptoms: The CEF tables on line cards or standby RPs may miss prefixes that are present in the CEF table on the active RP.

  Condition: This symptom is observed on a Cisco platform that is a distributed system (for example, on a Cisco 7500 series).

  Workaround: Enter the **clear cef linecard** command.

- CSCee48821

  Symptoms: For VLAN-over-MPLS circuits, a router may silently ignore all Ethernet packets that are destined for an Ethernet multicast address.

  Conditions: This symptom is observed when an Ethernet port is not configured to receive multicast packets. The symptom does not occur when a protocol such as CDP uses multicast addresses.

  Workaround: There is no workaround.

- CSCee50294

  Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml.

  There are multiple workarounds for this issue:

  There are four possible workarounds for this vulnerability:

  - Disabling the dhcp service
  - Control Plane Policing
  - Two versions of Access Control Lists

a. Disabling the DHCP Service

This vulnerability can be mitigated by utilizing the command:

no service dhcp

However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

b. Control Plane Policing Feature

The Control Plane Policy feature may be used to mitigate this vulnerability, as in the following example:

```
access-list 140 deny   udp host 192.168.13.1 any eq bootps
access-list 140 deny   udp any host 192.168.13.1 eq bootps
access-list 140 deny   udp any host 255.255.255.255 eq bootps
access-list 140 permit udp any any eq bootps
class-map match-all bootps-class
  match access-group 140
policy-map control-plane-policy
  class bootps-class
police 8000 1500 1500 conform-action drop exceed-action drop
control-plane
 service-policy input control-plane-policy
```

For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afad4.html.

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

c. Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address 192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
access-list 100 remark permit bootps from the DHCP server
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 remark deny bootps from any to router f1/0
access-list 100 deny   udp any host 10.89.236.147 eq bootps
access-list 100 remark deny bootps from any to router f0/0
access-list 100 deny   udp any host 192.168.13.2 eq bootps
access-list 100 remark deny bootps from any to router loopback1
access-list 100 deny   udp any host 192.168.61.1 eq bootps
access-list 100 remark permit all other traffic
access-list 100 permit ip any any
```

access-list 100 is applied to f0/0 and f1/0 physical interfaces.

```
interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

An alternate configuration for the interface access-list workaround.

This example would also need to be applied to all physical interfaces, but deny statements for all of the IP addresses configured on the router are not necessary in this approach. In this example, the address 192.168.13.1 represents a legitimate DHCP server.

```
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 permit udp any host 192.168.13.1 eq bootps
access-list 100 permit udp any host 255.255.255.255 eq bootps
access-list 100 deny   udp any any eq bootps

interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

- CSCee51721

  Symptoms: A memory leak may occur on a Port Adapter Carrier Card when you enter any of the following commands:

  - **show diag**
  - **show diag** *slot-number* (enter the slot in which the carrier card is placed for the *slot-number* argument)
  - **show tech-support**
  - **show controller** *controller-number* (enter the controller of the carrier card for the *slot-number* argument)
  - **show controllers**

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S1.

  Workaround: Avoid using any of the above-mentioned commands.

- CSCee60802

  Symptoms: A Cisco 7304 Port Adapter Carrier Card (7300-CC-PA) may lock up, and you may see the following error message:

  ```
  %PACC-3-HEARTBEAT_LOSS: PA Carrier Card Loss of heartbeat from linecard in slot <slot>
  ```

  Conditions: This symptom seems more likely to occur on a 7300-CC-PA with hardware revision 1.0 than on a 7300-CC-PA with a more recent hardware revision. To see the hardware revision of the 7300-CC-PA, enter **show diag** *slot* command.

Workaround: There is no workaround.

- CSCee78924

  Symptoms: A Cisco 7304 reloads with an unexpected exception error, and the following message is logged before the crash occurs:

  ```
  NSE100-3-ERRORINTR: Fatal error interrupt
  ```

  Conditions: The symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that runs Cisco IOS Release 12.2(20)S3 when an access control list (ACL) is applied to an interface or when an existing ACL is modified on an interface.

  Workaround: There is no workaround.

- CSCee82934

  Symptoms: The Parallel Express Forwarding (PXF) processor on a Cisco 7304 may punt the traffic to the RP for recursive IP routes if loadbalancing is triggered.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S, that functions as a provider edge (PE) router, and that has PXF enabled.

  Workaround: There is no workaround.

- CSCuk46249

  Symptoms: The **debug ipv6 cef** command is not accepted.

  Conditions: This symptom is observed in Cisco IOS Release 12.2 S and is platform-independent.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(20)S3

Cisco IOS Release 12.2(20)S3 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S3 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCee28796

  Symptoms: A Cisco 7304 may crash due to low I/O memory as a result of an IPC storm associated with writing the CDP multicast address to an Ethernet MAC filter.

  Conditions: This symptom is only observed on Cisco 7304 with an Ethernet, Fast Ethernet, or Gigabit Ethernet port adapter.

  Workaround: If CDP is not required for network management (SNMP), enter the **no cdp run** command in the startup configuration.

  If CDP is required for network management (SNMP), enter the **no cdp enable** command on each interface and subinterface in the startup configuration, except for the management interfaces and subinterfaces. (There is a maximum of 10 management interfaces and subinterfaces.)

IP Routing Protocols

- CSCdy26197

  Symptoms: A significant memory leak may occur on a Cisco router.

  Conditions: This symptom is observed when you configure and disable IP routing repetitively by using the **ip routing** global configuration command followed by the **no ip routing** global configuration command.

  Workaround: There is no workaround.

- CSCeb17467

  Symptoms: A Cisco router may reload when Border Gateway Protocol (BGP) is configured to carry Virtual Private Network version 4 (VPNv4) routes.

  Conditions: This symptom is observed when VPNv4 import processing occurs simultaneously with a BGP neighbor reset, for example, when a VPN routing and forwarding (VRF) instance is configured and you enter the **clear ip bgp *** privileged EXEC command.

  Workaround: There is no workaround.

- CSCec43805

  Symptoms: The **distance bgp** *external-distance internal-distance local-distance* address family or router configuration command may be missing from a Border Gateway Protocol (BGP) IPv4 Virtual Private Network (VPN) configuration in the output of the **show running-config** privileged EXEC command when all of the following keywords in the **address-family ipv4 vrf** *vrf-name* router configuration command are configured with their default values:

```
- aggregate-address    Configure BGP aggregate entries
- auto-summary         Enable automatic network number summarization
- bgp                  BGP specific commands
- default              Set a command to its defaults
- default-information  Control distribution of default information
- default-metric       Set metric of redistributed routes
- distance             Define an administrative distance
- distribute-list      Filter networks in routing updates
- exit-address-family  Exit from Address Family configuration mode
- help                 Description of the interactive help system
- maximum-paths        Forward packets over multiple paths
- neighbor             Specify a neighbor router
- network              Specify a network to announce via BGP
- no                   Negate a command or set its defaults
- redistribute         Redistribute information from another routing protocol
- synchronization      Perform IGP synchronization
- table-map            Map external entry attributes into routing table
```

  However, the **distance bgp** *external-distance internal-distance local-distance* address family or router configuration command functions fine because the BGP administrative distance for the VPN in which the command is configured does get changed.

  Conditions: The symptom is observed after the BGP IPv4 VPN configuration is saved in NVRAM and the router is reloaded.

  Workaround: Change any of the keywords for the **address-family ipv4 vrf** *vrf-name* router configuration command (see the Symptoms section above) to a nondefault value.

- CSCec48816

  Symptoms: A router may reload unexpectedly when you remove a **network** command. There is a small window during which this symptom can occur: when a **network** command that covers an interface that is running OSPF is removed and when there are outstanding packets from this interface in OSPF queue.

  Conditions: This symptom is observed on a Cisco router that has the **router ospf** global configuration command enabled.

  Workaround: There is no workaround.

- CSCed33044

  Symptoms: ARP may not function properly on the remote side of point-to-point Fast Ethernet link with a default static route until the remote side is pinged.

  Conditions: This symptom is observed on a Cisco router when ARP and /31 mask are configured on a point-to-point link Fast Ethernet link with a default static route. The symptom is platform-independent.

  Workaround: There are four different workarounds:

  - Use a /30 netmask on the point-to-point Fast Ethernet connection.
  - Configure a static ARP entry for the remote side of the Fast Ethernet link.
  - Enter the **ip proxy-arp** command on the remote side of the Fast Ethernet link.
  - Use an OSPF route instead of a default static route.

Miscellaneous

- CSCea60722

  Symptoms: A Cisco Express Forwarding (CEF) adjacency may not adjust when changes are made to the configuration.

  Conditions: This symptom is observed when you move the IP address from an ATM interface to another interface and when the next-hop router is still mapped in the ATM permanent virtual circuit (PVC). The CEF adjacency continues to point to the ATM interface.

  Workaround: Remove the ATM PVC, and reload the router.

- CSCea83647

  Symptoms: Traceback errors may be generated when a link flap occurs (for example, when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a link) or when you reload the microcode onto a line card.

  Conditions: This symptom can occur on a Cisco router that is configured for Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN).

  Workaround: There is no workaround.

  Further Problem Description: The problem may happen if a single prefix is reachable by both IGP and BGP. It may have an impact if the given prefix is distributed in BGP with MPLS labels. This problem could cause forwarding problems for prefixes learned by both IGP and BGP.

- CSCec27821

  Symptoms: A Network Processing Engine G-1 or G-100 (NPE-G1 or NPE-G100) may forward unicast IP packets that have a Layer 2 multicast MAC address.

Conditions: This symptom is observed on an NPE-G1 that is installed in a Cisco 7200 series or an NPE-G100 installed in a Cisco 7304.

Workaround: Create an access control list (ACL) to filter the packets.

Alternate Workaround: Configure a static multicast MAC address mapping to the ports of the connected Layer 2 switch.

- CSCed11793

  Symptoms: The output queue of a Gigabit Ethernet port may become stuck, preventing traffic from leaving the interface.

  Conditions: This symptom is observed on the Gigabit Ethernet port 0/1 (gig0/1) of a Network Processing Engine NPE-G1 (NPE-G1) that is installed in a Cisco 7200 series.

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

  Alternate Workaround: Reload the router.

- CSCed16759

  Symptoms: There may be a large number of tracebacks when a moderate number of Ethernet VLANs is present in the router startup configuration.

  Conditions: This problem only occurs with Ethernet, Fast Ethernet, and Gigabit Ethernet port adaptors when CDP is enabled.

  Workaround: Disable CDP globally by entering the **no cdp run** command.

- CSCed35896

  Symptoms: There is no SNMP support for SFP insertion and removal of an SPA-2GE-7304 SPA card.

  Conditions: This symptom is only observed on an SPA-2GE-7304 card.

  Workaround: There is no workaround.

- CSCed40933

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory, which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml.

- CSCed47335

  Symptoms: A repeated TFTP download may put a loopback interface into the shutdown state.

  Conditions: This symptom is observed when you enter the **interface loopback** *number* command quickly followed by the **no interface loopback** *number* command.

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

- CSCed47560

  Symptoms: The native Gigabit Ethernet ports of a Cisco 7200 series NPE-G1 or a Cisco 7301 may stop forwarding traffic.

  Conditions: This symptom is observed in a stress situation when bursty traffic is received.

  Workaround: There is no workaround.

- CSCed52163

  Symptom: When the HSRP MIB is polled and there are HSRP groups configured on subinterfaces, an error such as “OID not increasing” may occur on the device that is polling the router. In some cases, a CPUHOG traceback may occur on a router when the HSRP MIB is polled, especially when a lot of interfaces are configured.

  Conditions: This symptom is observed under either one of the following two conditions:

  – An SNMP HSRP query triggers a loop in the getnexts. Some MIB browsers catch this, and exit with a message stating “OID not increasing”.

  – A scaling problem may occur with HSRP when there are a high number of tracked interfaces. For every standby track statement, every interface is tested to see if it is an HSRP tracked interface. No defined thresholds have been identified and tested that qualify when this scaling problem may occur. The more interfaces there are configured, the greater is the possibility that the problem occurs.

  Workaround: Do not initiate an SNMP query for HSRP.

  Alternate Workaround: Enter the **snmp-server** global configuration command to specify which MIBs are available, as in the following example:

  ```
  snmp-server view HSRP internet included
  snmp-server view HSRP ciscoHsrpMIB excluded
  snmp-server view HSRP ciscoHsrpExtMIB excluded
  snmp-server community public view HSRP RW 20
  snmp-server community private view HSRP RW 20
  ```

- CSCed56856

  Symptoms: An OC-3 POS line card may generate a FATAL RX SOAP error.

  Conditions: This symptom is observed when an OC-3 POS line card is present in a Cisco 7304 and when you reload the line card or when you reset an interface of the line card while traffic is being processed.

  Workaround: There is no workaround. The OC-3 POS line card recovers on its own.

- CSCed57753

  Symptoms: IP packets of sizes larger than the interface MTU of an MPLS-enabled interface may be dropped. Packet fragmentation during the IP-to-MPLS switching fails.

  Conditions: This problem happens on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2(20)S or 12.2(20)S1 when large IP packets are sent through a tunnel across an MPLS-enabled interface. The interface has the **tag-switching ip** command enabled.

  Workaround: Configure the MTU value of the MPLS-enabled interface to be large enough so that packet fragmentation is not invoked.

- CSCed66306

  Symptoms: A PXF on a Cisco 7304 NSE-100 may run out of memory for compiled ACLs, causing the download to PXF to fail.

  Conditions: This symptom is observed when the total number of ACL rules is very large (in the 1000s to 10,000s range).

  Workaround: Reduce the total number of ACL rules.

- CSCed75572

  Symptoms: A Cisco 7304 router may take a long time to boot.

Conditions: This symptom is observed when many VLANs are configured on an Ethernet interface.

Workaround: There is no workaround.

- CSCed83521

  Symptoms: Traffic on a subinterface may be dropped due to the configuration at the port level.

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

  Workaround: There is no workaround.

- CSCed87307

  Symptoms: A POS interface may flap or may be in the up/down state. This symptom is related to PXF. You can check the state of the interface (in this example interface 4/0) by entering the **show pxf interface pos 4/0** command:

```
router# show pxf interface pos 4/0
PXF-If: Y 00016  PO4/0        (Up, Processing Input)
  Features: in=CEF iACL Nflow  [0x40E],  out=None [0x0]  qstatus=XOFF
<=====!!!!!
  Ingress Packets:       18994389   Input Drop Packets :         383430
     MPLS Packets:              0
  Egress Packets :       52949973   Output Drop Packets:        5871161
```

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S1.

  Workaround: There is no workaround.

- CSCed91798

  Symptoms: A Cisco IOS DHCP relay or server may stop functioning.

  Conditions: This symptom is observed when the **ip cef** command is enabled.

  Workaround: Disable the **ip cef** command.

- CSCed93338

  Symptoms: Input errors and ignores may be seen on an OC-12 POS interface that is inserted in a Cisco 7304 that has an NPE-G100 processor. The input errors count and ignores count may be equal to each other.

  Conditions: This symptom is observed when an ATA flash disk is installed or removed from device disk0: and while traffic is traversing on interfaces.

  Workaround: Do not remove an ATA flash disk from disk0: while traffic is traversing on any interfaces.

- CSCee03734

  Symptoms: A Cisco 7304 that is configured with redundant NSE-100 processors may report IPC packet corruptions and an IPC buffers memory leak.

  Conditions This problem is reported on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S2.

  Workaround: There is no workaround.

- CSCee05036

  Symptoms: Some packets may be dropped from a Gigabit Ethernet SPA.

  Conditions: This problem only occurs on a Cisco 7304 with an NSE-100 processor when multiple VLANs are configured on the Gigabit Ethernet SPA and when each VLAN has a certain amount of egress traffic. The heavier the traffic, the more packets may be dropped.

Workaround: Configure a QoS service policy and apply this policy to each VLAN on the Gigabit Ethernet SPA.

- CSCee05810

  Symptoms: A SYS-3-CPUHOG message with tracebacks shows up repeatedly in the logs regarding a process IP RIB update.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.0(20)S1 when a full BGP table and several VRFs are configured.

  Workaround: There is no workaround.

- CSCee05907

  Symptoms: The sum of the packet and byte count of the VLAN subinterfaces is much less than the packet and byte count of the main interface.

  Condition: This is symptom is observed on a Cisco 7304 that is configured with an NSE processor.

  Workaround: There is no workaround.

- CSCee08534

  Symptoms: A standby RP on a Cisco 7304 may hang or crash when you disable or change the value of the **max-reserved-bandwidth** command for a port.

  Conditions: This symptom only occurs when a policy map is also configured on the port. The policy must be configured with a QoS function that reserves bandwidth such as the bandwidth, shaping, priority, or other QoS functions. The symptom does not occur when a policy map with policing is configured. The symptom can be easily reproduced and the service policy can be applied to any port to observe the symptom.

  Follow these steps to reproduce the symptom:

  1. Configure a policy map with a QoS function.
  2. Configure the interface with the policy map and the **max-reserved-bandwidth 100** command.
  3. Modify the *percent* argument of the **max-reserved-bandwidth** *percent* command.

  Workaround: Enter the **hw-module standby reset** ECEC command on the standby RP. Doing so enables the standby RP to pick up the new value of the **max-reserved-bandwidth** command.

- CSCee23602

  Symptoms: There is no next-hop loadbalancing support for VPN traffic.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that has PXF enabled.

  Workaround: There is no workaround.

- CSCee27268

  Symptoms: The redundancy modes RPR+ and SSO may not function on a Cisco 7304.

  Conditions: This symptom is observed on a Cisco 7304 that has a Port Adapter Carrier Card (7300-CC-PA) or a Shared Port Adapter Modular Services Card (7300-MSC-100).

  Workaround: If you need RPR+ or SSO, remove the cards that cause the redundancy mode to fall back to RPR.

- CSCee32234

  Symptoms: For certain prefixes, the Parallel Express Forwarding (PXF) processor of a Network Service Engine 100 (NSE-100) may punt packets to the route processor.

Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S, that functions as a provider edge (PE) router, and that has PXF enabled.

Workaround: There is no workaround.

- CSCee35507

  Symptoms: A Cisco 7304 may crash when NetFlow accounting is enabled on the PXF processor.

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

  Workaround: There is no workaround.

- CSCee38003

  Symptoms: A Cisco 7304 may hang.

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

  - The egress side is a native Gigabit Ethernet (GE) port and there is heavy traffic that triggers a double dequeue.
  - The ingress traffic is from the link side and the egress Layer 2 encapsulation length minus the total length the ingress header of 8 bytes and the ingress Layer 2 encapsulation length is 4, or the ingress traffic is from the native GE side and the egress Layer 2 encapsulation length minus the ingress Layer 2 encapsulation length is 4.
  - The class queue shaping configuration bandwidth of the egress interface is more than 500 mbps.
  - If the ingress traffic is from the native GE side: the packet size is more than 64 bytes.
  - PXF packet processing is a one-pass process.

  Workaround: Apply a feature to the input interface (for example, QoS, RPF, ACL) to ensure that the packet processing is a two-pass process. This workaround does impact the performance if the PXF usage is high.

- CSCee55454

  Symptoms: The Parallel Express Forwarding (PXF) processor on a Cisco 7304 that functions as a Provider Edge (PE) router may add the wrong VPN label in a multi-VRF and multi-loadbalancing configuration that faces the MPLS core. This situation may cause a VRF route leakage or may cause VRF routes to be dropped on the PE router at the far end.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S.

  Workaround: Disable PXF.

- CSCee60264

  Symptoms: The Parallel Express Forwarding (PXF) processor on a Cisco 7304 router that functions as a Provider Edge (PE) router may not perform loadbalancing in a dual-homed CE configuration, causing traffic to be punted to the RP.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S.

  Workaround: There is no workaround.

- CSCin68378

  Symptoms: A router crashes due to a Redzone Corruption when receiving IPv6 packets.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with either an NSE-100 or an NPE-G100.

  Workaround: There is no workaround.

- CSCin72573

  Symptoms: IP directed broadcast may not function.

  Conditions: This symptom is observed on a Cisco platform when CEF is enabled.

  Workaround: Disable CEF globally by entering the **no ip cef** global configuration command.

- CSCuk50070

  Symptoms: The packet length can be incorrect when switching IPv6 multicast packets.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(18)S or Release 12.2(20)S during normal IPv6 multicast forwarding.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(22)S and later releases.

Resolved Caveats—Cisco IOS Release 12.2(20)S2

Cisco IOS Release 12.2(20)S2 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S2 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCeb72053

  Symptoms: A spurious access may occur on a VIP.

  Conditions: This symptom is observed on a Cisco 7500 series when traffic is being sent.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdv57965

  Symptoms: Although you may able to configure more than 4 Gbps of bandwidth for Resource Reservation Protocol (RSVP) or for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, the actual reserved bandwidth that is established for RSVP or the MPLS TE tunnel may be much less than 4 Gbps.

  The output of the **show running-config interface** *type number* privileged EXEC command shows the configured bandwidth. The output of the **show ip rsvp reservation** EXEC command shows the actual reserved bandwidth for RSVP.

  Conditions: This symptom is observed when the interface on which RSVP or the MPLS TE tunnel is configured does have sufficient bandwidth available to satisfy the configured bandwidth but the actual reserved bandwidth is less than the configured bandwidth.

  Workaround: There is no workaround.

Miscellaneous

- CSCdz27929

  Symptoms: The Parallel Express Forwarding (PXF) processor of a Network Services Engine 100 (NSE-100) may not forward MPLS packets on the dot1q native VLAN.

Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S1.

Workaround: There is no workaround.

- CSCec14039

  Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

  ```
  Last reset from watchdog reset
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1 and that is running Cisco IOS Release 12.2(14)S3. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCec23607

  Symptoms: The **match cos** command may be enabled in error.

  Conditions: This symptom is observed on a Cisco 7200 series and a Cisco 7304 that is configured with an NSE-100. This feature is not supported on the Cisco 7200 series and the Cisco 7304.

  Workaround: There is no workaround.

- CSCec31206

  Symptoms: The amount of free memory on a router decreases as the memory that is held by the Simple Network Management Protocol (SNMP) engine process increases. The decrease in the amount of free memory can be verified by examining the output of the **show proc mem | i SNMP** privileged EXEC command.

  Conditions: This symptom is observed when SNMP is used to attempt to set values in the LDP-MIB, TE-MIB, or VPN-MIB.

  Workaround: Avoid using SNMP to set values in the MIBs. Use the CLI on the router to set the values needed.

- CSCec51591

  Symptoms: When you enter the **hw-module slot** *slot-number* **stop** privileged EXEC command, interprocess communications (IPC) errors may occur on a remotely connected router, and I/O memory may be depleted, which may cause unstable operation of the remotely connected router.

  Conditions: This symptom is observed when you enter the **hw-module slot** *slot-number* **stop** privileged EXEC command on a local router that is connected to an 8-port Ethernet 10BASE-T port adapter (PA-8E) that is installed in a port adapter carrier card on a Cisco 7304 and when traffic is flowing between the two routers.

  Workaround: Do not enter the **hw-module slot** *slot-number* **stop** privileged EXEC command.

- CSCed11691

  Symptoms: Traffic may be switched by the RP.

  Conditions: This symptom is observed on a Cisco 7304 when you configure keepalives for a tunnel number that is higher than three.

  Workaround: Reload the router.

- CSCed11700

  Symptoms: Traffic may gradually stop being switched by the PXF processor and may be taken over by the RP, eventually causing 100 percent CPU utilization on the RP.

Conditions: This symptom is observed on a Cisco 7304 with a large number of GRE tunnels (2000) during a long-term test (20 hours) while the tunnels flap at the rate of approximately 30 tunnels per minute.

Workaround: Reboot the router.

- CSCed17858

  Symptoms: A router may crash or hang when traffic is sent to the Fast Ethernet (FE) port.

  Conditions: This symptom is observed on a Cisco 7304 when CEF switching is enabled on the FE port.

  Workaround: Disable CEF switching on the FE port by entering the **no ip route-cache** command.

- CSCed20042

  Symptoms: A Cisco router may unexpectedly reload if IPv6 encounters a routing loop, and IPv6 CEF is enabled.

  Conditions: This symptom occurs under the following conditions:

  – IPv6 must be enabled

  – IPv6 CEF must be enabled

  – The IPv6 RIB must have recursive entries that form a loop, for example:

```
Router# show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
B   ::/0 [200/0]
     via 2::2
C   1::/64 [0/0]
     via ::, Ethernet0/0
L   1::2/128 [0/0]
     via ::, Ethernet0/0
C   2::/64 [0/0]
     via ::, Ethernet1/0
L   2::1/128 [0/0]
     via ::, Ethernet1/0
B   2001::/16 [200/0]
     via 2002::1
B   2002::/16 [200/0]
     via 2001::1
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

  Note that 2001::/16 and 2002::/16 results in a recursion loop because 2001::/16 is accessible via 2002::/16 and 2002::/16 is accessible via 2001::/16.

  Workaround: Disable IPv6 CEF using the global configuration command **no ipv6 cef**.

- CSCed34080

  Symptoms: Tunneled traffic may not be switched via PXF.

  Conditions: This symptom is observed on a Cisco 7304 for certain tunnel ID combinations.

  Workaround: There is no workaround.

- CSCed38279

  Symptoms: A “process watchdog timeout” with a “Fatal Alignment Error” may occur for an ACL.

  Conditions: This symptom is observed only in Cisco IOS Release 12.2(20)S1 when you configure many large ACLs (the number of ACLs and the number of access-list entries are both large).

  Workaround: There is no workaround.

- CSCed46665

  Symptom: The auxiliary port may not send any characters to a modem.

  Condition: This symptom is observed when you dial through a modem to the auxiliary port on an NSE-100 that is installed in a Cisco 7304.

  Workaround: There is no workaround.

- CSCed48249

  Symptoms: Some PVCs may stop forwarding traffic after an HA switchover when the RP in slot 2 of a Cisco 7304 is the active RP.

  Conditions: This symptom is observed when a large number of PVCs are configured on the router.

  Workaround: There is no workaround.

- CSCed48460

  Symptoms: A Cisco 7304 may reload unexpectedly because of a watchdog reset.

  Conditions: This symptom is observed on a Cisco 7304 with an NPE-G100.

  Workaround: There is no workaround.

- CSCed49665

  Symptoms: Host packets may be sent on wrong interfaces.

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

  Workaround: There is no workaround.

- CSCed51664

  Symptoms: Gigabit Ethernet interfaces on a Network Processing Engine G-1 (NPE-G1) may not accept packets with long MPLS headers. This situation may decrease the performance of some network environment such as an Ethernet over MPLS (EoMPLS) environment.

  Packets with a size that exceeds the maximum MTU in the output of the **show controller gigabitethernet 0/x** command may be dropped.

  Conditions: This symptom is observed on a Cisco 7200 series.

  Workaround: Increase the MTU at the interface level.

- CSCed54484

  Symptoms: A Cisco 7304 may have incorrect netflow masks. Rather than the correct network mask, /0 masks are incorrectly used.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S and that has PXF enabled when the destination is loadbalanced to more than one next hop.

Workaround: Disable PXF. However, when PXF is disabled, other issues may occur because of higher CPU utilization.

- CSCed57980

  Symptoms: Packet forwarding may fail on ATM interfaces that are configured for VRF forwarding.

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

  Workaround: After the router has reloaded, manually reapply the VRF forwarding configuration and the IP address to the ATM interfaces.

- CSCed61707

  Symptoms: Although the state is UP/UP, a GE interface may not forward traffic because of an incomplete ARP entry.

  Condition: This symptom is observed on a Cisco 7403 when GE autonegotiation is off.

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

- CSCed63220

  Symptoms: A Cisco 7304 may reload unexpectedly.

  Conditions: This symptom is observed when more than 1023 VRFs are configured.

  Workaround: Do not configure more than 1023 VRFs.

- CSCed68125

  Symptoms: CPU hog messages may be generated when you attempt to bring up more than 2500 VCs.

  Conditions: This symptom is observed on a Cisco 7304.

  Workaround: There is no workaround.

- CSCed68575

  Cisco Internetwork Operating System (IOS) Software releases trains 12.0 S, 12.1 E, 12.2, 12.2 S, 12.3, 12.3 B and 12.3 T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

- CSCed75813

  Symptoms: When Multilink PPP packets are received out of order at the bundle point, an NPE-G100 fails to reorder them and drops the packets.

  Conditions: This symptom is observed on a Cisco 7304.

  Workaround: There is no workaround.

- CSCed76358

  Symptoms: Channelized port adapters such as the PA-MC-8E1 may stop transmitting traffic. The port adapter does not recover from this condition, even after the traffic stops.

Conditions: This symptom is observed under heavy traffic conditions.

Workaround: There is no workaround.

- CSCed77606

  Symptoms: When traffic goes through an MPLS TE tunnel and the router terminating the TE tunnel is directly connected to the router sending the traffic, traffic may become blackholed. When the router terminating the TE tunnel is one or more hops further, traffic passes through fine.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(18)S or 12.2(20)S1, that has an NSE-100, and that has PXF enabled.

  Workaround: Disable PXF by entering the **no ip pxf** command. Ensure that you understand the impact of this command prior to applying it: the command causes all traffic to be switched by the RP and, depending on the traffic load on the router, may cause high CPU utilization.

- CSCed77668

  Symptoms: A wrong ACL permit or deny statement may occur or wrong ACL-based QoS classifications may occur.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S1 and that is configured with an NSE-100. The symptom does not occur in Cisco IOS Release of 12.2(20)S or earlier 12.2 S releases.

  Workaround: There is no workaround.

- CSCed83148

  Symptoms: An I/O memory leak may occur on a Cisco 7304 with a Network Services Engine 100 (NSE-100) in a redundant configuration.

  Conditions: This symptom is observed when the native Gigabit Ethernet (GE) interfaces on the standby NSE-100 are not administratively shut down but are not up because of cable issues.

  Workaround: Bring up the native GE interfaces on the standby NSE-100. Doing so stops the I/O memory leak.

- CSCed83813

  Symptom: Changing the IP address of the Fast Ethernet interface 0 on an NSE-100 may cause the interface to flap.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S1.

  Workaround: There is no workaround.

- CSCed89576

  Symptoms: Traffic shaping may not function.

  Conditions: This symptom is observed on a Cisco 7304 that has a Network Services Engine 100 (NSE-100) when a service policy is attached to a subinterface. This symptom occurs after the router has reloaded or when the configuration is changed, depending on the encapsulation type of the subinterface.

  Workaround: Detach and reattach the service policy to the interface.

- CSCed93776

  Symptoms: Traffic may stop and a 7300-CC-PA carrier card may reload one minute after the traffic has stopped when one of the following port adapters is installed in the 7300-CC-PA carrier card:

  - PA-MC-8E1
  - PA-MC-8T1
  - PA-MC-8TE1+

  Conditions: This symptom is observed on a Cisco 7304 when the 7300-CC-PA carrier card runs FPGA version 1.11. To find out which FPGA version runs on the 7300-CC-PA carrier card, enter the **show diag** *slot* EXEC command. The FPGA version information is listed at the end of the command output.

  Workaround: There is no workaround. After the 7300-CC-PA carrier card has reloaded, traffic resumes automatically.

- CSCin35946

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

  Symptoms 1: When the Rivest, Shamir, and Adleman (RSA) public key of the peer of Cisco router that is running Cisco IOS Release 12.3 is manually configured on the router, the router may reload and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions 1: This symptom is observed when you enter the following sequence of commands:

  - **crypto key pubkey-chain rsa** global configuration command
  - **addressed-key** *key-address* public key chain configuration command
  - **key-string** *key-string* public key configuration command

  Workaround 1: Do not configure the RSA public key of a peer statically on the router; rather, use certificates. This workaround may not be acceptable in situations in which a certification authority (CA) server is not available or deployed.

  Symptoms 2: When a Cisco router has saved the RSA public key of any peer in its configuration and is booted up with Release 12.3, the router may reload and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions 2: This symptom is observed when you have configured the RSA public key of the peer by using the following sequence of commands:

  - **crypto keyring** *keyring-name* global configuration command
  - **rsa-pubkey address** address keyring configuration command
  - **key-string** *key-string* public key configuration command

  Workaround 2: Do not configure the RSA public key of a peer statically on the router; rather, use certificates. This workaround may not be acceptable in situations in which a certification authority (CA) server is not available or deployed.

- CSCin41685

  Symptoms: A ping to a Cisco 7304 with an NSE-100 may not be completely acknowledged.

  Conditions: This symptom is observed in the following two situations:

  - A sweep ping to a directly-connected Cisco 7304.
  - A ping to a loopback interface with a packet of certain size (991 bytes).

  Workaround: There is no workaround.

- CSCin52270

  Symptoms: IP multicast traffic may not be fast-switched.

  Conditions: This symptom is observed on a Cisco 7304 with an Network Processing Engine G-100 (NPE-G100).

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(20)S1

Cisco IOS Release 12.2(20)S1 is a rebuild release for Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. The caveats in this section are resolved in Cisco IOS Release 12.2(20)S1 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCdy43232

  Symptoms: Packets may be forwarded to the process level even though fast switching is enabled for both the global table and the VPN routing/forwarding (VRF) table of a Cisco router.

  Conditions: This symptom is observed when a Multicast Virtual Private Network (MVPN) is configured with fast switching on an egress provider edge (PE) router.

  Workaround: There is no workaround.

- CSCeb48835

  Symptoms: Boot variables may not be cleared, may not be set, or may become corrupted.

  Conditions: This symptom is observed when you copy a configuration to the startup configuration, for example by entering the **copy system:running-config nvram:startup-config** EXEC command. The old boot variables may not be replaced with the new boot variables; instead, they may be appended incorrectly. The old boot variables should be replaced with the new boot variables.

  Workaround: First, enter the **no boot system** global configuration command and save the configuration. Then, configure the new boot statement.

- CSCeb80481

  Symptoms: A memory leak may occur in the "SNMP Engine" process, which can be verified in the output of the **show processes memory | SNMP ENGINE** privileged EXEC command.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(26)S and Release 12.2(18)S when you enter the **snmpget** command for the MPLS-LSR-MIB MIB.

  Workaround: There is no workaround.

- CSCec02876

  Symptoms: A memory allocation failure may occur on compiled access control list (ACL) tables. There may be continued attempts to recompile the ACLs that fail.

  Conditions: This symptom is observed when compiled ACLs are enabled by entering the **access-list compiled** global configuration command, and the total number of ACL entries is relatively large (over 1500 lines). Random or constantly changing traffic patterns may cause the compiled ACL tables to grow to the point at which memory fragmentation causes the memory allocation failure.

  Workaround: Disable and then reenable the compiled ACLs by entering the **no access-list compiled** global configuration command followed by the **access-list compiled** global configuration command.

Alternate Workaround: Completely disable the compiled ACLs.

Second Alternate Workaround: ACLs may sometimes be rearranged to make the list shorter or less complex. This will reduce the memory requirements. Large ACLs used for Border Gateway Protocol (BGP) route prefixes may be converted to use a prefix list configuration instead.

- CSCec40175

  Symptoms: A router may reload unexpectedly during bootup when more than 2000 virtual circuits (VCs) are configured on an 8-port ATM Inverse MUX E1 or T1 port adapter (PA-A3-8E1IMA or PA-A3-8T1IMA). The same symptom may occur on a running router when more than 2000 VCs are created in quick succession.

  Conditions: These symptoms are observed on a Cisco 7304 that is configured with a Network Processing Engine G100 (NPE-G100), a 7300-CC-PA carrier card, and a PA-A3-8E1IMA or PA-A3-8T1IMA.

  Workaround: There is no workaround.

- CSCec51772

  Symptoms: When a service policy with a police statement is applied to a port that is configured for NetFlow, the flow cache in the output of the **show ip cache flow** user EXEC or privileged EXEC command may not display the flow that is coming through this port.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S or Release 12.2(14)SZ and that is configured with a Network Services Engine 100 (NSE-100) when NetFlow accounting is enabled in the Parallel Express Forwarding (PXF) processor of the NSE-100 and when the traffic rate exceeds the drop rate limit of the police statement.

  Workaround: There is no workaround.

- CSCec62745

  Symptoms: A Packet-over-SONET (POS) line card that is installed in a Cisco 7304 may drop incoming packets that are smaller than 4 bytes, preventing echo replies of ping packets from being received. These echo replies are packets that have a size of 3 bytes and that have the backward explicit congestion notification (BECN) bit set.

  Conditions: This symptom is observed on a Cisco 7304 that functions as an originating customer edge (CE) router when the following conditions are present:

  – The destination CE router has the **map-class frame-relay** *map-class-name* global configuration command enabled.
  – The *map-class-name* argument is defined as **fecn-adapt**.
  – The destination CE sends echo replies to the originating CE router.

  Workaround: There is no workaround.

- CSCec64543

  Symptoms: The Parallel Express Forwarding (PXF) processor of a Network Services Engine (NSE-100) on a Cisco 7304 may send packets to the Route Processor (RP) for processing.

  Conditions: This symptom is observed when traffic is forwarded to a destination across multiple equal cost forwarding paths.

  Workaround: Disable one of the multiple forwarding paths.

- CSCec64603

  Symptoms: You may not be able to receive multicast packets on any Ethernet port adaptor after you have entered the **hw-module slot** *slot-number* **stop** privileged EXEC command followed by the **hw-module slot** *slot-number* **start** privileged EXEC command. The same symptom may occur after you have performed a physical online insertion and removal (OIR) of a Cisco 7304 Port Adapter Carrier Card (7300-CC-PA).

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2 S or Release 12.3 T and that is configured with a Network Services Engine 100 (NSE-100) and a 7300-CC-PA. The symptom may occur also when the Cisco 7304 is configured with a Network Processing Engine G100 (NPE-G100).

  Workaround: When an OIR is required, reload the router afterwards.

- CSCec69068

  Symptoms: The **crc** *size* interface configuration command and the **pos scramble-atm** interface configuration command may become lost from a Packet-over-SONET (POS) configuration.

  Conditions: This symptom is observed after a Cisco 7304 that is configured with a Network Services Engine 100 (NSE-100) has reloaded.

  Workaround: There is no workaround.

- CSCec74908

  Symptoms: The IP route cache may be disabled after you have entered the **hw-module slot** *slot-number* **stop** privileged EXEC command followed by the **hw-module slot** *slot-number* **start** privileged EXEC command on a Cisco 7304 Port Adapter Carrier Card (7300-CC-PA). The same symptom may occur after you have performed a physical online insertion and removal (OIR) of the 7300-CC-PA.

  When the router is configured with a Network Services Engine 100 (NSE-100) and the IP route cache becomes disabled, all packets are punted to the Route Processor (RP).

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 7300-CC-PA.

  Workaround: First, shut down the router. Then, perform an OIR.

- CSCec75000

  Symptoms: The GE-to-GE throughput rate of the native Gigabit Ethernet (GE) ports of a Network Processing Engine G100 (NPE-G100) may be lower than you would expect. The line card-to-line card switching performance is not affected.

  Conditions: This symptom is observed on a Cisco 7304.

  Workaround: There is no workaround.

- CSCec80049

  Symptoms: When a tunnel interface goes down, a new Label Switched Path (LSP) is not signaled until the forwarding adjacency hold timer expires.

  Conditions: This symptom is observed on a Cisco router that is configured with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

  Workaround: There is no workaround.

- CSCec82849

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

  1. Symptom 1: The output of the **show disk0:** EXEC command may not display the information for the current disk but rather for the previous disk that was installed.

Condition 1: This symptom is observed on a Cisco 7304 after you have performed an online insertion and removal (OIR) of a compact flash disk.

Workaround 1: Enter the **dir disk0:** EXEC command to display the information about the current disk.

2. Symptom 2: When you enter the **fsck disk0:** privileged EXEC command for a compact flash disk, the disk may become corrupted.

   Condition 2: This symptom is observed on a Cisco 7304 after you have performed an online insertion and removal (OIR) of a compact flash disk.

   Workaround 2: There is no workaround.

- CSCec83116

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

  1. Symptom 1: A Cisco 7304 may reload unexpectedly when you remove and readd one or more service policies.

     Condition 1: This symptom is observed when you apply quality of service (QoS) policies to both physical interfaces and subinterfaces on the same port by entering the **service-policy** interface configuration command, you reload the router, and you remove and readd one or more service policies.

     Workaround 1: Boot the router without the service policies applied to the physical interface. Then, apply the service policies to the physical interface. Note that the symptom does not occur when you apply service policies to subinterfaces only, you reload the router, and you remove and readd one or more service policies.

  2. Symptom 2: A Cisco 7304 may reload unexpectedly when you apply a service policy to a permanent virtual circuit (PVC).

     Condition 2: This symptom is observed when you first apply the service policy to an ATM subinterface, remove the service policy from the ATM subinterface, and then apply the service policy to a PVC.

     Workaround 2: Do not apply the service policy to the ATM subinterface: this configuration is not supported. You may apply the service policy to the PVC.

  3. Symptom 3: A Cisco 7304 may reload unexpectedly when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an ATM interface.

     Condition 3: This symptom is observed when you first attach a service policy to a subinterface of the ATM main interface and then enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration on the main interface.

     Workaround 3: Do not apply the service policy to the ATM subinterface: this configuration is not supported.

- CSCed00323

  Symptoms: When input traffic is process-switched via a bridge virtual interface (BVI) or tunnel interface, the input queue of the BVI or tunnel interface may become wedged.

  Conditions: This symptom is observed on a Network Services Engine 100 (NSE-100).

  Workaround: There is no workaround.

- CSCed10406

  Symptoms: Packets that are switched through a tunnel interface may not be properly encapsulated and transmitted.

Conditions: This symptom is observed on a Cisco 7304 when an input feature such as an input access control list (ACL) is configured on an interface.

Workaround: There is no workaround.

- CSCed11124

  Symptoms: A low-bandwidth class may be allocated more than its share of bandwidth, at the expense of a high-bandwidth class.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Services Engine 100 (NSE-100) when the ratio of the configured bandwidths between two data classes is rather high (8:1 or higher) and when there is a priority class that receives traffic at at least 20 percent of the line rate. The traffic that is received by the data classes should be in the ratio of the configured bandwidths.

  Workaround: There is no workaround.

- CSCed26141

  Symptoms: The c7300-p-mz service provider image does not contain the support for the Cisco-Syslog-MIB MIB.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(14)SZ or Release 12.2(20)S.

  Workaround: There is no workaround. Note that support for the Cisco-Syslog-MIB MIB is available in the c7300-js-mz enterprise image.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed30094

  Symptoms: A Cisco router may reload when power-on diagnostics are enabled and the system memory exceeds 256 MB.

  Conditions: This symptom is observed when you boot the router from a boot image.

  Workaround: Disable the power-on diagnostics.

  Alternate Workaround: Load the system image from flash memory.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed46882

  Symptoms: Packets that enter an interface that is not configured for Virtual Private Network (VPN) routing/forwarding (VRF) may be forwarded according to the VRF default route when no route is found in the global routing table. This situation may cause packets to be leaked into a VRF instance.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(14)SZ6 or Release 12.2(20)S, that functions as a provider edge (PE) router, and that has Parallel Express Forwarding (PXF) enabled.

  Workaround: Configure the default route in the global routing table to be “Null0.”

  Alternate Workaround: Disable PXF.

- CSCin57765

  Symptoms: A router may become unresponsive and may reload when you append a file whose size is not a multiple of 512 bytes to an Advanced Technology Attachment (ATA) flash card (for example, boot disk, disk0, disk1).

  For example, this situation may occur when you enter the **show** *command* **| tee /append** *url* privileged EXEC command.

  Conditions: This symptom is observed on a Cisco platform that runs a Cisco IOS image that contains the fix for caveat CSCdz27200 and that utilizes an ATA flash card. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz27200. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Write the output of the **show** command to a new file instead of appending it to an existing file by entering the **show** *command* **| tee** *url* privileged EXEC command.

- CSCin64584

  Symptoms: Traffic shaping may not function as you would expect on a very congested output interface. The actual output traffic of the shaped class may be much lower than its shaping rate, or traffic shaping at the output interface may be inactive, which can be verified in the output of the **show policy-map interface** *interface-name* EXEC command.

Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Processing Engine G100 (NPE-G100) when the following conditions are present:

- The interface has an output policy attached that matches multiple classes.
- Traffic is shaped for only one or more classes.
- The aggregated output traffic is higher than the line rate traffic of the interface.
- Aggregated traffic is sent to an output interface, causing the output interface to become congested.

Workaround: In the policy map that specifies the traffic shaping, add traffic shaping for all other classes, including the default class. Ensure that the total shaping rate does not exceed the line rate of the output interface.

- CSCuk46869

  Symptoms: A spurious memory access may occur on a Cisco router and an "%ALIGN-3-SPURIOUS" error message may be generated.

  Conditions: This symptom is observed when you enter the **tunnel vrf** *vrf-name* global configuration command on a tunnel interface.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(20)S

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router, although some caveats are platform-independent. All the caveats listed in this section are open in Cisco IOS Release 12.2(20)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

IBM Connectivity

- CSCec68023

  Symptoms: When you enter the **dlsw bridge-group** *group-number* global configuration command, the following error messages and tracebacks may be generated:

  ```
  %IDBINDEX_SYNC-3-UNKNOWN_TYPE: IDB type is unknown and cannot be synced: "",0
  -Traceback= 4021FCAC 40220F58 4021FF10 4022122C 40455C90 40457D4C 41256D8C 412592B0
  4125982C 40CC9D04 4125C6C8 4125B83C 4125B6A8 412620AC 41293FD4 4128A660

  %IDBINDEX_SYNC-3-IDBINDEX_INITKEY: Cannot initialize IDB index table lookup key: "",0
  ```

  Conditions: This symptom is observed on a Cisco 7304 and a Cisco 7500 series that run Cisco IOS Release 12.2(20)S and that are configured for High Availability (HA).

  Workaround: There is no workaround. However, the symptom is of a cosmetic nature. Data-link switching plus (DLSw+) functions properly.

Miscellaneous

- CSCeb54391

  Symptoms: A Network Service Engine 100 (NSE-100) that is installed in a Cisco 7304 may reload unexpectedly.

Conditions: This symptom is observed when you attempt to apply a quality of service (QoS) service policy to an unspecified bit rate (UBR) ATM virtual circuit (VC) by using modular QoS CLI (MQC). The following is an example of such an attempt:

```
class-map match-any prec2
  match ip precedence 2
class-map match-any prec3
  match ip precedence 3
policy-map cc
  class prec2
   bandwidth 5000
  class prec3
   bandwidth 2000
!
interface ATM5/0
 no ip address
 pvc 0/200
  service-policy output cc
```

Workaround: There is no workaround. Note that the fix for this caveat prevents the router from reloading unexpectedly but still does not allow a QoS service policy to be applied to an UBR ATM VC by using MQC because the VC does not have any implied bandwidth. Note that the symptom does not occur in Cisco IOS Release 12.2(20)S.

- CSCec21527

  Symptoms: A Network Service Engine 100 (NSE-100) that is installed in a Cisco 7304 router may reload unexpectedly and report a bus error.

  Conditions: This symptom is observed when IP version 6 (IPv6) and Virtual Private Network (VPN) routing/forwarding (VRF) instances are enabled on the Cisco 7304 router.

  Workaround: There is no workaround.

- CSCec28416

  Symptoms: A low-bandwidth class may be allocated more than its share of bandwidth, at the expense of a high-bandwidth class.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Service Engine 100 (NSE-100) when the ratio of the configured bandwidths between two data classes is rather high (8:1 or higher) and when there is a priority class that receives traffic at at least 20 percent of the line rate. The traffic that is received by the data classes should be in the ratio of the configured bandwidths.

  Workaround: There is no workaround.

- CSCec38711

  Symptoms: The bandwidth allocation may be incorrect in an hierarchical traffic-shaping service policy that has multiple child classes.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Service Engine 100 (NSE-100).

  Workaround: There is no workaround.

- CSCec45364

  Symptoms: After a high availability (HA) switchover has occurred, tracebacks may occur.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an OC-12 Packet-over-SONET (POS) line card, that has Route Processor Redundancy Plus (RPR+) and Border Gateway Protocol (BGP) enabled, and when there is a high rate of traffic of about 1 Mbps.

  Workaround: There is no workaround.

- CSCec49218

  Symptoms: A Cisco 7304 may no longer offer the option to save the configuration.

  Conditions: This symptom is observed after two high availability (HA) switchovers have occurred and you have initiated the switchovers by entering the **redundancy force-switchover** privileged EXEC command.

  When you have completed a configuration on the router, the router should offer the option to save the configuration before you initiate a switchover.

  Workaround: Enter the **write memory** EXEC command to save the configuration before you initiate a switchover.

- CSCec51591

  Symptoms: When you enter the **hw-module slot** *slot-number* **stop** privileged EXEC command, interprocess communications (IPC) errors may occur on a remotely connected router, and I/O memory may be depleted, which may cause unstable operation of the remotely connected router.

  Conditions: This symptom is observed when you enter the **hw-module slot** *slot-number* **stop** privileged EXEC command on a local router that is connected to an 8-port Ethernet 10BASE-T port adapter (PA-8E) that is installed in a port adapter carrier card on a Cisco 7304 and when traffic is flowing between the two routers.

  Workaround: Do not enter the **hw-module slot** *slot-number* **stop** privileged EXEC command.

- CSCec64543

  Symptoms: The Parallel Express Forwarding (PXF) processor of a Network Service Engine (NSE-100) on a Cisco 7304 may send packets to the Route Processor (RP) for processing.

  Conditions: This symptom is observed when traffic is forwarded to a destination at a router that is configured for Border Gateway Protocol (BGP), when the destination was learned via Open Shortest Path First (OSPF), and when there are multiple forwarding paths to this destination.

  Workaround: Disable one of the multiple forwarding paths.

- CSCec67170

  Symptoms: A 4-port serial enhanced port adapter (PA-4T+) may not function when the Synchronous Data Link Control (SDLC) protocol is configured.

  Conditions: This symptom is observed on a Cisco 7304.

  Workaround: There is no workaround.

- CSCec67231

  Symptoms: After you have entered the **encapsulation bstun** interface configuration command to configure a Block Serial Tunnel (BSTUN) on a serial interface, all further BSTUN commands that you attempt to enter may be rejected.

  Conditions: This symptom is observed on a Cisco 7304.

  Workaround: There is no workaround.

- CSCed75316

  Symptoms: A link may not work intermittently between a 6-port E3 line card and a digital link DSU (DL3100E) when subrates are configured. Pings may not go through either.

  Conditions: This symptom is observed after you have reloaded a Cisco 7304 when the 6-port E3 line card is connected to an external digital link DSU and when the interface has the **dsu bandwidth** command enabled.

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

Resolved Caveats—Cisco IOS Release 12.2(20)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(20)S, which supports only the Cisco 7304 router. However, many caveats are platform-independent. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCea83367

  Symptoms: The running configuration may not be properly synchronized with the startup configuration after a switchover has occurred, causing the **snmp-server community public rw** global configuration command to be lost from the running configuration.

  Conditions: This symptom is observed on a Cisco router after a switchover has occurred.

  Workaround: After the switchover has occurred, manually reconfigure the **snmp-server community public rw** global configuration command.

- CSCeb08094

  Symptoms: A router may reload unexpectedly, generate a crashinfo file, and then pause indefinitely.

  Conditions: This symptom is observed on a Cisco router that is configured with the **exception dump** global configuration command.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCdy65658

  Symptoms: A policy map with multiple class maps may not synchronize correctly with a standby Route Processor (RP).

  Conditions: This symptom is observed on a Cisco router that is configured with dual RPs.

  Workaround: Reload the standby RP.

- CSCin22321

  Symptoms: If the netConfigSet and hostConfigSet variables of the OLD-CISCO-SYS-MIB MIB are set, the corresponding commands may not be executed, and the following error messages and tracebacks may be generated:

  ```
  %SYS-4-SNMP_NETCONFIGSET: SNMP netConfigSet request.
  Loading configuration from 10.10.10.10
  ```

```
%SYS-3-TIMERNEG: Cannot start timer (0x545E1928) with negative offset (-1).
-Process= "SNMP ENGINE", ipl= 6, pid= 143
-Traceback= 502308BC 5022E3F8 50233358 501B0A24 501B298C 501C3618 501C3800
50259C00 50255290 5024F444 502574BC 502576FC 5017C4F4 508EBE04 508EBBBC 508D4D8C

%PARSER-4-BADCFG: Unexpected end of configuration file.
```

Conditions: This symptom is platform independent.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCeb86989

  Symptoms: You may not be able to create an ATM permanent virtual circuit (PVC) with a virtual template.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an enhanced 1-port ATM OC-12/STM-4 port adapter (PA-A3-OC12).

  Workaround: There is no workaround.

- CSCec26643

  Symptoms: Packet-over-SONET (POS) interfaces on a 1-port POS OC-3c/STM-1 port adapter (PA-POS-OC3) that is installed in a Cisco 7200 series router that runs Cisco IOS Release 12.2(14)S3 may stop transmitting packets. The output packets counter stops incrementing.

  Conditions: This symptom is observed when you reload the router with a queueing configuration on the POS interfaces.

  Workaround: Remove the queueing configuration before you reload the router. Reapply the queueing configuration after the router has booted up.

IP Routing Protocols

- CSCdy60008

  Symptoms: If the interface bandwidth or delay is changed, a router may reload.

  Conditions: This symptom is observed after Enhanced Interior Gateway Routing Protocol (EIGRP) is terminated via the **no router eigrp** *as-number* global configuration command or the **no ip routing** global configuration command, causing the EIGRP process list to be invalid.

  Workaround: Reload the router after terminating EIGRP.

- CSCea46372

  Symptoms: A Cisco router may reload when you add Border Gateway Protocol (BGP) neighbor statements to the configuration.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S or Release 12.2 S when BGP neighbors are added by using a script that adds the BGP neighbors at a much faster rate than manual addition, and when a large BGP table is already present on the router before the script adds the BGP neighbors.

  Workaround: There is no workaround.

- CSCeb30338

  Symptoms: Packet loss may occur about once per minute.

  Conditions: This symptom is observed in an IP multicast environment when a router is directly connected to both a source and a receiver and when the shortest path tree (SPT) threshold is configured as infinite.

  The packet loss occurs about once per minute because the (S,G) entry is deleted every minute, causing the hardware shortcut to be deleted and reinstalled.

  Workaround: There is no workaround.

- CSCeb14838

  Symptoms: An interface cannot send Resource Reservation Protocol (RSVP) messages.

  Conditions: This symptom is observed after you have reloaded a Cisco router and RSVP is enabled on an interface just after you have entered the **no shutdown** interface configuration command on the interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface. This workaround is not effective for an unattended router.

- CSCeb57086

  Symptoms: A Cisco 10000 series that is configured with two Performance Routing Engine 1 (PRE-1) processors may stop functioning as a redundant system.

  Conditions: This symptom is observed when you enter the **bgp upgrade-cli** router configuration command.

  Workaround: Reload the standby PRE-1.

- CSCeb57662

  Symptoms: Configured static multicast routes may be ignored in the Reverse Path Forwarding (RPF) calculation.

  Conditions: This symptom is observed in Cisco IOS Release 12.2 S and is platform independent.

  Workaround: There is no workaround.

- CSCeb63120

  Symptoms: When refresh reduction is enabled and a Cisco router has been operational for a long time, valid Resource Reservation Protocol (RSVP) messages that are received from a neighbor may be dropped when the message IDs have cycled through the entire number space once (that is, from 0 to 4,294,967,295) and then progressed up to 2,147,483,648 (0x80000000).

  Conditions: This symptom is observed when a message ID number space begins at zero, increases up to 4,294,967,295 (32 bits), but then does not properly wrap back to zero, causing message IDs greater than 2,147,483,648 to be out of sequence, and to be dropped.

  Note that a neighboring router is able to send Message IDs and properly wraps back from 4,294,967,295 to zero, but the receiving router that does not record the wrap event, causing the symptom to occur.

  Workaround: There is no workaround.

- CSCeb65729

  Symptoms: Border Gateway Protocol (BGP) routes may not be recognized.

  Conditions: This symptom is observed when the **match ip next-hop** route-map configuration command is configured with an access control list (ACL) that matches a particular route.

Workaround: There is no workaround.

- CSCeb68569

  Symptoms: Packets that are switched via process switching may cause high CPU utilization on a router.

  Conditions: This symptom is observed in an IP multicast environment when the packets are sent from a virtual host interface (VIF) and are destined for a multicast address. The packets should be switched via fast switching.

  Workaround: There is no workaround.

- CSCeb68925

  Symptoms: Enabling IP version 6 (IPv6) multicast routing by entering the **ipv6 multicast-routing** global configuration command may cause memory corruption. This situation may eventually cause the router to reload.

  Conditions: This symptom is observed on a Cisco 7200 series but may also occur on other platforms.

  Workaround: There is no workaround.

- CSCeb86563

  Symptoms: Multicast forwarding entries on a line card may become incorrect, causing packets to be forwarded to the Route Processor (RP). Packets may be dropped from the line card when the outgoing list becomes empty.

  Conditions: This symptom is observed after a high availability (HA) switchover has occurred.

  Workaround: Reload the line card after the HA switchover has occurred.

- CSCec10494

  Symptoms: A Cisco router or switch may reload unexpectedly when you enter the **show ip igmp tracking detail** EXEC command.

  Conditions: This symptom is observed when the **ip igmp explicit-tracking** interface configuration command is enabled and the entries in the cache have expired.

  Workaround: There is no workaround.

- CSCec16481

  A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

  The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

  Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

  http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml.

- CSCec27239

  Symptoms: A Cisco router that processes external link-state advertisements (LSAs) may generate spurious memory access tracebacks or reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that runs Open Shortest Path First version 3 (OSPFv3).

  Workaround: There is no workaround.

- CSCec43772

  Symptoms: When a large number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets is received, the input-queue counters of an interface may slowly increase, eventually causing the interface to become wedged.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(14)SZ3 or Release 12.2(18).

  Workaround: Reload the router.

- CSCin52817

  Symptoms: A Cisco router may reload unexpectedly when you manually reload the router.

  Conditions: This symptom is observed when Open Shortest Path First (OSPF) LSAs are being "maxaged" while you manually reload the router. This situation may occur because of a fluctuating network and is an extreme corner case that cannot be reproduced on demand. The symptom is very unlikely to occur.

  Workaround: There is no workaround.

ISO CLNS

- CSCeb72224

  Symptoms: A Cisco router that is running Intermediate System-to-Intermediate System (IS-IS) may not unset the IS-IS overload bit after a redundancy switchover, preventing the IS-IS connectivity from being restored.

  Conditions: This symptom is observed on a Cisco router that has two Route Processors (RPs) in a redundant configuration.

  Workaround: To restore the IS-IS connectivity, and to prevent the symptom from occurring again, enter the **no set-overload-bit on-startup** router configuration command on the primary RP.

Miscellaneous

- CSCea29102

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

  1. Symptoms: A Route Processor (RP) may reload when you enter the **clear ip bgp *** privileged EXEC command while interfaces flap continuously.

     Conditions: This symptom is observed when Virtual Private Network (VPN) routing/forwarding (VRF) forwarding is configured on the interfaces that flap.

     Workaround: There is no workaround.

  2. Symptoms: An RP may reload when you simultaneously enter the **clear ip bgp *** privileged EXEC command and perform an online insertion and removal (OIR) by entering the **hw-reload reset** EXEC command.

     Conditions: This symptom is observed when you perform an OIR of an interface that has a VRF configuration in which the connected route is learned via a network statement. The connected route is removed when you perform the OIR.

     Workaround: Do not simultaneously enter the **clear ip bgp *** privileged EXEC command and perform an OIR.

- CSCea60559

  Symptoms: The Simple Network Management Protocol (SNMP) agent may use 99 percent of the CPU bandwidth of a Route Processor (RP) for an arbitrarily long time (hours or days), without necessarily generating CPUHOG errors. This situation causes other processes on the router to fail because these processes do not receive the CPU bandwidth that they require:

  - Routes may time out.
  - Tunnels may go down.
  - Accessing the router via a Telnet connection to a network port may become impossible.
  - The command-line interface (CLI) via the console line may become quite slow to respond.

  The output of the **show snmp summary** EXEC command may indicate that the number of requests is "N" while the number of replies that were sent is "N-1." The output of the **show processes cpu | include SN** EXEC command may indicate that the SNMP process uses 99 percent of the CPU bandwidth of the RP.

  Conditions: These symptoms are observed when the MPLS-LSR-MIB MIB is enabled, you query the mplsXCTable or a MIB walk occurs, and there are more than 10,000 Multiprotocol Label Switching (MPLS) labels active. The symptoms are platform independent.

  Workaround: Perform the following steps:

  1. Shut down interfaces to bring the total count of active MPLS labels down to far below 10,000.
  2. Disable the MPLS-LSR-MIB MIB by entering the following sequence of commands:

     ```
     snmp-server view nolsrmib mplsLsrMIB exclude
     snmp-server community public view nolsrmib ro
     snmp-server view nolsrmib iso include
     ```

  Enter the **no shutdown** interface configuration command on all the interfaces that you shut down in Step 1.

- CSCea66218

  Symptoms: When a Tributary Unit Alarm Indication Signal (TU-AIS) is inserted for an E1 tributary on a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) in a Synchronous Payload Envelope (SPE), packet corruption may occur on the adjacent E1.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-STM-1.

  Workaround: There is no workaround.

- CSCea66218

  Symptoms: When a Tributary Unit Alarm Indication Signal (TU-AIS) is inserted for an E1 tributary on a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) in a Synchronous Payload Envelope (SPE), packet corruption may occur on the adjacent E1.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-STM-1.

- CSCeb05093

  Symptoms: A Cisco switch or router may reload when there is insufficient memory available to initialize Cisco IOS Server Load Balancing (SLB), which may occur when SLB is first configured or when the switch or router boots up. When the SLB initialization failure occurs, the following error message appears:

  ```
  % SLB command failed - unable to start slb.
  ```

  Conditions: This symptom is observed when you enter large initialization values for the *init-conn* or *init-sticky* arguments of the **ip slb entries** [**conn** [*init-conn* [*max-conn*]] | **sticky** [*init-sticky* [*max-sticky*]]] global configuration command.

Workaround: Enter smaller initial values for the *init-conn* or *init-sticky* arguments.

- CSCeb06452

  Symptoms: When multicast IP version 6 (IPv6) Cisco Express Forwarding (CEF) is enabled, packets (greater than or equal to 232 bytes) that are forwarded may be corrupted.

  Conditions: This symptom is observed on all Cisco platforms during normal multicast CEF software forwarding.

  Workaround: Use process switching.

- CSCeb08400

  Symptoms: When the MPLS VPN—Carrier Supporting Carrier feature is configured, the output of the **show mpls forwarding-table** user EXEC command may not display remote Virtual Private Network (VPN) routing/forwarding (VRF) prefixes on the provider edge (PE) router.

  Conditions: This symptom is observed when the following sequence of events occurs:

  1. You configure the **mpls ip** global configuration command on the interface of the PE router that connects to the customer edge (CE) router.
  2. You configure VRF instances.
  3. The interface of the PE router that connects to the CE router is present in the VRF database.
  4. You configure the **no mpls ip** global configuration command on the interface of the PE router that connects to the CE router.
  5. You enter the **ip address** interface configuration command for the interface of the PE router that connects to the CE router.
  6. You configure Border Gateway Protocol (BGP) VPN version 4 (VPNv4), and, if needed, you configure Interior Gateway Protocol (IGP) on the interface of the PE router that connects to the CE router.
  7. You reconfigure the **mpls ip** global configuration command on the interface of the PE router that connects to the CE router.

  Workaround: Enter the **clear ip route vrf** *vrf-name* EXEC command on the interface of the PE router that connects to the CE router.

  Alternate Workaround: Reload the PE router.

- CSCeb15038

  Symptoms: Even though you can enable traffic shaping on a physical interface of a Cisco router via the modular QoS CLI (MQC) or the regular command-line interface (CLI), traffic shaping does not take effect for traffic that leaves the physical interface via an egress traffic engineering (TE) tunnel.

  Conditions: This symptom is observed in a Multiprotocol Label Switching (MPLS) environment.

  Workaround: There is no workaround.

- CSCeb24407

  Symptoms: An IP version 6 (IPv6) link local address that has been manually configured by entering the **ipv6 address** *ipv6- address* **link-local** interface configuration command may disappear from the running configuration.

  Conditions: This symptom is observed when you reload the Cisco platform on which the IPv6 link local address is configured or when a switchover between Route Processors (RPs) occurs on this platform.

  Workaround: Reconfigure the IPv6 link local address.

Alternate Workaround: Manually configure the MAC address on the interface on which the IPv6 link local address is configured.

Workaround: There is no workaround.

- CSCeb52270

  Symptoms: An interface of a Cisco router may not be able to receive traffic that is destined for an address that is configured on the router.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(14)S or Release 12.2(18)S and is platform independent. This symptom occurs only if there is a route in a different VPN routing and forwarding instance (VRF) that is attached or connected to the interface. This can happen if the route has been exported from one VRF to another or if a static route in a VRF points to the interface in question.

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

- CSCeb54853

  Symptoms: IP Server Load Balancing (SLB) probes may fail although the output of the **show ip slb reals** privileged EXEC command indicates that the SLB probes are in the operational state.

  Conditions: This symptom is observed when a TCP probe is configured.

  Workaround: There is no workaround.

- CSCeb59165

  Symptoms: A standby card may not be able to switch to the active state.

  Conditions: This symptom is observed in a Redundancy Framework (RF) environment when ATM, High-Level Data Link Control (HDLC), or Frame Relay clients synchronize data during the "standby-bulk" state.

  Workaround: There is no workaround.

- CSCeb65671

  Symptoms: An incorrect virtual circuit (VC) disposition label may be generated, causing packets to drop.

  Conditions: This symptom is observed when VC label attributes, such as a control word setting or a VC type, do not match on a pseudowire.

  Workaround: Toggle the interface on which the pseudowire is configured by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCeb72516

  Symptoms: The **neighbor** *ip-address* **send-label** address family configuration command may not function properly for an IP version 6 (IPv6) Border Gateway Control (BGP) neighbor that is part of a BGP peer group in an IPv6 address family; the functionality of the **send-label** keyword may not be advertised to the peers.

  Conditions: This symptom is observed when you use BGP peer groups with a provider edge (PE) router that is running IPv6 in a Multiprotocol Label Switching (MPLS) environment (referred to as a 6PE router).

  Workaround: Enter the **neighbor** *ip-address* **send-label** address family configuration command for the IPv6 BGP neighbor before you make the IPv6 BGP neighbor part of the BGP peer group in the IPv6 address family.

- CSCeb72859

  Symptoms: Bulk configuration synchronization may be triggered when you enter the exit command in any configuration mode.

  Conditions: This symptom is observed on Cisco platforms that support high availability (HA) configuration synchronization.

  Workaround: There is no workaround.

- CSCeb76341

  Symptoms: A label may not be assigned for a peer provider edge (PE) router.

  Conditions: This symptom is observed on a Cisco 7500 series and a Cisco 12000 series in a Virtual Private Network (VPN) configuration with multiple route reflectors (RRs) and label controlled ATM (LC-ATM) links between PE routers. The symptom may also occur on other platforms.

  Workaround: There is no workaround.

- CSCeb77318

  Symptoms: When a load-balanced server uses the Don't Fragment (DF) bit in its responses, and fragmentation is needed in order to reach the client, a gateway may report this situation by using Internet Control Message Protocol (ICMP), message type 3 (destination unreachable), code 4 (datagram too big). The gateway's message is translated at a router and forwarded to the correct server, but the checksum may be invalid, causing the server to ignore the message and preventing the segment size from being decreased.

  Conditions: This symptom is observed when you use Cisco IOS Server Load Balancing (SLB) with Network Address Translation (NAT).

  Workaround: Do not configure NAT when you use Cisco IOS SLB.

- CSCec03066

  Symptoms: When you enter the **no ipv6 route** global configuration command, an IP version 6 (IPv6) static route that is deleted by the command may not be deleted from the IPv6 routing table.

  Conditions: This symptom is observed when two IPv6 static routes, each with a different administrative distance, point to the same destination.

  Workaround: Enter the **clear ipv6 route** *ipv6-prefix/prefix-length* privileged EXEC command to delete the IPv6 static route from the IPv6 routing table.

- CSCec03782

  Symptoms: A memory allocation failure may occur on compiled access control list (ACL) tables. There may be continued attempts to recompile the ACLs that fail.

  Conditions: This symptom is observed when compiled ACLs are enabled by entering the **access-list compiled** global configuration command, and the total number of ACL entries is relatively large (over 1500 lines). Random or constantly changing traffic patterns may cause the compiled ACL tables to grow to the point at which memory fragmentation causes the memory allocation failure.

  Workaround: Disable and then reenable the compiled ACLs by entering the **no access-list compiled** global configuration command followed by the **access-list compiled** global configuration command.

  Alternate Workaround: Completely disable the compiled ACLs.

  Second Alternate Workaround: ACLs may sometimes be rearranged to make the list shorter or less complex. This will reduce the memory requirements. Large ACLs used for Border Gateway Protocol (BGP) route prefixes may be converted to use a prefix list configuration instead.

- CSCec11541

  Symptoms: It may take up to 10 minutes for a Cisco router to read or download a configuration that contains 500 traffic engineering (TE) tunnels. When the configuration has been read or downloaded, the CPU utilization may be very high, even when the TE tunnels are down. The symptom may also occur when a smaller numbers of TE tunnels is configured, but to a lesser extent.

  Conditions: This symptom is observed on a Cisco router that is configured for Multiprotocol Label Switching (MPLS).

  Workaround: There is no workaround.

- CSCec14083

  Symptoms: Any Cisco vendor-specific attribute (VSA) may be rejected during authorization, even though the VSA is valid and supported.

  Conditions: This symptom is observed in Cisco IOS Release 12.2 S when an exception routine occurs.

  Workaround: There is no workaround.

- CSCec14424

  Symptoms: High CPU utilization may occur on the Route Processor (RP) of a Parallel Express Forwarding (PXF) processor of a Network Service Engine 100 (NSE-100).

  Conditions: This symptom is observed on a Cisco 7304 that is configured for tag switching when any of the following protocols or features are also configured:

  - Tag Distribution Protocol (TDP)
  - Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN)
  - VPN Routing/Forwarding Lite (VRF Lite)
  - MPLS-traffic engineering (MPLS-TE)

  Workaround: There is no workaround.

- CSCec26563

  Symptoms: A Cisco router that is in the process of setting up a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed under unusual circumstances when the following series of events occur:

  - You disable MPLS TE tunnels on the router by entering the **no mpls traffic-eng tunnels** global configuration command.
  - You enter one of the following MPLS TE interface configuration commands on an interface:

    mpls traffic-eng attribute-flags *attributes*

    mpls traffic-eng administrative-weight *weight*

    mpls traffic-eng flooding thresholds
  - The router attempts to set up a TE tunnel over this interface while the interface state changes to "up." (This event causes the router to reload.)

  Workaround: Before you enter any of the above-mentioned MPLS TE interface configuration commands on the interface, ensure that MPLS TE tunnels are enabled on the interface by entering the **mpls traffic-eng tunnels** interface configuration command. Before you disable MPLS TE tunnels on the interface by entering the **no mpls traffic-eng tunnels** interface configuration command, ensure that any of the above-mentioned MPLS TE interface configuration commands are removed from the interface.

- CSCec28094

  Symptoms: A Cisco 7304 that is configured to reboot automatically may not do so.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Processing Engine G-100 (NPE-G100) and occurs when the router goes down after a fatal exception.

  Workaround: Power-cycle the router.

  Alternate Workaround: Send a break signal via the console connection to the NPE-G100 while the NPE-G100 is in the process of rebooting automatically. Then, from ROM monitor (ROMmon) mode, reset the router.

- CSCec29504

  Symptoms: A Cisco router that is configured with redundant Route Processors (RPs) may reload unexpectedly.

  Conditions: This symptom is observed when the RPs use the Checkpoint Facility (CF) with bundled clients.

  Workaround: There is no workaround.

- CSCec33834

  Symptoms: ATM Cell Loss Priority (CLP) marking may not function on a Cisco 7304 that is configured with a Network Processing Engine G-100 (NPE-G100).

  Conditions: This symptom is observed when a policy map is configured for ATM CLP marking and is attached to an ATM virtual circuit (VC) that is configured on an output interface of a 2-port OC-3 ATM line card.

  The symptom occurs because the NPE-G100 fails to pass the CLP bit indication for each egress packet to the ATM VC that is configured on the output interface of the 2-port OC-3 ATM line card, preventing the CLP bit in the ATM output cells from being marked.

  Workaround: There is no workaround. Note that ATM CLP marking does not function but that ATM functionality is not affected.

- CSCec34830

  Symptoms: The Parallel Express Forwarding (PXF) processor of a Cisco 7304 may pause indefinitely or reload unexpectedly.

  Conditions: This symptom is observed when a Multiprotocol Label Switching (MPLS) packet is received on a generic routing encapsulation (GRE) tunnel that is configured on the Cisco 7304.

  Workaround: There is no workaround.

- CSCec39988

  Symptoms: The load rate of interface description blocks (IDBs) may be incorrect.

  Conditions: This symptom is observed on a Cisco 7304 when the **tunnel mpls traffic-eng auto-bw** interface configuration command is configured on Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

  Workaround: There is no workaround.

- CSCec42645

  Symptoms: An ATM permanent virtual circuit (PVC) that is created after a high availability (HA) switchover has occurred may not come up.

  Conditions: This symptom is observed on a Cisco 7304 when the active Network Service Engine (NSE) has come up from the standby state.

  Workaround: Configure the ATM PVC before an HA switchover occurs.

- CSCec43129

  Symptoms: A Cisco 7304 may pause indefinitely or reload unexpectedly while processing statistics packets from the Parallel Express Forwarding (PXF) processor. When the PXF processor processes quality of service (QoS) traffic, the PXF processor sends these statistics packets to the Route Processor (RP).

  Even if the Cisco 7304 does not pause indefinitely or reload unexpectedly, the QoS statistics from different interfaces or classes, or from both, may become mixed up in such a way that there are no QoS statistics for a class, or traffic from one class on an interface is reported as coming from a different class.

  The output of the **show policy-map interface** EXEC command displays the QoS statistics, which are also accessible through the CISCO-CLASS-BASED-QOS-MIB MIB.

  Conditions: This symptom is observed when you boot up the Cisco 7304 or when you make any QoS configuration changes while there are service policies attached to interfaces, subinterfaces, or ATM virtual circuits (VCs). The following commands change the QoS configuration:

  - **class-map**
  - **match**
  - **policy-map**
  - **class**
  - **set**
  - **police**
  - **bandwidth**
  - **priority**
  - **random-detect**
  - **shape**
  - **queue-limit**
  - **access-list**

  Note The **access-list** global configuration command is only relevant if the access control list (ACL) that is stated in the command is referred to by at least one **match access-group** class-map configuration command.

  Workaround: Reload the Cisco 7304 without any service policy applied to any interface, subinterface, or ATM VC. When the Cisco 7304 has booted up, manually apply the service policies to the interfaces, subinterfaces, or ATM VCs.

  Before you change any QoS configuration (as described in the conditions), detach all service policies from the interfaces, subinterfaces, or ATM VCs. Then, make the necessary changes and reattach the service policies.

- CSCec43308

  Symptom: The **ip default-network** global configuration command may be ignored by the Parallel Express Forwarding (PXF) processor, causing packets that do not have a route specified to be dropped instead of being forwarded to the default network.

Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Service Engine 100 (NSE-100).

Workaround: Disable the PXF processor by entering the **no ip pxf** global configuration command.

- CSCec43621

  Symptoms: It may take a very long time (several hours) for Cisco 7304 to boot up.

  Conditions: This symptom is observed when the Cisco 7304 has many interfaces that are configured by using modular QoS CLI (MQC).

  Workaround: There is no workaround.

- CSCec46244

  Symptoms: A Cisco 7304 may reload unexpectedly.

  Conditions: This symptom is observed when you enter the **clear counters** EXEC command.

  Workaround: There is no workaround.

- CSCec50743

  Symptoms: A Cisco 7304 may reload unexpectedly after a high availability (HA) switchover has occurred.

  Conditions: This symptom is observed when the router is configured with 255 point-to-multipoint permanent virtual circuits (PVCs).

  Workaround: There is no workaround.

- CSCec52267

  Symptoms: The Parallel Express Forwarding (PXF) processor of a Network Service Engine 100 (NSE-100) may pause indefinitely or reload unexpectedly when the forwarding path is switched from IP to Multiprotocol Label Switching (MPLS).

  Conditions: This symptom is observed when traffic is being forwarded and the Border Gateway Protocol (BGP) peer or another routing protocol peer goes down, causing the forwarding path to be switched from IP to MPLS.

  Workaround: Ensure that both the primary path and the backup path are either IP or MPLS, but not a mixture of both.

- CSCec52753

  Symptoms: You may not be able to send a ping or traffic through the interface of an 8-port ATM Inverse Mux E1 port adapter (PA-A3-8E1IMA) or an 8-port ATM Inverse Mux T1 port adapter (PA-A3-8T1IMA). Packets are dropped without any counters being incremented (that is, silent drops occur).

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2 S and that is configured with a Network Processing Engine G-100 (NPE-G100), a 7300-CC-PA carrier card, and a PA-A3-8E1IMA or PA-A3-8T1IMA.

  Workaround: There is no workaround.

- CSCec61844

  Symptoms: A Cisco 7304 may reload unexpectedly when you perform an online insertion and removal (OIR) of an ATM line card or ATM port adapter.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Processing Engine G-100 (NPE-G100) when the router processes traffic.

  Workaround: There is no workaround.

- CSCin59908

  Symptoms: When NetFlow protocol-port aggregation is configured, a Cisco 7304 may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S and that is configured with a Network Service Engine 100 (NSE-100) when NetFlow accounting is enabled in the Parallel Express Forwarding (PXF) processor of the NSE-100.

  Workaround: There is no workaround.

- CSCec65084

  Symptoms: When you configure Ethernet over Multiprotocol Label Switching (EoMPLS) on a Cisco 7304, an "ip offset sanity check drop" error message may be displayed, and the end-to-end connectivity may appear to be terminated.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Service Engine 100 (NSE-100).

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCec29952

  Symptoms: A Cisco router will not form a Border Gateway Protocol neighbor under the **address-family ipv4** [**vrf** *vrf-name*] router configuration command if Message Digest 5 (MD5) authentication is configured.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(18)S.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCea43177

  Symptoms: A Cisco router may reload while you attempt to set up a Frame Relay switched virtual circuit (SVC).

  Conditions: This symptom is observed when you attempt to set up a Frame Relay SVC by using a data-link connection identifier (DLCI) that is already in use; for example, when a permanent virtual circuit (PVC) is configured by using the same DLCI.

  Workaround: When a PVC is configured by using the same DLCI, remove the PVC configuration before you attempt to set up the Frame Relay SVC.

- CSCeb33417

  Symptoms: A router may reload when it tries to add a permanent virtual circuit (PVC) to a bundle link.

  Conditions: This symptom is observed when a normal Local Management Interface (LMI) frame is received without the User-Network Interface (UNI) fragmentation header. This causes the frame to be processed on the bundle link instead of on the bundle.

  Workaround: There is no workaround.

- CSCeb72381

  Symptoms: When you configure Open Shortest Path First (OSPF) on a new Multilink Frame Relay (MFR) interface, the following traceback may be displayed:

  ```
  %OSPF-6-ZERO_BANDWIDTH: interface MFR100 has zero bandwidth
  ```

  Conditions: This symptom is observed on a Cisco router when you configure a new MFR interface or after the router has rebooted.

  Workaround: There is no workaround.

- CSCin53115

  Symptoms: It may not be possible to add a bundle link to a Multilink Frame Relay (MFR) interface.

  Conditions: This symptom is observed on a Cisco router that has data-link connection identifier (DLCI) 896 configured.

  Workaround: Do not configure DLCI 896.

Resolved Caveats—Cisco IOS Release 12.2(18)S13

Cisco IOS Release 12.2(18)S13 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S13 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCed09685

  Symptoms: When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

  Conditions: This problem happens only with command accounting enabled.

  Workaround: Disable command accounting.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml.

- CSCsf07847

  Symptoms: Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  Conditions: This issue occurs in Cisco IOS software images that have the fix for CSCse85200.

  Workaround: Disable CDP on interfaces where CDP is not required.

Further Problem Description: Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

- CSCsj44081

  Cisco IOS software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message when it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

  ```
  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

  Recommended Action: Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORR UPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

IP Routing Protocols

- CSCin95836

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

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

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

  NHRP is not enabled by default for Cisco IOS.

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

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Miscellaneous

- CSCeb21064

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

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

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

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

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

- CSCef77013

  Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also result in a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

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

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml.

- CSCin78324

  Symptoms: A Cisco router that is configured with a PA-MC-8TE1 port adapter may hang.

  Conditions: This symptom is observed on a Cisco 7200 VXR router that has a PA-MC-8TE1 port adapter and that is configured for IPSec encryption, either via tunnel protection or via a crypto map. The symptom may also occur on other platforms and in other releases.

  Workaround: Disable IPSec encryption.

- CSCsb12598

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- CSCsb45696

  Symptoms: A platform may reload in response to malformed 802.1x EAP traffic.

  Conditions: This symptom is observed on a Cisco Catalyst 3750 that runs Cisco IOS Release 12.2(25)SEC. However, the symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCsc72722

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

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

  Workaround: There is no workaround.

- 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.

- CSCsd81407

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

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254

  - Real-time Transport Protocol (RTP)
  - Facsimile reception

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

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

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

- CSCsd92405

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- CSCsd95616

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

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

- CSCse56501

  Symptoms: When two sockets are bound to the same port, the first File Descriptor always receives the requests.

  Conditions: This symptom is observed on a Cisco router when two sockets such as one IPv4 socket and one IPv6 socket are connected to the same UDP port.

Workaround: Use different UDP ports for different sockets.

- CSCse68138

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

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

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

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

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

- CSCsf04754

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

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

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

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

- CSCsg40567

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

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

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

- CSCsg70474

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

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254

  - Real-time Transport Protocol (RTP)
  - Facsimile reception

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

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

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

- CSCsi60004

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

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

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

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

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

TCP/IP Host-Mode Services

- CSCse05736

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

  Conditions: This symptom is seen under the following conditions:

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

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

Resolved Caveats—Cisco IOS Release 12.2(18)S12

Cisco IOS Release 12.2(18)S12 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S12 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml.

- 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.

- 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.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Miscellaneous

- CSCec06146

  Symptoms: A serial interface of a channelized port adapter may fail to enter the “up/up” state when you initially configure the interface or after a number of reconfigurations.

  Conditions: This symptom is observed on a channelized port adapter that is installed in a Cisco 7500 series or Cisco 7600 series when the following sequence of events occurs:

  1. You configure an interface by entering the **controller e3** *slot*/*port* global configuration command followed by the **e1** *line-number* **channel-group** *channel* **timeslots** *range* controller configuration command.
  2. You delete the interface by entering the **controller e3** *slot*/*port* global configuration command followed by the **no e1** *line-number* **channel-group** *channel* controller configuration command.
  3. You reconfigure the interface by entering the commands listed in Step 1.

  Although the symptom may occur when you initially configure the interface, it is more likely to occur when you configure, delete, and reconfigure the interface several times. In addition, the symptom may also occur after a link flap of an interface of one of the channelized cards.

  The symptom may occur on any of the following channelized port adapters: PA-MC-T3, PA-MC-2T3, PA-MC-xT1 (x = 2,4,8), PA-MC-xE1 (x = 2,4,8), and PA-MCX-xTE1 (x = 2,4,8).

  Workaround: When the interface does not enter the “up/up” state, configure the interface again.

- CSCec80902

  Symptoms: A Cisco 7500 series that is configured for Hierarchical Queuing Framework (HQF) may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed when you attempt to print queue statistics for priority classes within the same layer of a policy map.

  Workaround: There is no workaround.

- 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.

- CSCed76109

  Symptoms: On a Cisco 7500 series that is equipped with Versatile Interface Processors (VIPs) with ATM port adapters, the ATM PVCs may not come back up after the ATM interface flaps. This occurs because the interfaces in the VIP do not transmit any packets but still process incoming traffic.

  Conditions: This symptom is observed in a dLFIoATM environment in which distributed Class Based Weighted Fair Queueing (dCBWFQ) is configured on PPPoATM virtual templates.

  Workaround: Apply any kind of distributed queueing on any interface or subinterface of the affected VIP. Doing so triggers all interfaces to start transmitting again, enabling the ATM PVCs to come back up.

- CSCef56327

  Symptoms: You may not be able to configure the **clock source line** command during the configuration of the SONET controller on a Cisco router in which a PA-MC-STM1 port adapter is installed.

  When you enter the **clock source line** command during the configuration of the SONET controller, the output of the **show running-config** command indicates that the clock source is set to line. However, the output of the **show controllers sonet** command indicates that the clock is set to internal, and when you enter the **show running-config** command again, the output indicates this time that the clock source is set to internal.

  Conditions: This symptom is observed when the PA-MC-STM1 port adapter is connected back-to-back via dark fiber to another PA-MC-STM1 port adapter.

  Workaround: Enter the **overhead s1byte ignore** command on the SONET controller before you configure the clock source.

- 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.

- 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.

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(18)S11

Cisco IOS Release 12.2(18)S11 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S11 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCec87736

  Symptoms: TX Simple Network Management Protocol (SNMP) counters do not update on Fast Ethernet subinterfaces for distributed Cisco Express Forwarding (dCEF) traffic.

  Conditions: This symptom is observed on Cisco IOS Release 12.0(26)S and Release 12.3. The hardware is DEC21140A, and the interface receiving the traffic is not located on the same Versatile Interface Processor (VIP). The symptom may also occur in other releases.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeb17467

  Symptoms: A Cisco router may reload when Border Gateway Protocol (BGP) is configured to carry Virtual Private Network version 4 (VPNv4) routes.

  Conditions: This symptom is observed when VPNv4 import processing occurs simultaneously with a BGP neighbor reset, for example, when a VPN routing and forwarding (VRF) instance is configured and you enter the **clear ip bgp *** privileged EXEC command.

  Workaround: There is no workaround.

- CSCee41172

  Symptoms: The **maximum-paths import** *number-of-paths* command enables a VRF to import additional paths in addition to the bestpath. If the original path of the import path is withdrawn, wrong import paths may be purged. This situation may cause traffic disruption up to 15 seconds.

  Conditions: This symptom is observed when the original path of the best import path is withdrawn and the import path is at the end of the path list (that is, the one learned the very first). In this situation, all import paths that are derived from other paths may be purged as well. If the imported net has only import paths, the net may not be reachable until other paths are reimported.

  Workaround: Ensure that the import path is at the top of the path list or use the same route descriptor (RD) for all import paths.

Miscellaneous

- CSCed32385

  Symptom: When a RPR, RPR+, or SSO switchover occurs on a Cisco 7500 series, a “cbus complex” error message may be generated, all VIPS may reload, and the following error message is generated:

  ```
  HA-2-NO_QUIESCE: Slot <slot#> did not quiesce, it will be disabled and then reloaded.
  ```

  Similar symptoms may occur when the **service single-slot-reload-enable** command is not configured on the router. However, in this situation, the “cbus complex” error message is generated after the “HA-2-NO_QUIESCE” error message.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S.

Workaround: There is no workaround.

- CSCed81317

  Symptoms: When an import map is configured on a VPN Routing/Forwarding (VRF) instance, the CE-learned routes are filtered out, preventing them from appearing in the VRF routing table.

  Conditions: This symptom is observed when the **import map** *word* command is configured as part of the VRF configuration. Note that eBGP routes are not filtered out.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(18)S10

Cisco IOS Release 12.2(18)S10 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S10 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCef68103

  Symptoms: A Cisco 7200 series may reload when flash disk 1 is accessed.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2S only when the router is configured with both an NPE-G1 and an I/O controller.

  Workaround: Ensure that only flash disk 2 is accessed.

- 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.

Interfaces and Bridging

- CSCin86455

  Symptoms: Auto-provisioning may be disabled on a Cisco router that is configured with a PA-A3 port adapter.

  Conditions: This symptom is observed when a VC class that is configured for create on-demand is attached to the main ATM interface and then the create on-demand configuration is removed and re-applied to the VC class.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface of the PA-A3 port adapter.

IP Routing Protocols

- CSCed67358

  Symptoms: An IPv6 PIM neighbor may be down after changing the PIM configuration.

Conditions: This symptom is observed when the **no ipv6 pim** command is entered on some subinterfaces of a physical Ethernet interface and when PIM is enabled on several subinterfaces of the same physical Ethernet interface. The symptom affects both IPv4 and IPv6, and configurations with multicast and OSPF Hello messages.

Workaround: There is no workaround.

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

ISO CLNS

- CSCeh61778

  Symptom: A Cisco device running IOS and enabled for Intermediate System-to- Intermediate System (IS-IS) routing protocol may reset with a SYS-2-WATCHDOG error from a specifically crafted malformed IS-IS packet. The IS-IS protocol is not enabled by default.

  Conditions: The IS-IS crafted malformed IS-IS Packet that requires processing will not be forwarded across a Level 1/Level 2 boundary. The specifically crafted malformed IS-IS packet would require local attachment to either a Level 1 or Level 2 router. A Cisco device receiving the malformed IS-IS packet will forward the malformed packet to its neighbors, and may reset.

  Workaround: There is no workaround. Enabling IS-IS Authentication is seen as a best practice, and can be leveraged as a mitigation technique.

Miscellaneous

- CSCin31767

  Symptoms: A Cisco router may reload when you enter the **show atm map** privileged EXEC command.

  Conditions: This symptom is observed on all Cisco routers after you have first deleted a subinterface on which a static map bundle was configured.

  Workaround: First remove the static map bundle; then, delete the subinterface.

Resolved Caveats—Cisco IOS Release 12.2(18)S9

Cisco IOS Release 12.2(18)S9 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S9 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsa81379

  NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

The removal of NetFlow Feature Acceleration does not affect any other aspects of NetFlow operation, for example Access-list processing. The features are separate and distinct.

Cisco Express Forwarding (CEF) supersedes the deprecated NetFlow Feature Acceleration.

Additionally, the following MIB objects and OIDs have been deprecated and removed from the NetFlow MIB (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration          1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable    1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot         1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot            1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable                 1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry                 1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType                  1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot                  1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive                1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches              1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches              1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges         1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

Miscellaneous

- CSCdz84963

  Symptoms: A VIP that is installed in a Cisco 7500 series runs out of memory after some time of operation. The output of the **show processes memory** command shows that the CEF IPC background process holds a lot of memory, and the output of the **show buffers** command on the VIP shows that many buffers are used by IPC.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(18)S8 after dCEF is enabled.

  Workaround: Disable dCEF. Note that the symptom does not occur in Release 12.2(14)S13.

- CSCec86420

  Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

  The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

  This bug is a complementary fix to CSCeb56909 which addresses this vulnerability.

  More details can be found in the security advisory which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml.

- CSCef61610

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Resolved Caveats—Cisco IOS Release 12.2(18)S8

Cisco IOS Release 12.2(18)S8 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S8 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCdz27562

  Symptoms: Executing an snmpwalk command on a loopback interface causes a response that is sourced from the IP address of the physical interface.

  Conditions: This symptom is observed on a Cisco 12000 series but also affects other platforms.

  Workaround: Execute the snmpwalk command on the physical interface.

Interfaces and Bridging

- CSCef00510

  Symptoms: Packets that originate from a Cisco router that is configured with a PA-MC-8TE1+ port adapter may be corrupted and have an invalid FCS. These packets may have the address and control fields compressed even when PFC and ACFC options are explicitly disabled.

  Conditions: This symptom is observed only when traffic is presented simultaneously on several B-channels.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Miscellaneous

- CSCdz72292

  Symptoms: An interface of an 8-port multichannel E1 port adapter (PA-MC-8E1) may start to flap and may finally pause indefinitely with the output queue stuck. The output of the **show interfaces** privileged EXEC command may show information similar to the following:

```
Serial1/1:1 is up, line protocol is up
  Encapsulation HDLC, crc 16, Data non-inverted
  Keepalive set (120 sec)
  Last input 00:00:03, output 04:14:23, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 21952
  Queueing strategy: weighted fair
  Output queue: 30/4000/64/21855 (size/max total/threshold/drops)
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     43903807 packets input, 3646461183 bytes, 0 no buffer
     Received 0 broadcasts, 321 runts, 0 giants, 0 throttles
     5160 input errors, 4 CRC, 0 frame, 0 overrun, 0 ignored, 2945 abort
     42026998 packets output, 2185017012 bytes, 0 underruns
```

```
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     31 carrier transitions
  no alarm present
  Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags
```

The following traceback may be observed in the router log:

```
%LINK-4-TOOBIG: Interface Serial60:1, Output packet size of 1526 bytes too big
 Traceback=  0x604007F8  0x604A927C  0x6084E4D4  0x6057425C  0x60CE921C 0x60CE55EC
%LINK-4-TOOBIG: Interface Serial20:1, Output packet size of 1526 bytes too big
 Traceback=  0x604007F8  0x604A927C  0x6084E4D4  0x6057425C  0x60CE921C 0x60CE55EC
```

Conditions: This symptom is observed on a Cisco router after a few weeks of normal operation.

Workaround: There is no workaround.

- CSCea87364

  Symptoms: Distributed Cisco Express Forwarding (DCEF) may become disabled on a Versatile Interface Processor (VIP) or Cisco 12000 series line card (LC), and the following error message may appear on the console:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 12: Window did not open, LC to RP IPC is
  non-operational
  ```

  Conditions: This symptom is observed on a Cisco 7500 series VIP2-50 and VIP4- 80 in which ATM OC-3 port adapters such as the PA-A1-OC3 or PA-A3-OC3 are installed when the Cisco 7500 series is upgraded to Cisco IOS Release 12.0(24) S or Release 12.0(24)S1. This symptom is also observed on a Cisco 12000 series LC during significant, prolonged routing table churn.

  Workaround: Reload CEF on the VIP or LC by entering the **clear cef linecard** *slot-number* EXEC command.

  Alternate Workaround: Restart the VIP by performing an online insertion and removal (OIR). Restart the LC by executing the **hw-module slot** *slot #* **reload** command.

- CSCeb52181

  Symptoms: A Cisco platform that accesses the “system:/vfiles/tmstats_ascii” virtual file (for example, via “more system:/vfiles/tmstats_ascii”) may crash because of bus error.

  Conditions: This symptom is observed under normal working conditions when no configuration changes are made on a Cisco platform that runs Cisco IOS Release 12.0S, 12.1E, 12.2, 12.2.S or 12.3. When the “system:/vfiles/tmstats_ascii” virtual file is not used, the symptom does not occur.

  Workaround: There is no workaround.

- CSCec31781

  Symptoms: When you enter the **redundancy force-switchover** privileged EXEC command on a Cisco 7500 series, a Versatile Interface Processor (VIP) may reload when the router returns to the Stateful Switchover (SSO) mode.

  Conditions: This symptom is observed on a Cisco 7500 series that runs the rsp-pv-mz image of Cisco IOS Release 12.0(25)S1 but may also occur in other releases.

  Workaround: There is no workaround.

- CSCed92837

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series, the standby Route Switch Processor (RSP) my hang just before downloading the image. This situation may prevent the router from entering the STANDBY-HOT state and from being capable to perform a switchover until the standby RSP is reset.

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.0S or 12.2S and that is configured for SSO/Nonstop Forwarding (NSF).

  Workaround: There is no workaround. After the problem occurs, you can recover the router by either waiting for an IPC timer to expire (the default time is 30 minutes) or by entering the **hw-module sec-cpu reset** command.

- CSCed95499

  Symptoms: A Cisco router may crash if a PA driver attempts to convert an uncached iomem address to a cached iomem address.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

  Workaround: There is no workaround.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP “source quench” messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef67682

  Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml contain fixes for this issue.

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

- CSCeg08629

  Symptoms: A Cisco 7500 series may generate CCB playback errors and reload the secondary Route Switch Processor (RSP).

  Conditions: This symptom is observed when there are channelized T3 port adapters installed in the router and when a channel-group parameter is configured before the channel group is created. To recover from the symptoms, reload the router.

  Workaround: Configure the channel-group via the **t1** *t1-line-number* **channel-group** *channel-group-number* **timeslots** *list-of-timeslots* command before you configure any options such as framing of FDL on the channel group.

- CSCeg67788

  Symptoms: The 5-minute output rate in the output of the **show interfaces** command is incorrect for serial interfaces that are configured on a PA-MC-8TE1+ port adapter.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2S or Release 12.3 and that is configured with a PA-MC-8TE1+ port adapter.

  Workaround: There is no workaround.

- CSCuk51673

  Symptoms: Distributed Cisco Express Forwarding (DCEF) may become disabled and the following error message may appear on the console:

  ```
  %FIB-3-NOMEM: Malloc Failure, disabling DCEF %FIB-2-FIBDOWN: CEF has been disabled
  due to a low memory condition.
  ```

  Conditions: This symptom is observed on a Cisco platform that is configured for DCEF. The occurrence of the symptom depends on how much memory is allocated at runtime.

  Workaround: There is no workaround. After the symptom has occurred, re-enable DCEF by entering the **ip cef distributed** command.

- CSCuk55193

  Symptoms: On a router that runs Cisco IOS Release 12.2S and that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), a configuration change that causes one or more LDP sessions to be terminated may cause the router to reload in a manner similar to the following:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x64, pc=0x41285C40,
  ra=0x41285C30, sp=0x44B1C378
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x64, pc=0x41285C40,
  ra=0x41285C30, sp=0x44B1C378
  TLB (store) exception, CPU signal 10, PC = 0x41285C40
  ```

  The symptom may occur with either LDP or Tag Distribution Protocol (TDP).

  Conditions: This symptom is extremely unlikely to occur and requires a very unlikely timing of events between LDP and TCP. The symptom may occur in the following releases and their rebuilds: Release 12.2(18)S, 12.2(20)S, 12.2(22)S, and 12.2(25)S.

  There are many configuration commands that may trigger the symptom, including entering the **no ip vrf** command to remove a VRF that has LDP-enabled interfaces, entering the **no mpls ldp router-id** command to trigger a change to the LDP router ID, or entering the **no mpls ip** interface configuration command to disable LDP on an interface.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCec83030

  Symptoms: A parity error on a Versatile Interface Processor (VIP) card may cause other VIPs to go to a wedged state.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(18)S7

Cisco IOS Release 12.2(18)S7 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S7 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial-In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

IP Routing Protocols

- CSCec22723

  Symptoms: A router may unexpectedly reload because of a watchdog timeout or bus error in OSPF.

  Conditions: This symptom is observed when iSPF is configured under OSPF.

  Workaround: Remove the iSPF configuration from OSPF by entering the **no ispf** command.

- CSCed60800

  Symptoms: The withdraw message of a multipath (not bestpath) from a BGP neighbor deletes the path from the BGP table but it does not uninstall the route from the IP routing table.

  Conditions: This symptom is observed when the **maximum-paths eibgp** command or **maximum-paths ibgp** command is configured.

  Workaround: Enter the **clear ip bgp *** or disable the **maximum-paths eibgp** command or **maximum-paths ibgp** command.

  Alternate Workaround: Ensure that the number of possible EBGP peers is less or equal to two. In this situation, the symptom is transient and not obviously noticeable.

- CSCee59315

  Symptoms: A BGP VPNv4 table may contain paths that may be imported from deleted BGP table entries or from table entries that have a different prefix from the importing prefix.

  ```
  An example of a path from a deleted BGP table entry is as follows:
  Router# sh ip bgp v v vpn2 192.168.0.0
  BGP routing table entry for 200:2:192.168.0.0/32, version 52
  Paths: (1 available, best #1, table vpn2)
    Advertised to non peer-group peers:
    10.4.1.2
  ```

```
  2 100, imported path from 2829:2829:185404173:11.13.11.13/-53
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:3
```

The entry that this path is imported from has been removed from the table and its memory contents contain an incorrect pattern. When the incorrect pattern is displayed as a prefix, it appear as "2829:2829:185404173:11.13.11.13/-53".

A mismatched prefix appears as follows:

```
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 54
Paths: (2 available, best #1, table vpn2)
Flag: 0x820
  Advertised to non peer-group peers:
  10.10.10.10 10.20.20.20
  2
    10.4.1.2 from 10.4.1.2 (10.4.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:2
  2 100, imported path from 200:2:172.16.0.0/24
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external
      Extended Community: RT:1:3
```

This BGP VPNv4 table entry is for prefix 192.168.0.0/32 but it shows that a path is imported from 172.16.0.0/24. This situation occurs when a path has a link to a deleted BGP table entry, and then the memory for the deleted entry is reused for a new table entry of which the prefix may not match with the importing entry.

Conditions: These symptoms are observed when you enter the **maximum-paths import** *number* command in router BGP address-family IPv4 VRF mode. The *number* argument indicates the number of paths to import from one VRF to another.

Workaround: Remove the **maximum-paths import** *number* command from the router BGP address-family IPv4 VRF mode.

Miscellaneous

- CSCec10116

  Symptoms: An MPLS VPN PE router uses a source address from its global routing table for some packets that originate in one of its VRF interfaces.

  Conditions: This symptom is observed when an MPLS VPN PE router replies to an ICMP Echo Request that was sent from a VRF interface of another router via the MPLS backbone to the network or broadcast address of the VRF interface on the MPLS VPN PE router.

  Workaround: There is no workaround.

- CSCec72813

  Symptoms: Spurious memory access errors may occur when you configure a class map by entering the **match ip** command.

  Conditions: This symptom is observed on a Cisco 7304.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(18)S6

Cisco IOS Release 12.2(18)S6 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S6 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCea36491

  Symptoms: When a Telnet session is made to a router after a VTY session pauses indefinitely, the user in the Telnet session may not be able to enter the configuration mode. When these symptoms occur, interfaces may enter the wedged state with Simple Network Management Protocol (SNMP) traffic.

  Conditions: This behavior is observed on ATM and Packet over SONET (POS) interfaces. This behavior is not platform-specific.

  Workaround: Disable Simple Network Management Protocol (SNMP) configuration traps by entering the **no snmp-server enable traps** config global configuration command.

- CSCed88768

  Symptoms: Certain type-7 encrypted forms of passwords may not work.

  Conditions: This symptom is observed when you upgrade a Cisco router to Cisco IOS Release 12.2(18)S or a release that is based on Release 12.2(18)S such as Release 12.2(18)SE, 12.2(18)SV, or 12.2(18)SW.

  Workaround: When the upgrade is complete, reconfigure the same password as you used before the software upgrade.

- CSCee58479

  Symptoms: When you configure an interface of a PA-MC-8TE1 on a Cisco 7200 series, the router to which the interface of the PA-MC-8TE1 is connected at the other end may crash.

  Conditions: This symptom is observed when the interface of the PA-MC-8TE1 functions in channelization mode and when CDP is enabled.

  Workaround: Disable CDP globally by entering the **no cdp run** global configuration command or by entering the **no cdp enable** interface configuration command on the interface of the router to which the PA-MC-8TE1 interface is connected at the other end.

- CSCef46191

  A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

  Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

The Advisory is available at
http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

ISO CLNS

- CSCec39973

  Symptoms: A router that runs Intermediate System-to-Intermediate System (IS- IS) may reload unexpectedly when there are a lot of adjacencies that continue to flap.

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

  In Release 12.0 S, the symptom may occur when you enter the **router isis** global configuration command followed by the **fast- flood** router configuration command.

  In Release 12.3, the symptom may occur when you enter the **router isis** global configuration command followed by the **ip fast- convergence** router configuration command.

  Workarounds: Prevent IS-IS adjacencies from flapping. There is no other workaround for Release 12.2 S.

  For Release 12.0 S, do not enter the **router isis** global configuration command followed by the **fast-flood** router configuration command.

  For Release 12.3, do not enter the **router isis** global configuration command followed by the **ip fast-convergence** router configuration command.

Miscellaneous

- CSCeb79911

  Symptoms: Backward explicit congestion notification (BECN) packets may be dropped by an Any Transport over Multiprotocol Label Switching (AToM) tunnel.

  Conditions: This symptom is observed when you configure AToM in the network core, the network core contains Frame Relay interfaces, and BECN is enabled.

  Workaround: There is no workaround.

- CSCed45942

  Symptoms: A router with a configuration size that is larger than the NVRAM size reloads because of a bus error and stack overflow or stack corruption when you enter the **show config** command simultaneously with the **write terminal** or **show running-config** command.

  Conditions: This symptom is observed when the **service compress-config** command or **boot config** command is enabled.

  Workaround: Do not enter the above-mentioned commands simultaneously, reduce the size of the configuration, or increase the size of the NVRAM.

  Further Problem Description: This problem was introduced in Cisco IOS Release 12.1(8a)E1, so most Cisco IOS 12.1 E releases are exposed to this problem. The problem may also occur in Release 12.2 S.

- CSCed52578

  Symptoms: The MPLS packets are forwarded with a bogus label when they are sent out on a loadshared non-VRF MPLS enabled “Internet” interface from a VRF.

  Condition: A static route for the VRF should be configured to reach the Internet, which would in turn be configured to recurse over 2 static routes to reach the next hop for the global Internet.

Workaround: Shut down one of the interfaces to remove the load-sharing condition.

- CSCed88854

  Symptoms: A VIP with an ATM port adapter crashes with a bus error.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(18)S3 when the ATM interface changes to the down state.

  Workaround: Configure the **random-detect** command in a policy map and attach the service policy to the ATM PVC.

- CSCee15798

  Symptoms: After an SSO switchover or when a line card reloads, routes may be deleted from the CEF forwarding tables on the line cards.

  Conditions: This symptom is observed when a large number of recursive routes is configured and when an SSO switchover occurs. NDB updates from the routing protocols may not be downloaded to the line cards if they are received while a line card is downloading.

  Workaround: Clear the line cards and reload the full CEF forwarding database by entering the **clear cef linecard** command after the routing protocols have converged.

- CSCee18883

  Symptoms: All VIPs in a Cisco 7500 series restart as a consequence of a Cbus complex that is triggered by a stuck output. Just before the output becomes stuck, IPC timeout errors occur.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(5) in a dLFIoATM environment. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCee23517

  Symptoms: The CEF tables on line cards or standby RPs may miss prefixes that are present in the CEF table on the active RP.

  Condition: This symptom is observed on a Cisco platform that is a distributed system (for example, on a Cisco 7500 series).

  Workaround: Enter the **clear cef linecard** command.

- CSCee26700

  Symptoms: A router may experience a memory leak when the LSR MIB is queried.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.2(15)T10 but is software-independent.

  Workaround: Disable the LSR MIB queries and reboot the device to reclaim the leaked memory.

- CSCee50294

  Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml.

There are multiple workarounds for this issue:

There are four possible workarounds for this vulnerability:

- Disabling the dhcp service
- Control Plane Policing
- Two versions of Access Control Lists

a. Disabling the DHCP Service

This vulnerability can be mitigated by utilizing the command:

no service dhcp

However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

b. Control Plane Policing Feature

The Control Plane Policy feature may be used to mitigate this vulnerability, as in the following example:

```
access-list 140 deny   udp host 192.168.13.1 any eq bootps
access-list 140 deny   udp any host 192.168.13.1 eq bootps
access-list 140 deny   udp any host 255.255.255.255 eq bootps
access-list 140 permit udp any any eq bootps
class-map match-all bootps-class
  match access-group 140
policy-map control-plane-policy
  class bootps-class
police 8000 1500 1500 conform-action drop exceed-action drop
control-plane
 service-policy input control-plane-policy
```

For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afad4.html.

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

c. Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address 192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
access-list 100 remark permit bootps from the DHCP server
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 remark deny bootps from any to router f1/0
access-list 100 deny   udp any host 10.89.236.147 eq bootps
access-list 100 remark deny bootps from any to router f0/0
access-list 100 deny   udp any host 192.168.13.2 eq bootps
```

```
access-list 100 remark deny bootps from any to router loopback1
access-list 100 deny   udp any host 192.168.61.1 eq bootps
access-list 100 remark permit all other traffic
access-list 100 permit ip any any
```

access-list 100 is applied to f0/0 and f1/0 physical interfaces.

```
interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

An alternate configuration for the interface access-list workaround.

This example would also need to be applied to all physical interfaces, but deny statements for all of the IP addresses configured on the router are not necessary in this approach. In this example, the address 192.168.13.1 represents a legitimate DHCP server.

```
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 permit udp any host 192.168.13.1 eq bootps
access-list 100 permit udp any host 255.255.255.255 eq bootps
access-list 100 deny   udp any any eq bootps

interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

- CSCuk41411

  Symptoms: After you enter the **clear cef linecard** command, RRP information may not be displayed correctly in the output of the **show cef linecard** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or Release 12.2S, that has two Route Processors, and that is configured for RPR+.

  Workaround: Do not enter the **clear cef linecard** command when the router is configured for RPR+.

  Alternate Workaround: Reload the router after you enter the **clear cef linecard** command.

- CSCuk46249

  Symptoms: The **debug ipv6 cef** command is not accepted.

  Conditions: This symptom is observed in Cisco IOS Release 12.2 S and is platform-independent.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Resolved Caveats—Cisco IOS Release 12.2(18)S5

Cisco IOS Release 12.2(18)S5 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S5 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCed59930

  Symptom: A software-forced crash may occur on an NPE-G1 after you have reloaded the NPE-G1, and the NPE-G1 may enter the boot mode.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(18)S3 when traffic is entering the router while the NPE-G1 is being reloaded and when there is a high CPU utilization on the NPE-G1.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCec16481

  A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

  The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

  Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

  http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml.

Miscellaneous

- CSCec22929

  Symptoms: A software-forced reload may occur on a Cisco 7200 series after an OIR of a PA-2T3+ port adaptor.

  Conditions: This symptom is observed when traffic enters through the interface of the port adapter.

  Workaround: Shut down the interface of the port adapter before you perform an OIR.

- CSCed11793

  Symptoms: The output queue of a Gigabit Ethernet port may become stuck, preventing traffic from leaving the interface.

  Conditions: This symptom is observed on the Gigabit Ethernet port 0/1 (gig0/1) of a Network Processing Engine NPE-G1 (NPE-G1) that is installed in a Cisco 7200 series.

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

  Alternate Workaround: Reload the router.

- CSCed29514

  Symptoms: A Cisco 7200 series NPE-G1 built-in GE (SBeth) MAC filter may accept NULL DAs (00-00-00-00-00-00). This unintentional behavior may pose a denial of service security risk in customer environments when their networks are flooded with NULL DAs.

  Conditions: This symptom is observed when NULL DAs are presented to an NPE-G1 GE interface. This situation may be either a third-party vendor product flaw or a third-party vendor documentation error. (The third-party vendor documentation states that NULL DAs may be used for unused MAC Filter entries, implying that they are not accepted.)

  Workaround: There is no workaround.

- CSCed40933

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory, which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml.

- CSCed47560

  Symptoms: The native Gigabit Ethernet ports of a Cisco 7200 series NPE-G1 or a Cisco 7301 may stop forwarding traffic.

  Conditions: This symptom is observed in a stress situation when bursty traffic is received.

  Workaround: There is no workaround.

- CSCed91798

  Symptoms: A Cisco IOS DHCP relay or server may stop functioning.

  Conditions: This symptom is observed when the **ip cef** command is enabled.

  Workaround: Disable the **ip cef** command.

- CSCee03112

  Symptoms: Downloading to an ATA flash disk may fail and the following error may appear:

  ```
  %Error writing disk2:/c7200-js-mz.122-14.S7.bin (TF I/O failed in data-out phase)
  ATA_Status time out waiting for card ready.
  ATA_Status time out waiting for card ready.
  ATA_Status time out waiting for card ready.
  ```

  The image size on the flash disk is 0 bytes.

  Conditions: This problem is seen on a Cisco 7200 series NPE-G1 that runs Cisco IOS Release 12.2(14)S5 or Release 12.2(14)S7.

  Workaround: Attempt a second time; the second attempt may be successful, but you will need to check the image size, even if there were no errors.

- CSCee08880

  Symptoms: EoMPLS configured on a 3-port Gigabit Ethernet line card may fail when CEF is disabled.

  Conditions: This symptom is observed on Cisco 12000 series that runs Cisco IOS Release 12.0(23)S6. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCee31450

  Symptoms: Ipv6 packets may not be switched via CEFv6 but may be blackholed.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S4 when the packets are switched from an FE interface to a POS interface.

  Workaround: There is no workaround.

- CSCin72573

  Symptoms: IP directed broadcast may not function.

  Conditions: This symptom is observed on a Cisco platform when CEF is enabled.

  Workaround: Disable CEF globally by entering the **no ip cef** global configuration command.

- CSCuk45567

  Symptoms: When you perform a physical online insertion and removal (OIR) of a Route Switch Processor (RSP), the router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series when Routing Information Protocol next generation (RIPng) for IPv6 is configured.

  Workaround: There is no workaround.

- CSCuk50070

  Symptoms: The packet length can be incorrect when switching IPv6 multicast packets.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(18)S or Release 12.2(20)S during normal IPv6 multicast forwarding.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(22)S and later releases.

Resolved Caveats—Cisco IOS Release 12.2(18)S4

Cisco IOS Release 12.2(18)S4 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S4 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCdy50225

  Symptoms: A Cisco 12000 series may reload when a line card has failed and you perform a Simple Network Management Protocol (SNMP) query to cpmCPUTotalTable from a network management station (NMS).

  Conditions: This symptom is observed under very rare situations on a Cisco 12000 series but may also occur on other Cisco platforms.

  Workaround: When a line card has failed, do not perform an SNMP query to cpmCPUTotalTable from an NMS.

- CSCea83367

  Symptoms: The running configuration may not be properly synchronized with the startup configuration after a switchover has occurred, causing the **snmp-server community public rw** global configuration command to be lost from the running configuration.

  Conditions: This symptom is observed on a Cisco router after a switchover has occurred.

  Workaround: After the switchover has occurred, manually reconfigure the **snmp-server community public rw** global configuration command.

Interfaces and Bridging

- CSCec35856

  Symptoms: The **media-type** interface configuration command cannot be configured on an FEIP interface on a Cisco router.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdv57965

  Symptoms: Although you may able to configure more than 4 Gbps of bandwidth for Resource Reservation Protocol (RSVP) or for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, the actual reserved bandwidth that is established for RSVP or the MPLS TE tunnel may be much less than 4 Gbps.

  The output of the **show running-config interface** *type number* privileged EXEC command shows the configured bandwidth. The output of the **show ip rsvp reservation** EXEC command shows the actual reserved bandwidth for RSVP.

  Conditions: This symptom is observed when the interface on which RSVP or the MPLS TE tunnel is configured does have sufficient bandwidth available to satisfy the configured bandwidth but the actual reserved bandwidth is less than the configured bandwidth.

  Workaround: There is no workaround.

- CSCeb68569

  Symptoms: Packets that are switched via process switching may cause high CPU utilization on a router.

  Conditions: This symptom is observed in an IP multicast environment when the packets are sent from a virtual host interface (VIF) and are destined for a multicast address. The packets should be switched via fast switching.

  Workaround: There is no workaround.

- CSCec40377

  Symptoms: A multicast router may stop sending Protocol Independent Multicast (PIM) join messages.

  Conditions: This symptom is observed on a Cisco router that is configured for multicast routing when buffer allocation failures occur and when the I/O memory is low.

  Workaround: Disable and reenable multicast routing.

Miscellaneous

- CSCdw65342

  Symptoms: CyBus error 10 and QA zero link errors may occur some time after a switchover.

  Conditions: This symptom is observed on a Cisco 7500 series when a VIP reads an invalid “bufhdr” pointer and attempt to write it to MEMD.

  Workaround: There is no workaround.

- CSCeb22276

  Symptoms: Some Simple Network Management Protocol (SNMP) packets may linger in the input queue while they are processed. However, the packets do exit the queue on their own without any intervention from the user. This fix allows these packets to be removed from the queue more quickly.

  Conditions: This symptom is observed on a device that runs Cisco IOS software and that supports SNMP operations. In addition, the SNMP request must contain a valid community string.

  Workaround: Protect the SNMP community strings with good password management. Permit SNMP traffic only from trusted devices.

- CSCec37042

  Symptom: A Cisco 7301 or Cisco 7401ASR may boot up in the boot image rather than in the Cisco IOS image.

  Conditions: This symptom is observed in the following configurations:

  – On a Cisco 7301 that is configured with a Network Processing Engine G1 (NPE-G1) and that runs a c7301-boot-mz image.

  – On a Cisco 7401ASR that is configured with a Cisco Network Service Engine (NSE) and that runs a c7400-kboot-mz image.

  The symptom is observed in Cisco IOS Release 12.2(16)B2 but may also occur in Release 12.2 S, 12.3, 12.3 B, or 12.3 T.

  Workaround: Enable the router to boot the image from a disk by entering the **boot system** global configuration command.

- CSCed20042

  Symptoms: A Cisco router may unexpectedly reload if IPv6 encounters a routing loop, and IPv6 CEF is enabled.

  Conditions: This symptom occurs under the following conditions:

  – IPv6 must be enabled

  – IPv6 CEF must be enabled

  – The IPv6 RIB must have recursive entries that form a loop, for example:

```
Router# show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
B   ::/0 [200/0]
     via 2::2
C   1::/64 [0/0]
     via ::, Ethernet0/0
L   1::2/128 [0/0]
     via ::, Ethernet0/0
C   2::/64 [0/0]
     via ::, Ethernet1/0
L   2::1/128 [0/0]
     via ::, Ethernet1/0
B   2001::/16 [200/0]
     via 2002::1
B   2002::/16 [200/0]
     via 2001::1
L   FE80::/10 [0/0]
     via ::, Null0
```

```
L   FF00::/8 [0/0]
     via ::, Null0
```

Note that 2001::/16 and 2002::/16 results in a recursion loop because 2001::/16 is accessible via 2002::/16 and 2002::/16 is accessible via 2001::/16.

Workaround: Disable IPv6 CEF using the global configuration command **no ipv6 cef**.

- CSCed51664

  Symptoms: Gigabit Ethernet interfaces on a Network Processing Engine G-1 (NPE-G1) may not accept packets with long MPLS headers. This situation may decrease the performance of some network environment such as an Ethernet over MPLS (EoMPLS) environment.

  Packets with a size that exceeds the maximum MTU in the output of the **show controller gigabitethernet 0/x** command may be dropped.

  Conditions: This symptom is observed on a Cisco 7200 series.

  Workaround: Increase the MTU at the interface level.

- CSCed68575

  Cisco Internetwork Operating System (IOS) Software releases trains 12.0 S, 12.1 E, 12.2, 12.2 S, 12.3, 12.3 B and 12.3 T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

- CSCed72297

  Symptoms: Multiple SYS-3-CPUHOG error messages may be generated in the LDP process, eventually followed by a watchdog timeout crash:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (422/8),process
  = LDP.
  -Traceback= 6101DFC0 6102546C 61016FE4 6101CE24 6101728C 61017A30
  ...
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = LDP.
  -Traceback= 6085658C 6101DE48 6102546C 61016FE4 6101CE24 6101728C 61017A30
  ```

  After the router has reloaded, the output of the **show version** command indicates “Last reset from watchdog reset.”

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S4 or Release 12.2(22)S and that is configured for MPLS LDP.

  Workaround: There is no workaround.

- CSCin35946

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

  Symptoms 1: When the Rivest, Shamir, and Adleman (RSA) public key of the peer of Cisco router that is running Cisco IOS Release 12.3 is manually configured on the router, the router may reload and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

Conditions 1: This symptom is observed when you enter the following sequence of commands:

- **crypto key pubkey-chain rsa** global configuration command
- **addressed-key** *key-address* public key chain configuration command
- **key-string** *key-string* public key configuration command

Workaround 1: Do not configure the RSA public key of a peer statically on the router; rather, use certificates. This workaround may not be acceptable in situations in which a certification authority (CA) server is not available or deployed.

Symptoms 2: When a Cisco router has saved the RSA public key of any peer in its configuration and is booted up with Release 12.3, the router may reload and generate the following error message:

```
%ALIGN-1-FATAL: Illegal access to a low address
```

Conditions 2: This symptom is observed when you have configured the RSA public key of the peer by using the following sequence of commands:

- **crypto keyring** *keyring-name* global configuration command
- **rsa-pubkey address** address keyring configuration command
- **key-string** *key-string* public key configuration command

Workaround 2: Do not configure the RSA public key of a peer statically on the router; rather, use certificates. This workaround may not be acceptable in situations in which a certification authority (CA) server is not available or deployed.

Resolved Caveats—Cisco IOS Release 12.2(18)S3

Cisco IOS Release 12.2(18)S3 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S3 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeb08094

  Symptoms: A router may reload unexpectedly, generate a crashinfo file, and then pause indefinitely.

  Conditions: This symptom is observed on a Cisco router that is configured with the **exception dump** global configuration command.

  Workaround: There is no workaround.

- CSCeb20967

  Symptoms: A Route Switch Processor (RSP) may reload unexpectedly when a bus error with an invalid memory address occurs while packets are placed into a hold queue.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.1(14)E4 or Release 12.2 S when the following sequence of events occurs:

  1. A packet is switched via Cisco Express Forwarding (CEF).
  2. The egress interface has queueing/shaping configured.
  3. The egress interface is congested, causing the packet to be placed into the hold queue.

  Workaround: There is no workaround.

- CSCec69536

  Symptoms: When you reload a Cisco 7500 series router with a new Cisco IOS software image, the router may reload unexpectedly during the bootup process and generate an “Imprecise cache parity error” message.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a Route Switch Processor 8 (RSP8) and that runs Cisco IOS Release 12.2(18)S when you reload the router with an image of Cisco IOS Release 12.3 T.

  Workaround: Do not reload the router. Rather, power-cycle the router to properly load the image of Cisco IOS Release 12.3 T.

Interfaces and Bridging

- CSCeb86989

  Symptoms: You may not be able to create an ATM permanent virtual circuit (PVC) with a virtual template.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an enhanced 1-port ATM OC-12/STM-4 port adapter (PA-A3-OC12).

  Workaround: There is no workaround.

- CSCec26643

  Symptoms: Packet-over-SONET (POS) interfaces on a 1-port POS OC-3c/STM-1 port adapter (PA-POS-OC3) that is installed in a Cisco 7200 series router that runs Cisco IOS Release 12.2(14)S3 may stop transmitting packets. The output packets counter stops incrementing.

  Conditions: This symptom is observed when you reload the router with a queueing configuration on the POS interfaces.

  Workaround: Remove the queueing configuration before you reload the router. Reapply the queueing configuration after the router has booted up.

IP Routing Protocols

- CSCdy26197

  Symptoms: A significant memory leak may occur on a Cisco router.

  Conditions: This symptom is observed when you configure and disable IP routing repetitively by using the **ip routing** global configuration command followed by the **no ip routing** global configuration command.

  Workaround: There is no workaround.

- CSCec43805

  Symptoms: The **distance bgp** *external-distance internal-distance local-distance* address family or router configuration command may be missing from a Border Gateway Protocol (BGP) IPv4 Virtual Private Network (VPN) configuration in the output of the **show running-config** privileged EXEC command when all of the following keywords in the **address-family ipv4 vrf** *vrf-name* router configuration command are configured with their default values:

```
- aggregate-address    Configure BGP aggregate entries
- auto-summary         Enable automatic network number summarization
- bgp                  BGP specific commands
- default              Set a command to its defaults
```

```
- default-information  Control distribution of default information
- default-metric       Set metric of redistributed routes
- distance             Define an administrative distance
- distribute-list      Filter networks in routing updates
- exit-address-family  Exit from Address Family configuration mode
- help                 Description of the interactive help system
- maximum-paths        Forward packets over multiple paths
- neighbor             Specify a neighbor router
- network              Specify a network to announce via BGP
- no                   Negate a command or set its defaults
- redistribute         Redistribute information from another routing protocol
- synchronization      Perform IGP synchronization
- table-map            Map external entry attributes into routing table
```

However, the **distance bgp** *external-distance internal-distance local-distance* address family or router configuration command functions fine because the BGP administrative distance for the VPN in which the command is configured does get changed.

Conditions: The symptom is observed after the BGP IPv4 VPN configuration is saved in NVRAM and the router is reloaded.

Workaround: Change any of the keywords for the **address-family ipv4 vrf** *vrf-name* router configuration command (see the Symptoms section above) to a nondefault value.

- CSCec48816

  Symptoms: A router may reload unexpectedly when you remove **network** commands.

  Conditions: This symptom is observed on a Cisco router that has the **router ospf** global configuration command enabled.

  Workaround: There is no workaround.

- CSCin52817

  Symptoms: A Cisco router may reload unexpectedly when you manually reload the router.

  Conditions: This symptom is observed when Open Shortest Path First (OSPF) LSAs are being "maxaged" while you manually reload the router. This situation may occur because of a fluctuating network and is an extreme corner case that cannot be reproduced on demand. The symptom is very unlikely to occur.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb54853

  Symptoms: IP Server Load Balancing (SLB) probes may fail although the output of the **show ip slb reals** privileged EXEC command indicates that the SLB probes are in the operational state.

  Conditions: This symptom is observed when a TCP probe is configured.

  Workaround: There is no workaround.

- CSCeb80481

  Symptoms: A memory leak may occur in the "SNMP Engine" process, which can be verified in the output of the **show processes memory | SNMP ENGINE** privileged EXEC command.

Conditions: This symptom is observed in Cisco IOS Release 12.0(26)S and Release 12.2(18)S when you enter the **snmpget** command for the MPLS-LSR-MIB MIB.

Workaround: There is no workaround.

- CSCec14039

  Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

  ```
  Last reset from watchdog reset
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1 and that is running Cisco IOS Release 12.2(14)S3. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCec32573

  Symptoms: The Class-Based Packet Marking feature may not count packets correctly.

  Conditions: This symptom is observed when you compare the number of packets that are counted by the Class-Based Packet Marking feature with the number of packets that are counted by the class-map match counter.

  Workaround: There is no workaround.

- CSCec80049

  Symptoms: When a tunnel interface goes down, a new Label Switched Path (LSP) is not signaled until the forwarding adjacency hold timer expires.

  Conditions: This symptom is observed on a Cisco router that is configured with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

  Workaround: There is no workaround.

- CSCec85172

  Symptoms: Control plane policy fails to match Address Resolution Protocol (ARP) packets with the **match protocol arp** class-map configuration command when the ingress interface has Inter-Switch Link (ISL) or Dot1q encapsulation.

  Conditions: This symptom occurs when a service policy is attached to the control plane in input direction.

  Workaround: There is no workaround.

- CSCed08172

  Symptoms: When you enter the **write memory** privileged EXEC command on a Cisco 7206VXR, a long delay may occur during the transfer of packets.

  Conditions: This symptom is observed on a Cisco 7206VXR that is configured with a Network Processing Engine G-1 (NPE-G1), that is running Cisco IOS Release 12.2(18)S or a later release, and that is functioning as a Multiprotocol Label Switching (MPLS) provider edge (PE) router.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(14)S3.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond

terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCin53040

  Symptoms: A secondary Route Switch Processor (RSP) that is configured with 512 MB of RAM may not recognize the 512 MB of RAM.

  Conditions: This symptom is observed on a Cisco 7500 series that has a primary and a secondary RSP and that runs a Cisco IOS image that has a size larger than 20 MB.

  Workaround: Configure the secondary RSP with 256 MB of RAM.

- CSCin57765

  Symptoms: A router may become unresponsive and may reload when you append a file whose size is not a multiple of 512 bytes to an Advanced Technology Attachment (ATA) Flash card (for example, boot disk, disk0, disk1).

  For example, this situation may occur when you enter the **show** *command* **| tee /append** *url* privileged EXEC command.

Conditions: This symptom is observed on a Cisco platform that runs a Cisco IOS image that contains the fix for caveat CSCdz27200 and that utilizes an ATA Flash card. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz27200. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: Write the output of the **show** command to a new file instead of appending it to an existing file by entering the **show** *command* **| tee** *url* privileged EXEC command.

- CSCuk47482

  Symptoms: A router may reload unexpectedly while you disable label distribution protocol (LDP) on an interface.

  Conditions: This symptom is observed on a router that has several interfaces that are configured for LDP when you disable LDP on all interfaces and when there is still one open TCP connection that is passively used by LDP while you disable LDP on the last interface.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCeb21552

  Symptoms: The following error message may be displayed when a router receives a connection request on command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports:

  ```
  %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.2.2
  ```

  Conditions: This symptom is observed on a Cisco router that has the remote shell (rsh) disabled.

  Workaround: Filter the traffic that is destined for command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports.

  First, enter the **show ip interface brief** EXEC command to display the usability status of interfaces that are configured for IP. The output may look like the following:

  ```
  Interface      IP-Address      OK? Method Status                Protocol
  Ethernet0/0    172.16.1.1      YES NVRAM  up                    up
  Ethernet1/0    unassigned      YES NVRAM  administratively down down
  Serial2/0      192.168.2.1     YES NVRAM  up                    up
  Serial3/0      192.168.3.1     YES NVRAM  up                    up
  Loopback0      10.1.1.1        YES NVRAM  up                    up
  ```

  Then, create the following access control list (ACL) for the router and apply this ACL to all interfaces that are enabled with the **ip access-group 177 in** router configuration command:

  ```
  access-list 177 deny tcp any host 172.16.1.1 eq 514
  access-list 177 deny tcp any host 172.16.1.1 eq 544
  access-list 177 deny tcp any host 192.168.2.1 eq 514
  access-list 177 deny tcp any host 192.168.2.1 eq 544
  access-list 177 deny tcp any host 192.168.3.1 eq 514
  access-list 177 deny tcp any host 192.168.3.1 eq 544
  access-list 177 deny tcp any host 10.1.1.1 eq 514
  access-list 177 deny tcp any host 10.1.1.1 eq 544
  access-list 177 permit ip any any
  ```

Resolved Caveats—Cisco IOS Release 12.2(18)S2

Cisco IOS Release 12.2(18)S2 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S2 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCec73305

  Symptoms: The ifOutUcastPkts object may be missing for serial interfaces when the ifTable table is walked in the Interfaces Group MIB (IF-MIB.my).

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S or Release 12.2(20)S.

  Workaround: Force the ifOutUcastPkts object to show up by entering the **no snmp-server sparse-table** configuration terminal command.

EXEC and Configuration Parser

- CSCin22321

  Symptoms: If the netConfigSet and hostConfigSet variables of the OLD-CISCO-SYS-MIB MIB are set, the corresponding commands may not be executed, and the following error messages and tracebacks may be generated:

  ```
  %SYS-4-SNMP_NETCONFIGSET: SNMP netConfigSet request. Loading configuration from
  10.10.10.10
  ```

  ```
  %SYS-3-TIMERNEG: Cannot start timer (0x545E1928) with negative offset (-1). -Process=
  "SNMP ENGINE", ipl= 6, pid= 143 -Traceback= 502308BC 5022E3F8 50233358 501B0A24
  501B298C 501C3618 501C3800 50259C00 50255290 5024F444 502574BC 502576FC 5017C4F4
  508EBE04 508EBBBC 508D4D8C
  ```

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file.
  ```

  Conditions: This symptom is platform independent.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeb77038

  Symptoms: A Cisco router may pause indefinitely because of a bus error, and the following error message may appear:

  ```
  System returned to ROM by bus error at PC 0x60B5F1C0, address 0xEF4321E5
  ```

  Conditions: This symptom is observed on a Multiprotocol Label Switching (MPLS) provider edge (PE) router.

  Workaround: There is no workaround.

- CSCec43772

  Symptoms: When a large number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets is received, the input-queue counters of an interface may slowly increase, eventually causing the interface to become wedged.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(14)SZ3 or Release 12.2(18)S.

Workaround: Reload the router.

- CSCin53052

  Symptoms: The IP address of an interface on which Virtual Private Network (VPN) routing/forwarding (VRF) instances are configured may become lost.

  Conditions: This symptom is observed on a Cisco 7200 series after the IP routing process restarts.

  Workaround: Manually reconfigure the IP address on the interface.

ISO CLNS

- CSCin57685

  Symptoms: A Cisco 7200 series may reload unexpectedly while sending Connectionless Network Service (CLNS) packets.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(18)S1.

  Workaround: There is no workaround.

Miscellaneous

- CSCea60722

  Symptoms: A Cisco Express Forwarding (CEF) adjacency may not adjust when changes are made to the configuration.

  Conditions: This symptom is observed when you move the IP address from an ATM interface to another interface and when the next-hop router is still mapped in the ATM permanent virtual circuit (PVC). The CEF adjacency continues to point to the ATM interface.

  Workaround: Remove the ATM PVC, and reload the router.

- CSCec22912

  Symptoms: When you configure a channelized interface, the following error message and tracebacks may be displayed:

  ```
  %INTERFACE_API-3-NODESTROYSUBBLOCK: The SWIDB subblock named OUNIC was not removed
  -Traceback= 502722FC 50272604 502727DC 5027281C 506A0960 506A57D8 506AA920 506AB788
  506AB91C 506ABD54 5020EC20 5021D5BC 502D011C 502D0108
  ```

  Conditions: This symptom is observed when you first delete and then reconfigure a channelized interface.

  Workaround: There is no workaround.

- CSCec27821

  Symptoms: A Network Processing Engine G-1 (NPE-G1) may forward unicast IP packets that have a Layer 2 multicast MAC address.

  Conditions: This symptom is observed on an NPE-G1 that is installed in a Cisco 7200 series.

  Workaround: Create an access control list (ACL) to filter the packets.

  Alternate Workaround: Configure a static multicast MAC address mapping to the ports of the connected Layer 2 switch.

- CSCec37783

  Symptoms: Network Time Protocol (NTP) clients may not be able to synchronize to an NTP time server.

  Conditions: This symptom is observed when a Cisco router that functions as an NTP time server has the **ntp source** global configuration command enabled and when the router sends NTP packets via a source (src) port that is set to zero.

  Workaround: Disable the **ntp source** command.

Resolved Caveats—Cisco IOS Release 12.2(18)S1

Cisco IOS Release 12.2(18)S1 is a rebuild release for Cisco IOS Release 12.2(18)S. The caveats in this section are resolved in Cisco IOS Release 12.2(18)S1 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCdz89972

  Symptoms: The **media-type mii** interface configuration command cannot be configured on a Fast Ethernet interface on a Cisco router.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

ISO CLNS

- CSCeb72224

  Symptoms: A Cisco router that is running Intermediate System-to-Intermediate System (IS-IS) may not unset the IS-IS overload bit after a redundancy switchover, preventing the IS-IS connectivity from being restored.

  Conditions: This symptom is observed on a Cisco router that has two Route Processors (RPs) in a redundant configuration.

  Workaround: To restore the IS-IS connectivity, and to prevent the symptom from occurring again, enter the **no set-overload-bit on-startup** router configuration command on the primary RP.

Miscellaneous

- CSCdz04297

  Symptoms: A router may pause indefinitely instead of restarting.

  Conditions: This symptom is observed when the router is handling invalid addresses in the cached address space.

  Workaround: There is no workaround.

- CSCeb15038

  Symptoms: Even though you can enable traffic shaping on a physical interface of a Cisco router via the modular QoS CLI (MQC) or the regular command-line interface (CLI), traffic shaping does not take effect for traffic that leaves the physical interface via an egress traffic engineering (TE) tunnel.

Conditions: This symptom is observed in a Multiprotocol Label Switching (MPLS) environment.

Workaround: There is no workaround.

- CSCeb52270

  Symptoms: An interface of a Cisco router may not be able to receive traffic that is destined for an address that is configured on the router.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(14)S or Release 12.2(18)S and is platform independent. This symptom occurs only if there is a route in a different VPN routing and forwarding instance (VRF) that is attached or connected to the interface. This can happen if the route has been exported from one VRF to another or if a static route in a VRF points to the interface in question.

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

- CSCeb58931

  Symptoms: A Cisco 7304 router with a Network Services Engine 100 (NSE-100) that is running Cisco IOS Release 12.2 S reloads when NetFlow aggregation and export are configured.

  Conditions: This symptom is observed when NetFlow accounting is enabled in the Parallel eXpress Forwarding (PXF) processor on the NSE-100.

  Workaround: There is no workaround.

- CSCeb59165

  Symptoms: A standby card may not be able to switch to the active state.

  Conditions: This symptom is observed in a Redundancy Framework (RF) environment when ATM, High-Level Data Link Control (HDLC), or Frame Relay clients synchronize data during the "standby-bulk" state.

  Workaround: There is no workaround.

- CSCeb76341

  Symptoms: A label may not be assigned for a peer provider edge (PE) router.

  Conditions: This symptom is observed on a Cisco 7500 series and a Cisco 12000 series in a Virtual Private Network (VPN) configuration with multiple route reflectors (RRs) and label controlled ATM (LC-ATM) links between PE routers. The symptom may also occur on other platforms.

  Workaround: There is no workaround.

- CSCeb78695

  Symptoms: A Route Processor (RP), Switch Processor (SP), or Route Switch Processor (RSP) may reload when you enter the **show** *flash-filesystem***: all** or **show** *flash-filesystem***: chips** EXEC command.

  Conditions: This symptom is observed in Cisco IOS Release 12.2 S and is platform independent.

  Workaround: There is no workaround.

- CSCec08434

  Symptoms: The Cisco 7200 series boothelper image for Cisco IOS Release 12.2(14)S2 may reload unexpectedly, and the router may return to the ROM monitor (ROMmon) mode.

  Conditions: This symptom is observed when you install a 2-port Token Ring Inter-Switch Link 100BASE-TX port adapter (PA-2FEISL-TX) or a 1-port ATM Enhanced OC-3 Packet-over-SONET (POS) port adapter in a Cisco 7200 series Network Processing Engine G-1 (NPE-G1) and you reload, reset, or power up the router with the boothelper image.

Workaround: Remove the PA-2FEISL-TX or 1-port ATM Enhanced OC-3 POS port adapter when you reload, reset, or power up the router with the boothelper image. Once the router has booted up, you can reinstall the port adapters.

- CSCec29952

  Symptoms: A Cisco router will not form a Border Gateway Protocol neighbor under the **address-family ipv4** [**vrf** *vrf-name*] router configuration command if Message Digest 5 (MD5) authentication is configured.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(18)S.

  Workaround: There is no workaround.

- CSCec22970

  Symptoms: When the **negotiation auto** command is enabled, the Gigabit Ethernet port link is up and down between the Cisco 7301 router and the network processing engine-G1 (NPE-G1).

  Conditions: This symptom is observed on a Cisco 7301 router but is platform independent.

  Workaround: Enter the **no negotiation auto** command on the interface of each router.

- CSCin33783

  Symptoms: Entering the **shutdown** command followed by the **no shutdown** command on the Gigabit Ethernet interface prevents customer edge-to-customer edge (CE-to-CE) pings from going through.

  Conditions: This symptom is observed when Ethernet over Multiprotocol Label Switching (EoMPLS) is configured in VLAN mode on the Gigabit Ethernet interface of a Network Processing Engine G1 (NPE-G1) on a Cisco 7200 series router.

  Workaround: Configure EoMPLS in VLAN mode on a port adapter (for example, Gigabit Ethernet or Fast Ethernet).

Wide-Area Networking

- CSCin50541

  Symptoms: A router may reload after you enter the **ppp multilink** interface configuration command.

  Conditions: This symptom occurs when multilink is configured on an active serial interface and neither the **ppp multilink group** interface configuration command nor the **multilink virtual-template** global configuration command is entered. Under these conditions, multilink normally fails to create a bundle because of the lack of a configuration source for the bundle interface, but in this instance, it causes the router to reload.

  Workaround: Use the **shutdown** interface configuration command to shut down the serial interface until it is configured with the **ppp multilink group** interface configuration command.

Open Caveats—Cisco IOS Release 12.2(18)S

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(18)S. All the caveats listed in this section are open in Cisco IOS Release 12.2(18)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCeb57015

  Symptoms: The throughput for traffic across a provider edge (PE) router that is running IP version 6 (IPv6) in a Multiprotocol Label Switching (MPLS) environment (also referred to as a 6PE router) may be lower than expected. For example, the throughput may be about 4 Mbps.

  The output of the **debug ipv6 cef drop** privileged EXEC command shows that the packets are switched via Cisco Express Forwarding (CEF) from the interface that is enabled for IPv6 to the MPLS network, but does not show any packets that are forwarded from the MPLS network to the interface that is enabled for IPv6, which indicates that the packets from the MPLS network are process-switched rather than switched via CEF.

  Conditions: This symptom is observed on a Cisco 7500 series that functions as a 6PE router and that is configured with 2-port Fast Ethernet port adapters.

  Workaround: There is no workaround.

- CSCeb70645

  Symptoms: Some packets may be ignored on a Gigabit Ethernet interface, and input errors may be generated, which can be seen in the output of the **show interfaces gigabitethernet** and the **show controllers gigabitethernet** privileged EXEC commands.

  Conditions: This symptom is observed on a Cisco 7200 series when the CPU load is increased.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCeb86989

  Symptoms: You may not be able to create an ATM permanent virtual circuit (PVC) with a virtual template.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an enhanced 1-port ATM OC-12/STM-4 port adapter (PA-A3-OC12).

  Workaround: There is no workaround.

IP Routing Protocols

- CSCea79433

  Symptoms: A Resource Reservation Protocol (RSVP) reservation may be torn down when a routing change occurs.

  Conditions: This symptom is observed on a Cisco router that is configured for Voice over IP (VoIP).

  Workaround: There is no workaround.

- CSCeb10154

  Symptoms: For each data packet that is handled on a Cisco router, spurious memory accesses may occur at addresses 0x1D and 0x22. When the traffic rate is high, the console may become unresponsive, and the router may pause until the call is cleared. The output of the **show alignment** EXEC command displays the following information:

```
Total Spurious Accesses 3984, Recorded 8
 Address  Count  Traceback
      1D    775  0x610CFA2C 0x60420754 0x60432D98
      24    775  0x610CFA38 0x60420754 0x60432D98
       3    775  0x610CFCF4 0x60420754 0x60432D98
       3    775  0x610B5D5C 0x610CFD20 0x60420754 0x60432D98
      22    221  0x610CFA2C 0x60429D48 0x60432D98
      24    221  0x610CFA38 0x60429D48 0x60432D98
       8    221  0x610CFCF4 0x60429D48 0x60432D98
       8    221  0x610B5D5C 0x610CFD20 0x60429D48 0x60432D98
```

  Conditions: This symptom is observed on a Cisco router that has a single physical interface that is configured for Resource Reservation Protocol (RSVP) over ATM switched virtual circuits (SVCs) on one subinterface and RSVP over ATM permanent virtual connections (PVCs) on another subinterface. The symptom is related to a timing difficulty because the symptom occurs only when the PVC is set up after the SVC.

  Workaround: There is no workaround.

- CSCeb28161

  Symptoms: Static routes may not be propagated from one provider edge (PE) router to other PE routers.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2 S or Release 12.3 and that functions as a PE router when static routes are configured and redistributed in a Border Gateway Protocol (BGP) Virtual Private Network version 4 (VPNv4) configuration.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb12931

  Symptoms: I/O memory allocation failure (MALLOCFAIL) may occur when you send a high traffic load through a permanent virtual circuit (PVC) that is configured on an 8-port ATM Inverse MUX E1 port adapter (PA-A3-8E1IMA) or on an 8-port ATM Inverse MUX T1 port adapter (PA-A3-8T1IMA).

  Conditions: This symptom is observed when the traffic rate is close to the line rate and when the maximum number (4096) of permanent virtual circuits (PVCs) is configured.

  Workaround: To recover part of the lost memory, reduce or stop the traffic flow and enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the port adapter. To recover all the lost memory, reload the router.

- CSCeb47930

  Symptoms: A Versatile Interface Processor (VIP) may reload because of memory corruption and may generate the following tracebacks:

  ```
  abort
  crashdump
  validblock
  validate_memory
  checkheaps
  checkheaps_process
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(18)S.

  Workaround: There is no workaround.

- CSCeb49716

  Symptoms: A Cisco 7200 series router that is configured with a Network Processing Engine G1 (NPE-G1) may not boot Cisco IOS software properly and may generate the following error message continuously:

  ```
  *** System Error Interrupt (IBIT6) ***
  int_stat register = 0xf400038
  BCM-1250 Error Interrupt, Cause(s):
  mask=0xf47effc3ffc0ecc3, cause=0x0300002000000000, real_cause=0x0300002000000000
  M_INT_GPIO_5 - Sturgeon 1 (MB2)
  OIR event on swappable port adaptor(s)
    PC = 0xbfc0ec98, SP = 0x80005540, RA = 0xbfc04634
    Cause Reg = 0x00004c00, Status Reg = 0x3040d003
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(14)S2.

  Workaround: Power-cycle the router.

- CSCeb52270

  Symptoms: An interface of a Cisco 7200 series may not be able to receive traffic that is destined for an address that is configured on the router.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(14)S1.

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

- CSCeb54527

  Symptoms: A Multiprotocol Label Switching (MPLS) Layer 2 virtual circuit (VC) may not come back up when the VC ID number is changed to a mismatching ID number and then changed back to the original ID number. A tunnel that is configured on the VC goes down when you change the VC ID number to the mismatching ID number.

  Conditions: This symptom is observed in a PPP over MPLS (PPPoMPLS) environment.

  Workaround: If the tunnel is using a loopback interface as the router ID, bring the tunnel back up by toggling the loopback interface.

- CSCeb54853

  Symptoms: IP Server Load Balancing (SLB) probes may fail although the output of the **show ip slb reals** privileged EXEC command indicates that the SLB probes are in the operational state.

  Conditions: This symptom is observed when a TCP probe is configured.

  Workaround: There is no workaround.

- CSCeb54901

  Symptoms: The Channel Interface Processor (CIP) microcode may fail to load, and error messages similar to the following may appear:

  ```
  %UCODE-3-BADCHKSUM: Bad checksum in slot0:cip218-120.hsma_test_kernel_hw5, found
  0xC620 expected 0x0
  %UCODE-3-RDFAIL: Unable to read ucode file slot0:cip218-120.hsma_test_kernel_hw5 from
  flash
  ```

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: There is no workaround.

- CSCeb72681

  Symptoms: When a burst of data at a high packet rate is presented for policing on a class, much more than the correct burst size may be allowed to go through before packets drops occur.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Service Engine 100 (NSE-100) in the following configuration:

  - The police rate is 500 Mbps.
  - The burst size is the default size of 0.25 seconds of data.
  - The overload is 10 percent.

  In this configuration, all data should be allowed through for 2.5 seconds. However, all data goes through for more than 3 seconds.

  Workaround: There is no workaround.

- CSCeb76341

  Symptoms: A label may not be assigned for a peer provider edge (PE) router.

  Conditions: This symptom is observed on a Cisco 7500 series and a Cisco 12000 series in a Virtual Private Network (VPN) configuration with multiple route reflectors (RRs) and label controlled ATM (LC-ATM) links between PE routers. The symptom may also occur on other platforms.

  Workaround: There is no workaround.

- CSCeb77675

  Symptoms: Border Gateway Protocol (BGP) may not allocate or advertise labels for the IP version 4 (IPv4) prefixes that are configured with the **network** *network-number* address family configuration or router configuration command. This situation may be caused by a race condition that prevents BGP from learning the labels from the Label Information Base (LIB).

  Conditions: This symptom is observed in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) configuration.

  Workaround: To enable BGP to learn the labels form the LIB, enter the **clear ip route** *network* EXEC command.

- CSCeb78898

  Symptoms: The default 0/0 Virtual Private Network (VPN) routing/forwarding (VRF) route for a Versatile Interface Processor (VIP) may not be present in the Cisco Express Forwarding (CEF) table, even though the Route Switch Processor (RSP) does contain the information about the default 0/0 VRF route.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP4.

  Workaround: Disable and then reenable CEF.

- CSCeb82042

  Symptoms: Many spurious accesses may occur on a Versatile Interface Processor (VIP) and a Route Switch Processor (RSP).

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP8 and that is configured for Multiprotocol Label Switching (MPLS).

  Workaround: There is no workaround.

- CSCeb82588

  Symptoms: Ethernet over Multiprotocol Label Switching (EoMPLS) traffic may fail on imposition.

  Conditions: This symptom is observed when you remove the EoMPLS configuration of a subinterface, causing the symptom to occur on all other subinterfaces that are configured on the main interface.

  Workaround: Instead of removing the EoMPLS configuration, shut down the subinterface.

- CSCeb82658

  Symptoms: The Parallel Express Forwarding (PXF) processor of a Network Service Engine 100 (NSE-100) may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7304 when a Reverse Path Forwarding (RPF) configuration is applied to an interface.

  Workaround: First shut down the interface, and then apply the RPF configuration.

- CSCeb82710

  Symptoms: When distributed Cisco Express Forwarding (dCEF) is configured on a generic routing encapsulation (GRE) provider edge (PE) router, IP packets may be ignored and dropped from an interface of a Versatile Interface Processor (VIP).

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(18)S.

  Workaround: Do not use dCEF; rather, use Cisco Express Forwarding (CEF).

- CSCin12121

  Symptoms: A Cisco 7200 series router that is configured with a Network Services Engine 1 (NSE-1) or a Cisco 7400 series router stops forwarding traffic.

  Conditions: This symptom is observed on an interface that has fair queueing or class-based weighted fair queueing (CBWFQ) enabled.

  Workaround: On the Cisco 7200 series router that is configured with an NSE-1, enter the **no ip pxf** command. On the Cisco 7400 series router, enter the **no fair-queue** command.

- CSCin51588

  Symptoms: When you reload the microcode onto an enhanced 8-port multichannel T1/E1 port adapter (PA-MC-8TE1+) while traffic is flowing through the port adapter, the following error message may appear:

  ```
  %RSP-3-RESTART: interface Serial0/0/4:0, not transmitting
  ```

  In most cases, the interfaces of the port adapter recover on their own. In very rare cases, the execution of a Cbus Complex occurs.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: If the interfaces of the port adapter do not recover on their own, execute a Cbus Complex.

- CSCuk45205

  Symptoms: When you deconfigure IP version 6 (IPv6) or IPv6 unicast Reverse Path Forwarding (uRPF) on a Cisco router that runs IPv6 Cisco Express Forwarding (dCEF), the configuration may not be removed from a Versatile Interface Processor (VIP) or line card, although it will be removed from the Route Switch Processor (RPS) or Route Processor (RP). This situation may cause IPv6 or IPv6 uRPF to continue to be applied to packets that are switched via dCEF.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 12000 series only when distributed Cisco Express Forwarding (dCEF) is enabled.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCeb65527

  Symptoms: Spurious memory accesses may occur on a Cisco 7301.

  Conditions: This symptom is observed on a Cisco 7301 that functions as a Layer 2 Tunneling Protocol (L2TP) network server (LNS).

  Workaround: There is no workaround.

- CSCin48239

  Symptoms: When you remove all channel groups from a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) that is installed in a Versatile Interface Processor (VIP), the VIP may reload and generate "%CCB-3-CCBCMDFAIL1" error messages.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2 S or Release 12.3(1) when 256 channel groups with AU-4 mapping are configured on the PA-MC-STM-1 and traffic is sent bidirectionally at a rate of 60 kpps with packet sizes of 100 bytes.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(18)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(18)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdz70112

  Symptoms: A Route Switch Processor (RPS) may pause indefinitely when you unconfigure the maximum transmission unit (MTU) size on an interface.

  Conditions: This symptom is observed on a Cisco 7500 series router in a PPP over Multiprotocol Label Switching (PPPoMPLS) environment.

  Workaround: There is no workaround.

- CSCdz72611

  Symptoms: A router may reload and generate the following error message:

  ```
  %%Error: Unrecognized midplane in chassis.
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch or a Cisco 7200 series, Cisco 7500 series, or Cisco 7600 series router that is running Cisco IOS Release 12.2 S.

  Workaround: There is no workaround.

- CSCdz74858

  Symptoms: A Route Switch Processor 16 (RSP16) may pause indefinitely or reload soon after it has booted up, and the boot Flash memory may become corrupt.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2 S.

  Workaround: There is no workaround.

- CSCdz75810

  Symptoms: Parser difficulties may occur when traps are added to the **snmp-server host** *host-address* global configuration command.

  Conditions: This symptom is observed when an incorrect Simple Network Management Protocol (SNMP) trap receiver is added by entering the **snmp-server host** *host-address* global configuration command and occurs because all traps are appended by default to this command in the running configuration.

  Workaround: There is no workaround. The fix for this caveat ensures that traps are no longer appended by default to the **snmp-server host** *host-address* global configuration command on the running configuration.

- CSCea90276

  Symptoms: You may not be able to load the Channel Interface Processor (CIP) microcode from any type of Flash device. When you attempt to do so, error messages similar to the following may appear:

  ```
  %CIP2-0-MSG: slot4 %LOADER-0-HEADER: Loading file
  slot0:cip218-120.CSCea27903_seg_eca:
  %CIP2-3-MSG: slot4 %LOADER-3-FOPENER: Error: file
  (slot0:cip218-120.CSCea27903_seg_eca) open failure code -2
  %CIP2-3-MSG: slot4 %LOADER-3-FOPEN: Error: Cannot open the input file
  "slot0:cip218-120.CSCea27903_seg_eca".
  ```

```
%CIP2-3-MSG: slot4 %LOADER-3-LOADRC: Error: Return code is 8(8)
%CIP2-0-MSG: slot1 %LOADER-0-HEADER: Loading file
slot0:cip218-120.CSCea27903_seg_pca:
%CIP2-3-MSG: slot1 %LOADER-3-FOPENER: Error: file
(slot0:cip218-120.CSCea27903_seg_pca) open failure code -2
%CIP2-3-MSG: slot1 %LOADER-3-FOPEN: Error: Cannot open the input file
"slot0:cip218-120.CSCea27903_seg_pca".
%CIP2-3-MSG: slot1 %LOADER-3-LOADRC: Error: Return code is 8(8)
%CIP2-0-MSG: slot1 %LOADER-0-HEADER: Loading file
slot0:cip218-120.CSCea27903_seg_eca:
%CIP2-3-MSG: slot1 %LOADER-3-FOPENER: Error: file
(slot0:cip218-120.CSCea27903_seg_eca) open failure code -2
%CIP2-3-MSG: slot1 %LOADER-3-FOPEN: Error: Cannot open the input file
"slot0:cip218-120.CSCea27903_seg_eca".
%CIP2-3-MSG: slot1 %LOADER-3-LOADRC: Error: Return code is 8(8)
%CIP2-0-MSG: slot4 %LOADER-0-HEADER: Loading file
slot0:cip218-120.CSCea27903_seg_eca:
%CIP2-3-MSG: slot4 %LOADER-3-FOPENER: Error: file
(slot0:cip218-120.CSCea27903_seg_eca) open failure code -2
%CIP2-3-MSG: slot4 %LOADER-3-FOPEN: Error: Cannot open the input file
"slot0:cip218-120.CSCea27903_seg_eca".
%CIP2-3-MSG: slot4 %LOADER-3-LOADRC: Error: Return code is 8(8)
```

The number of error messages and the names of the failed files depends on the configuration of the CIP.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: There is no workaround.

- CSCeb37423

  Symptoms: A Cisco 7500 series may reload because of a software condition when you enter the **no shutdown** interface configuration command on an interface.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for LAN Emulation (LANE).

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCdy65658

  Symptoms: A policy map with multiple class maps does not synchronize correctly with a standby route processor (RP).

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: Reload the standby RP.

- CSCdz89000

  Symptoms: A router may reload unexpectedly when the **show tech** EXEC command is entered.

  Conditions: This symptom is observed when the **show tech** EXEC command is entered on a Cisco 3660.

  Workaround: There is no workaround.

- CSCin37630

  Symptoms: A standby Route Switch Processor (RSP) may reload during bootup because of synchronization failures.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2 S when Route Processor Redundancy (RPR) or RPR Plus (RPR+) is configured.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCdz76961

  Symptoms: The 5-minute output rate in the output of the **show interfaces atm** or **show interfaces hssi** privileged EXEC command for ATM interfaces or High-Speed Serial Interfaces (HSSIs) respectively may be zero.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and other Cisco 7000 series routers.

  Workaround: There is no workaround.

- CSCdz90090

  Symptoms: A Fast Ethernet port may stop receiving unicast packets, causing pings and certain routing protocols to fail. The output of the **show interfaces** privileged EXEC command shows these unicast packets as “ignores.”

  Conditions: This symptom is observed a 2-port Fast Ethernet port adapter (PA- 2FE) that is installed in a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCea51200

  Symptoms: Subinterface counters may increment more slowly than expected when the **show interface atm** EXEC command is entered on a subinterface.

  Conditions: This symptom is observed when a user enters the **show interface atm** EXEC command on the subinterface of a Cisco router while traffic is going through the interface.

  Workaround: There is no workaround.

- CSCin40163

  Symptoms: An ATM interface may remain administratively down.

  Conditions: This symptom is observed when commands do not have any effect because the command-line interface (CLI) does not function. The symptoms are platform independent.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdu53656

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please see this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCdw50797

  Symptoms: A Cisco 12000 series may reload because of a bus error.

  Conditions: This symptom is observed after you enter the **show ip bgp regexp** *regexp* EXEC command.

  Workaround: There is no workaround.

- CSCdw84055

  Symptoms: Enhanced Interior Gateway Routing Protocol (EIGRP) may not form a neighbor relationship with message digest algorithm 5 (MD5) authentication.

  Conditions: The conditions under which this symptom occurs are not known at this time.

  Workaround: Disable MD5 authentication.

- CSCdy29423

  Symptoms: Border Gateway Protocol (BGP) may lose non-IP version 4 (non-IPv4) configurations after a Cisco router has reloaded.

  Conditions: This symptom is observed under either one of the following two conditions:

  – When you configure the **no bgp default ipv4-unicast** router configuration command, some peer group configurations may not be valid in the sequence that is saved by BGP. This situation prevents peer group members from being configured only under a non-IPv4 address family.

  – When all neighbors that are part of an IPv4 address family are disabled via the **no neighbor** *ip-address* **activate** router configuration command, this command is not saved in the configuration. After the router has reloaded, the neighbors are no longer disabled.

  Workaround for configurations that have the autonomous system configured in the peer group: Take the following three steps:

  1. Enter the **no bgp default ipv4-unicast** router configuration command.
  2. Do not configure any neighbor-specific session parameters in peer group members.
  3. Enable peer group members under the appropriate address family (such as IPv4 multicast or Virtual Private Network version 4 [VPNv4]) using the **neighbor** *ip-address* **peer-group** *peer-group-name* address family configuration command.

  Workaround for configurations that have the autonomous system configured in the neighbor: Take the following two steps:

  1. Enter the **no bgp default ipv4-unicast** router configuration command.
  2. Enable peer group members under the appropriate address family (such as IPv4 multicast or VPNv4) using the **neighbor** *ip-address* **peer-group** *peer-group-name* address family configuration command.

- CSCdy40742

  Symptoms: After a Border Gateway Protocol (BGP) neighbor resets, CPU utilization may run very high.

  Conditions: This symptom is observed when the “default-metric” router configuration command is enabled in the BGP router configuration.

  Workaround: There is no workaround.

- CSCdz36526

  Symptoms: A Cisco router may reload because of a bus error at the “ipnat_unlock_parent_entry” process.

  Conditions: This symptom is platform independent.

  Workaround: There is no workaround.

- CSCdz38203

  Symptoms: An Autonomous System Boundary Router (ASBR) in an inter-autonomous system (Inter-AS) Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) topology may advertise the wrong next hop (IP address of the external Border Gateway Protocol [eBGP] neighbor) to the eBGP neighbor ASBR for some VPN-IPv4 (VPNv4) prefixes.

  Conditions: This symptom is observed on a Cisco router that functions as an ASBR.

  Workaround: Manually change the IP next-hop configuration by entering the **set ip next-hop** router configuration command on either the Cisco router that functions as an ASBR or the neighbor ASBR that is using the route map.

- CSCdz53696

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

  1. Symptom 1: A Cisco router may reload during the Resource Reservation Protocol (RSVP) process.

     Condition 1: This symptom is observed when RSVP forwards a ResvError for a wildcard-filter (WF) style reservation.

     Workaround 1: There is no workaround.

  2. Symptom 2: A Cisco router may report a spurious access in the RSVP process.

     Condition 2: This symptom is observed when RSVP sends a ResvTear message for a traffic engineering (TE) tunnel.

     Workaround 2: There is no workaround.

  3. Symptom 3: A Cisco router may report a spurious access in the RSVP process.

     Condition 3: This symptom is observed when RSVP sends a ResvConfirm message from a router that is acting as an RSVP receiver endpoint that was configured with the **ip rsvp reservation-host** global configuration command.

     Possible Workaround 3: Enter the **ip rsvp reservation** global configuration command or the **ip rsvp listener** global configuration command instead of the **ip rsvp reservation-host** global configuration command.

- CSCdz59039

  Symptoms: When Reverse Path Forwarding (RPF) changes occur on a Route Processor (RP), only a "(*, G)" join is sent. The "(S, G)R" prunes that would cause a proxy join timer to be started at the upstream router for those "(S,G)" prunes are not sent. If the "(S, G)" prune is sent while the proxy join timer is running, the router removes the interface from the list but does not send a prune upstream because the proxy join timer is running.

  Conditions: This symptom is platform independent.

  Workaround: There is no workaround.

- CSCdz70283

  Symptoms: A router may reload when a Virtual Private Network (VPN) neighbor is deleted.

  Conditions: This symptom is observed on a Cisco router that has a VPN neighbor.

  Workaround: There is no workaround.

- CSCdz74130

  Symptoms: A bad magic number in the chunk header may lead to a memory corruption and may cause a router to reload.

  Conditions: This symptom is observed on a Cisco router that is configured for Resource Reservation Protocol (RSVP) after a specific invalid RSVP path message is received.

  Workaround: There is no workaround.

- CSCea06563

  Symptoms: It may take up to 5 minutes for a traffic engineering (TE) label switched path (LSP) tunnel to come up.

  Conditions: This symptom is observed when you change the encapsulation from High-Level Data Link Control (HDLC) to PPP or when you shut down an interface on which PPP encapsulation is configured.

  Workaround: To enable the TE LSP tunnel to come up immediately, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that functions as the TE LSP tunnel head.

- CSCea11704

  Symptoms: A Cisco router may reload when you enter the **clear ip bgp * soft out** privileged EXEC command.

  Conditions: This symptom is observed when a Network Address Translation (NAT) static network is configured to process multicast packets.

  Workaround: There is no workaround.

- CSCea13075

  Symptoms: The Multi Exit Discriminator (MED) that is received from a confederation external peer may be ignored in best path selection. The output of the **show ip bgp longer-prefixes** EXEC command does not indicate that any MED values were received.

  Conditions: This symptom is observed when Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) configurations are present.

  Workaround: There is no workaround.

- CSCea15407

  Symptoms: The changes implemented by CSCdy29423 changed and eliminated some commands to reflect their correct usage. This caveat (CSCea15407) describes the modifications that have been made to the command-line interface (CLI) of these commands to cause them to appear in the same manner before CSCdy29423 was implemented. The following are the affected commands:

  - **neighbor** *group-name* **activate** address family configuration command
  - **neighbor** *ip-address* **peer-group** *peer-group-name* address family configuration command

  Conditions: In Cisco IOS software releases that contain the fixes for CSCdy29423:

  - It is not necessary to manually activate the peer group, and the **neighbor** *group-name* **activate** address family configuration command will not show up in the configuration.
  - The **neighbor** *ip-address* **peer-group** *peer-group-name* address family configuration command under an address family is replaced by the **neighbor** *ip-address* **activate** router configuration command.

  In Cisco IOS software releases that contain the fixes for CSCea15407:

  - The CLI of the **neighbor** *group-name* **activate** address family configuration command will be available under the address family so that older versions Cisco IOS software will be able to read the configuration.
  - The CLI of the **neighbor** *ip-address* **peer-group** *peer-group-name* address family configuration command will be displayed under the address families for members of a peer group in a configuration.

  The changes implemented by CSCea15407 will allow the output of the **show running-config** EXEC command to be backward compatible with earlier versions of Cisco IOS software.

  Workaround: There is no workaround.

- CSCea19236

  Symptoms: A router may reload.

  Conditions: This symptom is observed when a Border Gateway Protocol (BGP) policy list is used on a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCea28131

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please see this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCea42500

  Symptoms: If the **default-information originate** router configuration command is entered on the Virtual Private Network (VPN) routing/forwarding (VRF) instance of a Cisco 12000 series that has the **address-family ipv4 vrf** command configured using the Border Gateway Protocol (BGP), the default route is learned correctly but the default route is entered incorrectly in the BGP routing table. This behavior may result in unexpected behavior on the other router if the other router does not have a correct default route.

The default static route of the VRF is not advertised by BGP after the default static route is configured under the VRF, and BGP may advertise the incorrect default route that is in the BGP routing table.

Conditions: This symptom is observed on a Cisco 12000 series that is running BGP.

Workaround: Perform either of the following steps:

- Enter a static default route under the VRF configuration.
- Configure an access control list (ACL).

- CSCeb57662

  Symptoms: Configured static multicast routes may be ignored in the Reverse Path Forwarding (RPF) calculation.

  Conditions: This symptom is observed in Cisco IOS Release 12.2 S and is platform independent.

  Workaround: There is no workaround.

- CSCea59359

  Symptoms: A Cisco 7500 series that is functioning as a provider edge (PE) router in a Multicast Virtual Private Network (MVPN) environment may stop sending Protocol Independent Multicast (PIM) register messages for the default multicast distribution tree (MDT) to its Rendezvous Point (RP). This situation prevents PE routers from establishing PIM adjacencies with other PE routers in the MVPN.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.0(24)S and that has the **ip pim register-rate-limit** global configuration command enabled. The symptom is not observed in Release 12.0(23)S or in earlier releases.

  Workaround: Enter the **clear ip mroute group-address** EXEC command for the default MDT group address.

  Alternate Workaround: Do not use the **ip pim register-rate-limit** global configuration command.

- CSCea63013

  Symptoms: When a Border Gateway Protocol (BGP) neighbor is deleted, the following error message may appear:

  ```
  % BGP: Peer is being deleted.
  ```

  Conditions: This symptom is observed when the BGP neighbor is configured for Network Layer Reachability Information (NLRI) mode and when it functions as both a unicast and a multicast neighbor.

  Workaround: There is no workaround. Delete the BGP neighbor later.

- CSCea79487

  Symptom: A Cisco router that is configured with IP multicast may reload because of a bus error.

  Conditions: This symptom is observed when a router sends (S,G) R join overrides to a neighbor, and the neighbor times out because of link flaps or because of another reason. The symptom is caused by a timing difficulty and is most likely to occur when the **ip pim spt-threshold infinity** global configuration command is configured on all routers in the network.

  A list of the affected releases can be found at the following location: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCds31596. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Possible Workaround: Remove the **ip pim spt-threshold infinity** global configuration command from all routers in the network to minimize the occurrence of the symptom.

- CSCeb04048

  Symptom: An Open Shortest Path First (OSPF) interface may be reported to be in the "down" state while the interface and the line protocol may be reported to be in the "up" state. This situation causes missing OSPF neighbor adjacencies on the OSPF interface that is in the "down" state.

  Condition: This symptom is observed when there are a large number of active interfaces and one of the following events has occurred:

  - You have upgraded a Cisco IOS image on a Route Processor (RP).
  - You have reloaded a RP.
  - You have reloaded microcode onto a line card.
  - You have reloaded microcode onto an RP.
  - You have reloaded microcode onto both a line card and an RP.

  Workaround: Use one of the following methods to recover the OSPF interface:

  - Enter the **clear ip ospf process** privileged EXEC command.
  - Enter the **clear ip route** *network* [*mask*] EXEC command, in which the *network* [*mask*] argument is the IP address of the OSPF interface that is in the "down" state.
  - Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the OSPF interface that is in the "down" state.

- CSCeb06813

  Symptoms: A Border Gateway Protocol (BGP) peer may not come up after you have disabled message digest 5 (MD5) authentication for BGP neighbors.

  Conditions: This symptom is observed when, on a router that is running BGP, you disable MD5 authentication for a BGP peer by using the **no neighbor** *ip-address* **password** router configuration command. The BGP session does not become established, even when you reset the BGP connection by entering the **clear ip bgp** *neighbor-address* privileged EXEC command or the **clear ip bgp *** privileged EXEC command.

  Workaround: After you have entered the **no neighbor** *ip-address* **password** router configuration command, reconfigure the BGP session for the neighbor at both sides of the connection.

  Alternate Workaround: Reload the router that is running BGP.

- CSCeb32598

  Symptoms: A Cisco router may reload when you enter the **show ip bgp regexp** EXEC command repeatedly. The router may also reload when you enter the **show ip bgp** EXEC command after you enter the **show ip bgp regexp** EXEC command.

  Conditions: This symptom is observed on a Cisco router that is configured with inbound policies that contain prefix lists, autonomous system path filter lists, and so on.

  Workaround: There is no workaround.

- CSCeb63120

  Symptoms: When refresh reduction is enabled and a Cisco router has been operational for a long time, valid Resource Reservation Protocol (RSVP) messages that are received from a neighbor may be dropped when the message IDs have cycled through the entire number space once (that is, from 0 to 4,294,967,295) and then progressed up to 2,147,483,648 (0x80000000).

  Conditions: This symptom is observed when a message ID number space begins at zero, increases up to 4,294,967,295 (32 bits), but then does not properly wrap back to zero, causing message IDs greater than 2,147,483,648 to be out of sequence, and to be dropped.

Note that a neighboring router is able to send Message IDs and properly wraps back from 4,294,967,295 to zero, but the receiving router that does not record the wrap event, causing the symptom to occur.

Workaround: There is no workaround.

- CSCeb65729

  Symptoms: Border Gateway Protocol (BGP) routes may not be recognized.

  Conditions: This symptom is observed when the **match ip next-hop** route-map configuration command is configured with an access control list (ACL) that matches a particular route.

  Workaround: There is no workaround.

- CSCeb68925

  Symptoms: Enabling IP version 6 (IPv6) multicast routing by entering the **ipv6 multicast-routing** global configuration command may cause memory corruption. This situation may eventually cause the router to reload.

  Conditions: This symptom is observed on a Cisco 7200 series but may also occur on other platforms.

  Workaround: There is no workaround.

ISO CLNS

- CSCdz69295

  Symptoms: A router may reload when a route that is learned via Intermediate System-to-Intermediate System (IS-IS) IP version 6 (IPv6) has more than eight equal-cost paths.

  Conditions: This symptom is observed when more than eight equal-cost links are configured between two IS-IS IPv6 routers. Depending on the network topology, the symptom may also occur when there are fewer than eight equal-cost links between an IS-IS IPv6 router and its neighbors.

  Workaround: Ensure that there are fewer than eight equal-cost links configured between two IS-IS IPv6 routers.

- CSCea24421

  Symptoms: Intermediate System-to-Intermediate System (IS-IS) loadbalancing may not function correctly.

  Conditions: This symptom is observed in a topology in which three routers—router A, router B, and router C—reside on a broadcast media. Router A is the root node that performs Shortest Path First (SPF) and has a direct path to both router B and router C. There is also an additional path between router A and router B. When you configure IS-IS to enable router A to reach router C along two equal-cost paths, router A may not use the direct path (that is, one of the two equal-cost paths) to router C but may only use the additional path via router B to reach router C.

  Workaround: There is no workaround.

Miscellaneous

- CSCdw69885

  Symptoms: A Cisco platform may reload when RFC 1577 is configured on an ATM interface.

  Conditions: This symptom is observed when the **atm arp-server** interface configuration command and the **debug atm smap-all** privileged EXEC command are enabled on the ATM interface and occurs only when a client attempts to establish a connection with the router while the Address Resolution Protocol (ARP) server is coming up.

  Workaround: Enter the **undebug atm smap-all** privileged EXEC command; then, reset the ATM interface.

- CSCdx22012

  Symptoms: A router may reload when the Border Gateway Protocol (BGP) update source is moved from the global default table to a Virtual Private Network (VPN) routing/forwarding (VRF) table.

  Conditions: This symptom is observed when a Multicast VPN (MVPN) tunnel uses the update source as the tunnel source.

  Workaround: There is no workaround.

- CSCdx31291

  Symptoms: When a provider edge (PE) router has multiple paths to an Autonomous System Boundary Router (ASBR) that is used as a next hop in a Virtual Private Network (VPN) routing/forwarding (VRF) static route with a global keyword, there is no Internet connectivity for the customers that are defined in the VRF.

  Conditions: This symptom is observed in a Multiprotocol Label Switching (MPLS) VPN.

  Workaround: Shut down one of the outgoing interfaces on the PE router.

- CSCdx60661

  Symptoms: In a Sniffer trace, the IP header checksum may be incorrect and may display an incorrect IP version of 10 instead of 4.

  Conditions: This symptom is observed when IP traffic is sent from a native (untagged) VLAN subinterface and when the IP header becomes corrupt because a matching policy rewrites the class of service (CoS) value to 5.

  Workaround: Do not apply a service policy with Layer 2 CoS marking on the native VLAN subinterface.

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCdx80484

  Symptom: A Cisco router may reload when you remove a Label Distribution Protocol (LDP) configuration before an Ethernet over Multiprotocol Label Switching (EoMPLS) configuration.

  Conditions: This symptom is observed in rare situations on a router that is configured for EoMPLS when you enter the **no mpls l2transport route** interface configuration command.

  Workaround: There is no workaround.

- CSCdx87500

  Symptoms: The **mstat** EXEC command and the **mtrace** EXEC command do not work as expected.

  Conditions: These symptoms are observed when the **mstat** EXEC command or the **mtrace** EXEC command is entered on an Multicast Distribution Tree (MDT) tunnel.

  Workaround: There is no workaround.

- CSCdy04665

  Symptoms: A memory allocation failure (MALLOCFAIL) may occur in a Turbo access control list (ACL) because of lack of memory.

  Conditions: This symptom is observed when the Turbo ACL table is being recompiled.

  Workaround: There is no workaround.

- CSCdy27264

  Symptoms: A Cisco 7400 series may reload because of a divide-by-zero error.

  Conditions: This symptom is observed if the **police** command is configured in the child policy of a Network Services Engine 1 (NSE-1) or a Cisco 7400 series that is running Cisco IOS Release 12.2 B.

  Workaround: There is no workaround.

- CSCdy47789

  Symptoms: Directly-connected neighbors may be displayed in the “Targeted Hellos” field in the output of the **show mpls ldp discovery** privileged EXEC, which is incorrect behavior. This situation does not impact routing functionality.

  Conditions: This symptom is observed in an Any Transport over Multiprotocol Label Switching (AToM) environment and is platform independent.

  Workaround: There is no workaround.

- CSCdy76871

  Symptoms: Multiprotocol Label Switching (MPLS) packets may be dropped.

  Conditions: This symptom is observed on a Cisco 7500 series and a Cisco 7600 series when one E1 link of a multilink bundle that consists of two E1 links fails on an 8-port multichannel E1 port adapter (PA-MC-8E1/120).

  Workaround: There is no workaround.

- CSCdy88118

  This caveat consists of three symptoms, three conditions, and three workarounds, all of which are related to the configuration of Multicast Distributed Switching (MDS) on subinterfaces:

  1. Symptom 1: When you configure MDS on a subinterface, the following incorrect error message may be generated:

     ```
     Multicast distributed switching is not allowed on sub-interfaces
     ```

     Condition 1: This symptom is observed when MDS is already configured on the main interface.

     Workaround 1: There is no workaround.

  2. Symptom 2: MDS may incorrectly be reported as being disabled on a subinterface while it is enabled and working fine.

     Condition 2: This symptom is observed in the output of the **show ip pim interface count** EXEC command. The command output is incorrect.

     Workaround 2: There is no workaround.

  3. Symptom 3: When you attempt to configure MDS on a subinterface, no error message is generated when it should be generated.

     Condition 3: This symptom is observed when the main interface is not configured for MDS and you attempt to configure MDS on a subinterface.

     Workaround 3: There is no workaround.

- CSCdy89749

  Symptoms: A Gigabit Ethernet Interface Processor plus (GEIP+) may report many alignment errors and the CPU utilization may stay at 100 percent.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCdz19517

  Symptoms: The Low Latency Queuing (LLQ) for IPSec Encryption Engines feature may not function. The output of the **show crypto engine qos** EXEC command may be incorrect and does not list all configured priority class entries.

  Conditions: This symptom is observed on all Cisco routers that are running Cisco IOS Release 12.2(13)T and that use the Low Latency Queuing (LLQ) for IPSec Encryption Engines feature. LLQ may not initialize correctly for some policy map configurations.

  Workaround: Define all priority class entries in the policy map before you define any nonpriority class entry.

- CSCdz43747

  Symptoms: A provider edge (PE) router may fail to bind a label for a route.

  Conditions: This symptom is observed after the route has flapped and recovered.

  Workaround: There is no workaround. To recover from the situation, enter the **no mpls ip** global configuration command followed by the **mpls ip** global configuration command.

- CSCdz56772

  Symptoms: A router that is configured for Cisco Express Forwarding version 6 (CEFv6) may reload when the supported state of an interface changes and when the associated prefix is deleted.

For example, a router may reload when a tunnel interface changes from a CEFv6 unsupported mode (for example, generic route encapsulation [GRE] IP version 6 [IPv6]) to a supported mode (for example, IPv6 IP) and you remove the associated IPv6 address by entering the **no ipv6 address** *ipv6-address* interface configuration command or by shutting down the tunnel interface.

Conditions: This symptom is observed on all platforms that are running Cisco IOS Release 12.2 S or Release 12.2(13)T.

Workaround: There is no workaround.

- CSCdz63050

  Symptoms: Outdrops may occur on a native Gigabit Ethernet interface of a Network Processing Engine G1 (NPE-G1), and the "bad length" counter in the output of the **show controllers gigabitethernet** privileged EXEC command may increase.

  This situation may prevent a customer premises equipment (CPE) from using FTP and HTTP communication when the CPE is connected to the Internet via a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) and a L2TP network server (LNS).

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1, that is functioning as an LNS, and that has Cisco Express Forwarding (CEF) enabled.

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

- CSCdz63708

  Symptoms: Any Transport over Multiprotocol Label Switching (AToM) configurations may disappear from a Cisco router.

  Conditions: This symptom is observed after you have reloaded the router.

  Workaround: There is no workaround.

- CSCdz65971

  Symptoms: The mplsVrflfUp MIB notification from the PPVPN-MPLS-VPN-MIB MIB is not sent on certain interfaces.

  Conditions: This symptom is observed on certain versions of T1, E1, or Packet over SONET (POS) interfaces.

  Workaround: The linkUp notification from the interfaces MIB can be used to notify a user when an interface transitions to the "operationally up" state.

- CSCdz66770

  Symptoms: Tag Distribution Protocol (TDP) may not convey the label change information for a prefix that is learned via an exterior Border Gateway Protocol plus (EBGP+) label to its TDP peers.

  Conditions: This symptom is observed on a Cisco 7500 series when TDP is used. The symptom does not occur when Label Distribution Protocol (LDP) is used.

  Workaround: There is no workaround.

- CSCdz67483

  Symptoms: You may not be able to configure the **encapsulation aal0** interface-ATM-VC configuration command for raw cell encapsulation on an ATM permanent virtual circuit (PVC).

  Conditions: This symptom is observed when the **pvc** *vpi*/*vci* **l2transport** interface-ATM-VC configuration command for ATM subinterfaces is configured on the PVC.

  Workaround: There is no workaround.

- CSCdz69161

  Symptoms: When you attempt to enter the **service single-slot-reload-enable** global configuration command, the following error message is generated:

  ```
  % Ambiguous command: "service single-slot-reload-enable"
  ```

  The command appears to be unavailable.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: There is no workaround.

- CSCdz75075

  Symptoms: An interautonomous system may fail when multiprotocol External Border Gateway Protocol (EBGP) multihop is configured between a Route Reflector (RR) for Virtual Private Network version 4 (VPNv4) and a router that is running the MPLS VPN—Inter-AS—IPv4 BGP Label Distribution feature.

  Conditions: This symptom is observed on an Autonomous System Boundary Router (ASBR) that is configured with a label controlled ATM (LC-ATM) interface, that is running the MPLS VPN—Inter-AS—IPv4 BGP Label Distribution feature, and that is connected to another ASBR in a cell-based Multiprotocol Label Switching (MPLS) network.

  Workaround: There is no workaround.

- CSCdz81658

  Symptoms: The interface receive ring of a native Gigabit Ethernet (GE) interface (gig0/1, gig0/2, or gig0/3) on a Network Processing Engine G1 (NPE- G1) may lock up.

  Conditions: This symptom is observed on a Cisco 7200 series router when the maximum transmission unit (MTU) is increased above the value of 2006 and the interface is subjected to stress traffic. (An MTU value of 2006 works fine, but a value of 2007 does not.)

  Workaround: There is no workaround.

- CSCdz85729

  Symptoms: A telco may exhibit alarms and frequency deviations of 2 to 3 ppm.

  Conditions: This symptom is observed if clock source internal is selected when a Cisco router is reloaded or booting up.

  Workaround: There is no deviation if the clock source is changed from the default source line to clock source internal and then back again to the clock source line.

- CSCdz87238

  Symptoms: Spurious detection of real server failures may occur when Cisco IOS Server Load Balancing (SLB) HTTP probes are active.

  Conditions: This symptom is observed in Cisco IOS Release 12.2 S when probes do not send the configured URL or headers in the request.

  Workaround: Ensure that the request “GET / HTTP/1.0” does return the status that is configured in the **expect** HTTP probe configuration command (which defaults to “200, OK”).

- CSCdz89449

  Symptoms: A loss of link adjacency that occurs on a provider edge (PE) interface may cause the improper cleanup of related data structures. When this behavior occurs, an error message that is similar to the following may be generated and the router may reload:

  ```
  %SYS-2-NOTQ: unqueue did not find 43D7B8E8 in queue 43B0C8CC - Process= "LDP", ipl=
  0, pid= 174
  ```

Conditions: This symptom is observed on a router that is running the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Carrier Supporting Carrier (CsC) feature.

Workaround: There is no workaround.

- CSCdz89852

  Symptoms: The Internet Security Association and Key Management Protocol (ISAKMP) key with a hardware encryption module is limited to 64 bytes when doing hardware-to-software encryption.

  Conditions: This symptom is observed with Cisco IOS Release 12.1(12c)E6.

  Workaround: Use 64 bytes or less for ISAKMP preshared keys if using hardware-to-software encryption.

- CSCea00377

  Symptoms: Cisco Express Forwarding for IP version 6 (CEFv6) may not be applied to incoming packets that are received on an FDDI interface. However, packets are forwarded normally in the process switching path.

  In addition, CEFv6 may not switch packets out of an FDDI interface. If this situation occurs, packets are sent to the process switching path at a limited rate. Then, the packets are forwarded normally.

  Conditions: This symptom is observed when CEFv6 is enabled globally. The symptom is not platform dependant.

  Workaround: To prevent the packets from being sent to the process switching path at a limited rate, disable CEFv6.

- CSCea00530

  Symptoms: A router may fail to handle the Label Withdraw if the Label Withdraw Message is received with a Forwarding Equivalence Class (FEC) type length value (TLV) and no Label TLV. The router may generate an error message that is similar to the following if a withdraw failure occurs:

  ```
  %LDP-3-UNKNOWN_MPLS_APP: ldp label withdraw message from 10.1.1.1:0; list type 7; afam
  1;
  ```

  Conditions: This symptom is observed on a Cisco router that is running Multiprotocol Label Switching (MPLS) and the Label Distribution Protocol (LDP).

  Workaround: There is no workaround.

- CSCea02291

  Symptoms: A Route Switch Processor (RSP) may reload.

  Conditions: This symptom is observed while traffic is sent on an RSP when Cisco Express Forwarding (CEF) commands such as the **ip cef** global configuration command or the **ip cef** distributed global configuration command are configured after the **mpls netflow egress** interface configuration command is configured.

  Workaround: Configure the CEF commands on the router before configuring the **mpls netflow egress** interface configuration command.

- CSCea09270

  Symptoms: A Cisco router that is functioning in a Multiprotocol Label Switching (MPLS) environment may reload.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2 S when a static recursive route to an IP version 4 (IPv4) internal Border Gateway Protocol (iBGP) peer exists.

  Workaround: Do not configure static recursive routes to the IPv4 iBGP peer.

- CSCea13771

  Symptoms: A Cisco uBR7100 series may reload and generate the following error message:

  ```
  %SYS-2-INTSCHED: 'suspend' at level 4
  ```

  Conditions: This symptom is observed on a Cisco uBR7100 series but may also occur on other platforms.

  Workaround: There is no workaround.

- CSCea15963

  Symptoms: In a setup that has two redundant provider edge (PE) routers that are connected to a Virtual Private Network (VPN), both of the PE routers may originate Multicast Distribution Tree (MDT) updates for the VPN source.

  In a worst case scenario, both PE routers may send a different mapping than the mapping that would cause the receivers to toggle between the different MDT data groups. In this situation, an immediate loss of data may be observed on the receivers.

  Conditions: This symptom is observed in a setup that has two redundant PE routers that are connected to a VPN source.

  Workaround: There is no workaround.

- CSCea19985

  Symptoms: A Cisco router that has a voice feature such as H.323 enabled may reload because of a bus error at address 0xD0D0D0B.

  Conditions: This symptom is observed on a Cisco 3700 series but may also occur on other routers.

  Workaround: There is no workaround.

- CSCea21665

  Symptoms: Entries in the tag forwarding table may disappear from a provider edge (PE) router.

  Conditions: This symptom is observed on a Cisco 7513 and a Cisco 7200 series that is functioning in a cell mode Multiprotocol Label Switching (MPLS) over ATM (MPLSoA) environment with the Multi-VC mode enabled. The label protocol is Label Distribution Protocol (LDP).

  Workaround: Enter the **clear ip route** *network* EXEC command on the affected PE router and enter the loopback address of the PE router as the *network* argument.

- CSCea22552

  GRE implementation of Cisco IOS is compliant with RFC2784 and RFC2890 and backward compatible with RFC1701.

  As an RFC compliancy this DDTS adds the check for bits 4-5 (0 being the most significant) of GRE header.

  This issue does not cause any problem for router operation.

- CSCea22981

  Symptoms: When you enter the **reserve** DSP interface configuration command, a Cisco 7200 series router may reload with the following error message:

  ```
  ALIGN-1-FATAL Corrupted program counter
  ```

  Conditions: This symptom is observed on a Cisco 7200 series router that is configured with a Network Processing Engine G1 (NPE-G1), a 2-port T1/E1 moderate capacity port adapter (PA-VXB-2TE1), and a 2 port T1/E1 high capacity port adapter (PA-VXC-2TE1).

  Workaround: Do not use the **reserve** DSP interface configuration command. It is not necessary to reserve digital signal processors (DSPs) as long as the DSP resources are not oversubscribed.

- CSCea24313

  Symptoms: A router may incorrectly move a default static route from an upstream router to another upstream router and then back again, and may continue to flap the route every 60 seconds.

  Conditions: This symptom is observed in the following configuration:

  A Cisco router (referred to as router A) is connected to two upstream routers (referred to as router B and router C) via a common interface. Router A is configured with two default recursive static routes, one via an address that is advertised by router B, the other one via an address that is advertised by router C.

  The administrative distances of the static routes are set in such a way that if both router B and router C are reachable, router A installs the default static route via router B. If router B becomes unreachable, router A installs the default static route via router C.

  Router B is advertising X::1. Router C is advertising X::2. Router A is configured in the following way:

  ```
  ipv6 route ::/0 X::1
  ipv6 route ::/0 X::2 2
  ```

  When router B stops advertising X::1, router A removes the default static route via router B and installs the default static via router C. This is correct behavior. However, 60 seconds after the transition, router A incorrectly reinstalls the default static route via router B and removes the default static route via router C. Another 60 seconds later, router A removes the static route via router B and reinstalls the static route via router C. This route flap occurs every 60 seconds.

  Possible Workaround: Do not rely on recursive static routes for the default route. For example, configure Interior Gateway Protocol (IGP) on routers B and C to advertise the default route. Appropriate configuration of metrics may ensure that the default route via router B is preferred to the one via router C, providing the same preference as the one that is obtained via static routes.

- CSCea25265

  Symptoms: A Parallel Express Forwarding (PXF) network processor may reload and generate the following error messages:

  ```
  %PXF-2-EXCEPTION: PXF exception on unit tmc.
  %PXF-2-RESTARTED: PXF tmc restarted.
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a Network Service Engine-1 (NSE-1) and on a Cisco 7400 series. The symptom occurs when the router receives a large number of streaming video feeds.

  Workaround: Disable PXF by entering the **no ip pxf** global configuration command.

- CSCea25622

  Symptoms: A Network Processing Engine G1 (NPE-G1) may reload unexpectedly and report the following message:

  ```
  System was restarted by reload
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

  Workaround: There is no workaround.

- CSCea25707

  Symptoms: A Cisco router may reload because of a software condition when running the LDP-MIB MIB. The router reloads because of a process watchdog timeout in the “SNMP ENGINE” process and logs an entry similar to the following one and logs a traceback:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SNMP ENGINE.
  %Software-forced reload
  ```

```
Unexpected exception, CPU signal 23, PC = 0x606F1FC4 ... Cause 00000024 (Code 0x9):
Breakpoint exception
```

Conditions: This symptom is observed after the router ID has been changed and when Label Distribution Protocol (LDP) sessions have been added or removed.

Workaround: Do not change the router ID. If the router ID has been changed, do not run the LDP-MIB MIB.

- CSCea25789

  Symptoms: A Cisco router may reload because of a bus error (Translational Lookaside Buffer [TLB] [load or instruction fetch] exception error), and an error message similar to the following is generated:

  ```
  Unexpected exception, CPU signal 10, PC = 0x60695434 -Traceback= ...
  Cause 80000008 (Code 0x2): TLB (load or instruction fetch) exception
  ```

  Conditions: This symptom is observed when Simple Network Management Protocol (SNMP) runs the LDP-MIB MIB.

  Workaround: Do not run the LDP-MIB MIB; rather, use one of the **show mpls ldp** commands to gather the required information.

- CSCea26842

  Symptoms: A Cisco 10720 may reload because of a software condition.

  Conditions: This symptom is observed when you deconfigure the **ipv6 access-list** global configuration command.

  Workaround: There is no workaround.

- CSCea27138

  Symptoms: Data Multicast Distribution Tree (MDT) mappings may be deleted too soon, causing a loss of data, or may not be deleted at all, causing unnecessary data to be transferred.

  Conditions: These symptoms are observed on a receiving provider edge (PE) router.

  Workaround: There is no workaround.

- CSCea29102

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

  1. Symptoms: A Route Processor (RP) may reload when you enter the **clear ip bgp *** privileged EXEC command while interfaces flap continuously.

     Conditions: This symptom is observed when Virtual Private Network (VPN) routing/forwarding (VRF) forwarding is configured on the interfaces that flap.

     Workaround: There is no workaround.

  2. Symptoms: An RP may reload when you simultaneously enter the **clear ip bgp *** privileged EXEC command and perform an online insertion and removal (OIR) by entering the **hw-reload reset** EXEC command.

     Conditions: This symptom is observed when you perform an OIR of an interface that has a VRF configuration in which the connected route is learned via a network statement. The connected route is removed when you perform the OIR.

     Workaround: Do not simultaneously enter the **clear ip bgp *** privileged EXEC command and perform an OIR.

- CSCea31844

  Symptoms: When you enter the **ip cef distributed** global configuration command and you create a tunnel interface, packets that are going through the tunnel interface are not switched via distributed switching, and the output of the **show running-config** EXEC command displays that the **no ip route-cache distributed** interface configuration command is enabled for the tunnel interface.

  Conditions: This symptom is observed on a Cisco 7500 series after you have reloaded the router, you have entered **ip cef distributed** global configuration command, you have created a tunnel interface using the **interface tunnel** *tunnel-number* command, and you have entered the **tunnel destination** *ip-address* interface configuration command.

  Workaround: Enter the **ip route-cache distributed** interface configuration command on the tunnel interface.

  Alternate Workaround: After you have reloaded the router and before you create a new tunnel, enter the **ip cef** global configuration command followed by the **ip cef distributed** global configuration command.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea32437

  Symptoms: Quality of service (QoS) policing and QoS marking may not function on a Cisco 7200 series Network Service Engine-1 (NSE-1).

  Conditions: This symptom is observed when QoS policing and QoS marking are configured on the main interface of the NSE-1, but traffic is switched on the subinterfaces of this main interface.

  Workaround: If this is an option, switch traffic on the main interface instead of on the subinterfaces.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea37783

  Symptoms: Even though you can configure Distributed Link Fragmentation and Interleaving (DLFI) on a Multilink PPP (MLP) link on an 8-port serial port adapter (PA-8T), interleaving may not function, causing excessive latency on voice traffic.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a Versatile Interface Processor (VIP) and a PA-8T.

  Temporary Workaround: Configure the **tx-ring-limit 2** interface configuration command on the serial interface. Repeat the workaround after the router or the MLP bundle has been reset.

- CSCea37935

  Symptoms: When both Cisco IOS Server Load Balancing (SLB) and Firewall Load Balancing are configured on the same platform, the platform may not send responses to Internet Control Message Protocol (ICMP) echo packets to an SLB virtual IP address.

  Conditions: This symptom is observed on all platforms that support SLB when the ICMP echo reply packet is returned via a firewall farm real server.

  Workaround: There is no workaround.

- CSCea38945

  Symptoms: A Cisco router that is configured with a 2-port Token Ring InterSwitch Link 100BASE-TX port adapter (PA-2FEISL-TX) and a Network Processing Engine G1 (NPE-G1) may reload upon bootup or when you enter the **no shutdown** interface configuration command.

  Conditions: This symptom is observed when support for the PA-2FEISL-TX is missing from a Cisco IOS software release.

  Workaround: Instead of a PA-2FEISL-TX, use a 2-port Fast Ethernet 100BASE-TX port adapter (PA-2FE-TX).

- CSCea39371

  Symptoms: A Cisco 7500 series router may unexpectedly reload because of a bus error.

  Conditions: This symptom is observed when Border Gateway Protocol (BGP), IP version 6 (IPv6), and distributed Cisco Express Forwarding (dCEF) are enabled concurrently.

  Workaround: Disable dCEF; instead, enable CEF.

- CSCea40426

  Symptoms: Encryption and decryption fail for maximum transmission unit (MTU) values between 1419 and 1420 (both inclusive), and the following error is generated:

  ```
  %VPN_HW-1-PACKET_ERROR: slot: 2 Packet Encryption/Decryption error, Other error.
  ```

  The output of the **show pas vam interface** privileged EXEC command displays the "Other Errors" counter; "Other Errors" occur when fragments are reassembled before decryption occurs.

  Conditions: This symptom is observed when you use a Cisco router that is configured with a Virtual Private Network (VPN) acceleration module (VAM) to encrypt traffic through generic routing encapsulation (GRE) tunnel endpoints, which are also configured for tag switching.

  Workaround: To enable the router to fragment packets differently, reduce the value of the tunnel MTU on the router to 1420 using the **ip mtu 1420** interface configuration command.

  Note that the MTU values between 1419 and 1420 for which the failure occurs are from the endpoints.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea48170

  Symptoms: When the RADIUS Load Balancing (RLB) of Cisco IOS Server Load Balancing (SLB) is enabled on a Cisco router, memory corruption may occur and the router may reload unexpectedly.

  Conditions: This symptom is observed when you use Cisco Appliance Server Architecture (CASA) replication or RADIUS sticky objects for high availability.

  Workaround: First, enter the **ip slb vserver** global configuration command; then, deconfigure the **replicate casa** slb-vserver configuration command.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea53049

  Symptoms: A Cisco router that is about to relinquish its designated forwarding position may send "winner" messages instead of "pass" messages, preventing the router that is supposed to become the designated forwarder to actually become the designated forwarder. This situation prevents traffic from being forwarded.

  Conditions: This symptom may be observed when bidirectional Protocol Independent Multicast (PIM) is enabled and you perform an online insertion and removal (OIR).

  Workaround: To clear the affected multicast group, enter the **clear ip mroute** *group-name* EXEC command.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea56559

  Symptoms: A Cisco router may reload during the boot-up process and generate the following error message and traceback:

  ```
  Unexpected exception to CPUvector 1200, PC = 80CEB9A0
  -Traceback= 80 <address>
  ```

  Conditions: This symptom is platform independent.

  Workaround: There is no workaround.

- CSCea58795

  Symptoms: Border Gateway Protocol (BGP) Virtual Private Network (VPN) labels may not be released to free up the available pool of labels in a router when a prefix that has a local label assigned to it is withdrawn. When a very large number of such prefixes is withdrawn, the router may eventually run out of available labels.

  Conditions: This symptom is observed on a Cisco router that functions as a provider edge (PE) router and that has VPN routing/forwarding (VRF) instances configured.

  Workaround: Increase the number of available labels, that is, configure a larger label range.

- CSCea60559

  Symptoms: The Simple Network Management Protocol (SNMP) agent may use 99 percent of the CPU bandwidth of a Route Processor (RP) for an arbitrarily long time (hours or days), without necessarily generating CPUHOG errors. This situation causes other processes on the router to fail because these processes do not receive the CPU bandwidth that they require:

  - Routes may time out.
  - Tunnels may go down.
  - Accessing the router via a Telnet connection to a network port may become impossible.
  - The command-line interface (CLI) via the console line may become quite slow to respond.

  The output of the **show snmp summary** EXEC command may indicate that the number of requests is "N" while the number of replies that were sent is "N-1." The output of the **show processes cpu | include SN** EXEC command may indicate that the SNMP process uses 99 percent of the CPU bandwidth of the RP.

  Conditions: These symptoms are observed when the MPLS-LSR-MIB MIB is enabled, you query the mplsXCTable or a MIB walk occurs, and there are more than 10,000 Multiprotocol Label Switching (MPLS) labels active. The symptoms are platform independent.

  Workaround: Perform the following steps:

  1. Shut down interfaces to bring the total count of active MPLS labels down to far below 10,000.
  2. Disable the MPLS-LSR-MIB MIB by entering the following sequence of commands:

     ```
     snmp-server view nolsrmib mplsLsrMIB exclude
     snmp-server community public view nolsrmib ro
     snmp-server view nolsrmib iso include
     ```

  Enter the **no shutdown** interface configuration command on all the interfaces that you shut down in Step 1.

- CSCea61966

  Symptoms: When you run RADIUS Load Balancing (RLB) of the Cisco IOS Server Load Balancing (SLB) feature in a redundant configuration, the standby RLB switch or router may reload.

  Conditions: This symptom is observed when stateful replication of the RADIUS user-name sticky database is configured.

  Workaround: Configure stateless redundancy.

- CSCea72654

  Symptoms: A Cisco router that is running Multiprotocol Label Switching (MPLS) may reload after a message similar to the following is generated:

  ```
  %SYS-3-OVERRUN: Block overrun at 5414B2C8 (red zone 00000000)
  ```

Conditions: This symptom is observed when more than 672 Label Distribution Protocol (LDP) sessions are established simultaneously and when LDP cannot perform some background tasks for an advertised Label Information Base (LIB) entry before the local label is changed or withdrawn.

Workaround: There is no workaround.

- CSCea73050

  Symptoms: A committed access rate (CAR) output rule may not function on a Spatial Reuse Protocol (SRP) interface.

  Conditions: This symptom is observed on a Cisco 7500 series, regardless if legacy quality of service (QoS) or modular QoS CLI (MQC) is configured.

  Workaround: There is no workaround.

- CSCea74222

  Symptoms: The Interior Gateway Protocol (IGP) label rewrite information for a remote provider edge (PE) router may be lost from a Cisco Express Forwarding (CEF) table on a local PE router.

  Conditions: This symptom is observed when a failure or route flap occurs in the following configuration:

  – The multi-virtual circuit (Multi-VC) mode is enabled in an ATM cell-mode Multiprotocol Label Switching (MPLS) network.

  – Two or more local PE routers are each connected to two separate ATM switches that are configured with label switch controllers (LSCs), or the PE routers are connected to separately controlled partitions of a single ATM switch.

  The following actions cause a failure or route flap:

  – You initiate a processor switch by entering the **switchcc** command.

  – LSC hot redundancy is reset.

  – You enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface in which MPLS is configured.

  Workaround: To recover from the situation, enter the **clear ip route** *network* EXEC command. Enter the loopback address of the remote PE router for which the label rewrite information is lost on the local PE router as the *network* argument.

- CSCea75235

  Symptoms: A Cisco 7200 series or Cisco 7500 series may drop Virtual Private Network (VPN) traffic for a period of time when one of the label switch controllers (LSCs) along a path is reset. The period of time is dictated by the time that a Label-Controlled ATM (LC-ATM) interface requires to reestablish the ATM label virtual circuit (LVC) by using the downstream-on-demand mode.

  Conditions: This symptom is observed on a Cisco 7200 series or Cisco 7500 series that functions in a Multiprotocol Label Switching VPN environment with a LC-ATM core that is configured with multiple paths to an egress provider edge (PE) router.

  Workaround: There is no workaround.

- CSCea80474

  Symptoms: On a Cisco router that runs IP over Multiprotocol Label Switching (MPLS), the Route Processor (RP) on which Label Distribution Protocol (LDP) is configured may attempt to access freed memory, causing the router to reload.

Conditions: This symptom is observed in rare situations on a Cisco router when an interface with hundreds of associated IP addresses is administratively disabled.

Workaround: There is no workaround.

- CSCea84387

  Symptoms: A user session may pause indefinitely, causing a Cisco router to become unresponsive.

  Conditions: This symptom is observed when multiple simultaneous users enter modular QoS CLI (MQC) commands on the same router via separate vty sessions.

  Workaround: Allow only one user at a time to enter MQC commands.

- CSCea84931

  Symptoms: Label Distribution Protocol (LDP) does not send a label release message in response to a label withdraw message.

  Conditions: This symptom is observed in an Any Transport over Multiprotocol Label Switching (AToM) configuration.

  Workaround: There is no workaround.

- CSCea86724

  Symptoms: A Cisco router that is configured for IP over Multiprotocol Label Switching (MPLS) may reload. CPUHOG messages may be displayed on the console before the router reloads.

  Conditions: This symptom is observed in configurations with many interfaces or IP addresses, or with a very large number of labelled prefixes.

  Workaround: There is no workaround.

- CSCea88663

  Symptoms: The Label Distribution Protocol (LDP) session between two adjacent routers may fail to establish when you configure the seconds argument of the **mpls ldp discovery hello interval** *seconds* global configuration command for one router to be significantly shorter in duration than the *seconds* argument of the same command for the other router.

  Conditions: This symptom is observed in an IP over Multiprotocol Label Switching (MPLS) configuration when the router that is configured with the *seconds* argument of longer duration is also configured to actively establish the TCP connection (in conformance with Section 2.5.2 of RFC 3036).

  The output of the **show mpls ldp discovery detail** privileged EXEC command indicates that the associated discovery interface of the router that is configured to actively establish the TCP connection is stuck in the “xmit (not ready)” state.

  The router that passively establishes the TCP connection may indicate via “NBRCHG” log messages that the LDP session comes up and immediately goes down repeatedly.

  Workaround: For both routers, configure the *seconds* argument to be of similar duration by using the **mpls ldp discovery hello interval** *seconds* global configuration command or the **mpls ldp discovery hello holdtime** *seconds* global configuration command.

- CSCeb06452

  Symptoms: When multicast IP version 6 (IPv6) Cisco Express Forwarding (CEF) is enabled, packets (greater than or equal to 232 bytes) that are forwarded may be corrupted.

  Conditions: This symptom is observed on all Cisco platforms during normal multicast CEF software forwarding.

  Workaround: Use process switching.

- CSCeb08400

  Symptoms: When the MPLS VPN—Carrier Supporting Carrier feature is configured, the output of the **show mpls forwarding-table** user EXEC command may not display remote Virtual Private Network (VPN) routing/forwarding (VRF) prefixes on the provider edge (PE) router.

  Conditions: This symptom is observed when the following sequence of events occurs:

  1. You configure the **mpls ip** global configuration command on the interface of the PE router that connects to the customer edge (CE) router.
  2. You configure VRF instances.
  3. The interface of the PE router that connects to the CE router is present in the VRF database.
  4. You configure the **no mpls ip** global configuration command on the interface of the PE router that connects to the CE router.
  5. You enter the **ip address** interface configuration command for the interface of the PE router that connects to the CE router.
  6. You configure Border Gateway Protocol (BGP) VPN version 4 (VPNv4), and, if needed, you configure Interior Gateway Protocol (IGP) on the interface of the PE router that connects to the CE router.
  7. You reconfigure the **mpls ip** global configuration command on the interface of the PE router that connects to the CE router.

  Workaround: Enter the **clear ip route vrf** *vrf-name* EXEC command on the interface of the PE router that connects to the CE router.

  Alternate Workaround: Reload the PE router.

- CSCeb08470

  Symptoms: A Cisco router may reload because of a protocol control information (PCI) parity error, boot up, and then reload again when it dumps the PCI bridge registers.

  Conditions: This symptom is observed on a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCeb09340

  Symptoms: RADIUS Load Balancing (RLB) may ignore the RADIUS framed-IP sticky database while RLB load-balances RADIUS accounting stop requests. Instead, RLB forwards the accounting stop requests to the next real server by using the round robin algorithm. This situation may cause stale host objects on a Service Selection Gateway (SSG).

  Conditions: This symptom is observed when the maximum number of RLB sticky connections for an SSG that is configured as an RLB real server is exceeded.

  Workaround: There is no workaround.

- CSCeb11203

  Symptoms: A Route Reflector (RR) that receives a prefix for a customer edge (CE) router may advertise this prefix to one of its clients, causing an erroneous route to be established.

  Conditions: This symptom is observed on a Cisco 7200 VXR series and a Cisco 7500 series that are running Cisco IOS Release 12.2(14)S1, that function as provider edge (PE) routers that are running IP version 6 (IPv6) in a Multiprotocol Label Switching (MPLS) environment (also referred to as 6PE routers), and that also function as RRs.

  Workaround: There is no workaround.

- CSCeb19074

  Symptoms: The following message may be generated when a Response Time Reporter (RTR) HTTP probe runs:

  ```
  IDMGR-3-INVALID_ID: bad id in id_to_ptr.
  ```

  Conditions: This symptom is observed when Cisco IOS Server Load Balancing (SLB) is configured.

  Workaround: Do not run an RTR HTTP probe when Cisco IOS SLB is configured.

- CSCeb21431

  Symptoms: Even though distributed Cisco Express Forwarding (dCEF) is enabled, a Gigabit Ethernet Interface Processor (GEIP) may fast-switch Multiprotocol Label Switching (MPLS) packets that are received on an Inter-Switch Link (ISL) subinterface instead of switching the packets via dCEF.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a GEIP. The symptom does not occur when the router is configured with a GEIP plus (GEIP+).

  Workaround: There is no workaround.

- CSCeb25177

  Symptoms: Even though distributed Cisco Express Forwarding (dCEF) is enabled, a spatial reuse protocol (SRP) controller may not use dCEF but may use fast switching instead.

  Conditions: This symptom is observed on a Cisco 7500 series when a Multiprotocol Label Switching (MPLS) packet is received.

  Workaround: There is no workaround.

- CSCeb26797

  Symptoms: A directed Label Distribution Protocol (LDP) session between two provider edge (PE) routers may not come up in an Any Transport over Multiprotocol Label Switching (AToM) configuration.

  Conditions: This symptom is observed when the value of the *seconds* argument in the **mpls ldp discovery targeted-hello holdtime** *seconds* global configuration command differs on both PE routers.

  Workaround: Ensure that the value of the *seconds* argument is equal on both PE routers.

- CSCeb28065

  Symptoms: A Cisco router that is configured for IP over Multiprotocol Label Switching (MPLS) may reload.

  Conditions: This symptom is observed when Label Distribution Protocol (LDP) peers of the Cisco router advertise a large number of IP addresses because interfaces flap or are configured.

  Workaround: There is no workaround.

- CSCeb35608

  Symptoms: A memory leak may occur on a Versatile Interface Processor (VIP) because buffers are not returned, which can be verified through the output of the **show memory summary** EXEC command: the first lines in the output display the processor memory and indicate that free memory is decreasing and that the largest contiguous memory block is decreasing.

  Conditions: This symptom is observed on a Cisco 7500 series when the VIP is configured with the **ip mroute-cache distributed** interface configuration command, when there are at least two outgoing interfaces, and when the bandwidth of the incoming traffic exceeds that of the outgoing interfaces.

Possible Workaround: Disable the **ip mroute-cache distributed** interface configuration on the VIP. To free up the held memory, reload the microcode onto the VIP.

- CSCeb36929

  Symptoms: When a Cisco router is performing tag imposition, it may reload because of a bus error.

  Conditions: This symptom is observed when you create a new generic routing encapsulation (GRE) tunnel after the router has booted up and when GRE packets are received through this GRE tunnel and forwarded as Multiprotocol Label Switching (MPLS) packets.

  Workaround: Enter the **tag-switching ip** interface configuration command followed by the **no tag-switching ip** interface configuration command on the newly-created GRE tunnel interface.

- CSCeb53438

  Symptoms: When you manually set the value of the *ring-limit* argument in the **tx-ring-limit** *ring-limit* interface configuration command, the value is lost when you reload the router, even though the value is properly saved in the running configuration and in the startup configuration.

  Conditions: This symptom is observed only when you manually set the value of the *ring-limit* argument for an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) and you reload the router.

  Workaround: There is no workaround.

- CSCeb55043

  Symptoms: A secondary Route Switch Processor (RSP) may reload unexpectedly when a service policy is detached from an ATM permanent virtual circuit (PVC).

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with two RSPs in a redundant configuration.

  Workaround: First, remove the PVC. Then, recreate the PVC without the service policy attached to it.

- CSCeb56909

  Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

  The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

  More details can be found in the security advisory which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml.

- CSCeb57543

  Symptoms: A virtual circuit (VC) that controls tag switching may pause indefinitely.

  Conditions: This symptom is observed on a Cisco 7500 series when you repeatedly perform a manual redundancy switchover.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the affected VC is configured.

- CSCeb65671

  Symptoms: An incorrect virtual circuit (VC) disposition label may be generated, causing packets to drop.

  Conditions: This symptom is observed when VC label attributes, such as a control word setting or a VC type, do not match on a pseudowire.

Workaround: Toggle the interface on which the pseudowire is configured by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCeb66639

  Symptoms: The Gigabit Ethernet ports on a Network Processing Engine G-100 (NPE-G100) may not respond.

  Conditions: This symptom is observed intermittently on a Cisco 7304 when the Gigabit Interface Converter (GBIC) media type is selected.

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

- CSCeb72859

  Symptoms: Bulk configuration synchronization may be triggered when you enter the **exit** command in any configuration mode.

  Conditions: This symptom is observed on Cisco platforms that support high availability (HA) configuration synchronization.

  Workaround: There is no workaround.

- CSCeb79576

  Symptoms: An outgoing label may not be installed in the Label Forwarding Information Base (LFIB) for an IP version 4 (IPv4) prefix.

  Conditions: This symptom is observed when the prefix is learned via a Border Gateway Protocol (BGP) session. This situation may occur when the prefix is deleted in the Label Information Base (LIB) and not allocated to any local label binding.

  Workaround: There is no workaround.

- CSCeb80989

  Symptoms: A Cisco router may reload because an incorrect number of strings are passed to create an error message.

  Conditions: This symptom is observed when a bulk configuration synchronization error occurs.

  Workaround: There is no workaround.

- CSCeb86648

  Symptoms: When NetFlow version 9 is configured, the correct value of the Border Gateway Protocol (BGP) next-hop router may not be present in the NetFlow version 9 records that are exported.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a Network Service Engine 100 (NSE-100) when the **ip flow-export version 9 bgp-nexthop** global configuration command is configured.

  Workaround: There is no workaround. To display the correct value of the BGP next-hop router, enter the **show ip cache verbose flow** EXEC command.

- CSCec05734

  Symptoms: No route may exist, preventing a Label Distribution Protocol (LDP) session from being established. This situation can be verified in the output of the **show mpls ldp discovery** privileged EXEC command.

  Conditions: This symptom is observed on a Cisco 7304 router that is configured with a port adapter carrier card in which a 2-port Fast Ethernet port adapter is installed.

  Workaround: There is no workaround.

- CSCin19645

  Symptoms: Some PPP over Ethernet over ATM (PPPoEoA) sessions may not come up.

  Conditions: This symptom is observed on a Cisco router when you attempt to bring up multiple PPPoEoA sessions across a number of Virtual Private Network (VPN) tunnels.

  Workaround: Disable keepalives on the virtual template.

- CSCin28606

  Symptoms: The output packet and byte counts in the output of a **show interfaces** privileged EXEC command may be invalid and cannot be cleared to 0. Large values may be displayed for output packets and bytes.

  Conditions: This symptom is observed on a Cisco router when you enter a **show interfaces** privileged EXEC command for any type of interface.

  Workaround: There is no workaround.

- CSCin28792

  Symptoms: You may not be able to attach a service policy to an Inverse Multiplexing over ATM (IMA) subinterface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(14)S.

  Workaround: There is no workaround.

- CSCin33181

  Symptoms: A customer edge (CE)-facing Gigabit Ethernet Interface Processor (GEIP), Enhanced Gigabit Ethernet Interface Processor (GEIP+), or a Versatile Interface Processor (VIP) with heavy bidirectional traffic may reload upon online insertion and removal (OIR) of the other VIP facing the core:

  Conditions: This symptom is observed on a GEIP, a GEIP+, or a VIP on a Cisco 7500 series Route Switch Processor (RSP) that is configured with Cisco Any Transport over Multiprotocol Label Switching (MPLS) (AToM).

  Workaround: There is no workaround.

- CSCin33561

  Symptoms: A Cisco switch or router may reload when you configure an ATM User-Network Interface (UNI) link on an ATM interface of an 8-port ATM Inverse MUX E1 or T1 port adapter (PA-A3-8E1IMA or PA-A3-8T1IMA).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series, Cisco 7500 series, and Cisco 7600 series when an ATM link is configured after the platform has booted up.

  Workaround: There is no workaround.

- CSCin33673

  Symptoms: An Inverse Multiplexing over ATM (IMA) interface may not come up.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7600 series when you reload the Multilayer Switch Feature Card (MSFC) or the Route Switch Processor (RSP).

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

- CSCin34322

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

  1. Symptom 1: A Versatile Interface Processor (VIP) may reload unexpectedly.

     Condition 1: This symptom is observed on a Cisco 7500 series when the VIP contains an 8-port ATM Inverse MUX E1 or T1 port adapter (PA-A3-8E1IMA or PA-A3-8T1IMA) and when you reload the Route Switch Processor (RSP).

     Workaround 1: There is no workaround.

  2. Symptom 2: A FlexWAN module may reload unexpectedly.

     Condition 2: This symptom is observed on a Cisco Catalyst 6500 series or a Cisco 7600 series when the FlexWAN module contains an 8-port ATM Inverse MUX E1 or T1 port adapter (PA-A3-8E1IMA or PA-A3-8T1IMA) and when you reload the Multilayer Switch Feature Card (MSFC).

     Workaround 2: There is no workaround.

- CSCin35198

  Symptoms: The SONET MIB data may not be updated. You can verify this situation in the output of the **show controllers sonet** EXEC command.

  Conditions: This symptom is observed on a Cisco router that is configured with a 1-port multichannel STM-1 port adapter.

  Workaround: There is no workaround.

- CSCin35854

  Symptoms: The controller of a 1-port multichannel STM-1 multimode port adapter (PA-MC-STM-1) may remain in the shutdown state. Even after you enter the **no shutdown** controller configuration command, the interface does not come up.

  Conditions: This symptom is observed on a PA-MC-STM-1 that is installed in a Cisco 7500 series when a large number of interfaces are configured on the PA- MC-STM-1.

  Workaround: There is no workaround.

- CSCin37176

  Symptoms: A remote line fault indication (RFI) or remote defect indication (RDI) may bring down an E1 link that is in the local loopback mode.

  Conditions: This symptom is observed on a multichannel STM-1 port adapter (PA- MC-STM1).

  Workaround: There is no workaround.

- CSCin37567

  Symptoms: The line protocol of the some channels of a 1-port multichannel STM-1 port adapter (PA-MC-STM) may go down.

  Conditions: This symptom is observed on a PA-MC-STM that is installed in a Cisco router that is running Cisco IOS Release 12.0 S, Release 12.1 E, Release 12.2 S, or Release 12.2 T.

  Workaround: There is no workaround.

- CSCin37893

  Symptoms: When you configuring a large number of channels on a 1-port multichannel STM-1 port adapter (PA-MC-STM), some of the channels may remain down because of insufficient FIFO resources.

Conditions: This symptom is observed when you reload the Cisco router in which the PA-MC-STM is installed.

Workaround: There is no workaround.

- CSCin39123

  Symptoms: A Cisco router that is configured for Any Transport over Multiprotocol Label Switching (AToM) may send AToM packets that are missing control words, even though control-word imposition is enabled. When another Cisco router receives such malformed packets, the router does not handle these packets properly during disposition.

  Conditions: This symptom may occur on all Cisco routers that employ software switching with AToM enabled. This symptom has specifically been observed on a Cisco 7200 series, Cisco 7400 series, and Cisco 7500 series that are configured for AToM.

  On a Cisco 7200 series router that is processing a heavy traffic load, the reception of malformed packets may cause the router to pause indefinitely.

  Workaround: There is no workaround.

- CSCin39504

  Symptoms: A Cisco router may reload when you remove a service policy configuration that includes the **shape** policy-map class configuration command from an interface or ATM permanent virtual connection (PVC).

  Conditions: This symptom is observed on a Cisco 7500 series but may also occur on other platforms.

  Workaround: There is no workaround.

- CSCin40371

  Symptoms: Traffic loss may occur when you configure the **no ip cef** global configuration command.

  Conditions: This symptom is observed on a Cisco router that has Cisco Express Forwarding (CEF) enabled by default, but that does not have the **no ip cef** global configuration command configured in the startup configuration.

  Workaround: After CEF has been enabled by default, disable CEF.

- CSCin41414

  Symptoms: A Cisco 7200 series may reload.

  Conditions: This symptom is observed when you enter the **verify** EXEC command on a Flash card device.

  Workaround: There is no workaround.

- CSCin41510

  Symptoms: An output service policy with a police feature may be rejected, and the following error message may be generated:

  ```
  Cannot attach flat policy to pvc/sub-interface. Hierarchical policy with shape in
  class-default is recommended
  ```

  Conditions: This symptom is observed when the output service policy is attached to multiple subinterfaces.

  Workaround: There is no workaround.

- CSCin43799

  Symptoms: The “VFC: filesystem” option is missing as a selectable option from the context-sensitive help feature of the command-line interface (CLI).

Conditions: This symptom is observed when you enter "?" after the **copy src filesystem** privileged EXEC command.

Workaround: There is no workaround.

- CSCin51631

  Symptoms: Operation, administration, and maintenance (OAM) management of ATM virtual circuits (VCs) may not function.

  Conditions: This symptom is observed on an 8-port ATM Inverse MUX E1 or T1 port adapter (PA-A3-8E1IMA or PA-A3-8T1IMA) that is installed in a Cisco 7304.

  Workaround: There is no workaround.

- CSCin53739

  Symptoms: When you enter the **show ip cache verbose flow** EXEC command on a Cisco 7304, the output of the command does not display the source interface, and the router may reload unexpectedly.

  Conditions: This caveat is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(18)S and that is configured with a Network Service Engine 100 (NSE-100) when NetFlow accounting is enabled on the Parallel Express Forwarding (PXF) processor of the NSE-100.

  Workaround: There is no workaround.

- CSCin53944

  Symptoms: The Parallel Express Forwarding (PXF) processor of a Network Service Engine 100 (NSE-100) may drop packets.

  Conditions: This condition is observed when Reverse Path Forwarding (RPF) is configured on a Packet-over-SONET (POS) interface and a Class A IP address is assigned to the POS interface.

  Workaround: Change the Class A IP address to another class IP address.

- CSCuk40771

  Symptoms: When IP version 6 (IPv6) packets are switched by using distributed switching, a Versatile Interface Processors (VIP) may reload because of an internal software error.

  Conditions: This symptom is observed on a Cisco 7500 series when Distributed Cisco Express Forwarding version 6 (DCEFv6) is enabled.

  Workaround: Disable dCEFv6 on the interfaces of the VIP.

- CSCuk42146

  Symptoms: The text segment of the software code of a standby Route Switch Processor (RSP) at the location 0x60270244 may have a corrupt value.

  When the standby RSP becomes the active RSP after a forced redundancy switchover, the software code corruption may cause the router to reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2 S and that is configured for High Availability (HA).

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCea60379

  Symptoms: A Cisco router may leak memory at a rate of up to 100 KB per day, resulting in the gradual reduction of the available memory.

Conditions: This symptom is observed on a Cisco router that is running Label Distribution Protocol (LDP). The symptom may be caused by applications that use TCP as the transport protocol.

Workaround: There is no workaround.

Wide-Area Networking

- CSCdz78099

  Symptoms: Multilink Frame Relay (MFR) may not function.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(14)S and Release 12.2(14)S1.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(14)S19

Cisco IOS Release 12.2(14)S19 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S19 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCin95836

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

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

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

  NHRP is not enabled by default for Cisco IOS.

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

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Miscellaneous

- CSCef77013

  Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also result in a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

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

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml.

- CSCsg70474

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

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

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

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

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

- CSCsi60004

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

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

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

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

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

Resolved Caveats—Cisco IOS Release 12.2(14)S18

Cisco IOS Release 12.2(14)S18 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S18 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCed09685

  Symptoms: When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

  Conditions: This problem happens only with command accounting enabled.

  Workaround: Disable command accounting.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

IP Routing Protocols

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing.

This advisory is available at:

http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml.

Miscellaneous

- CSCeb21064

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

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

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

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

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

- CSCek41696

  Symptoms: The **fsck** command does not function.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(14)S17 and that has an ATA file system.

  Workaround: Do not enter the **fsck** command. Rather, enter the **format** command.

- CSCin78325

  Symptoms: A serial interface of a PA-MC-8TE1+ continues to process packets even after the interface is placed in the "ADMINDOWN" state. The counters in the output of the **show interfaces serial** command may continue to increment even if the serial interface is shut down.

  Conditions: This symptom is observed on a serial interface of a PA-MC-8TE1+ when there is a channel-group configuration for the interface.

  Workaround: Remove the channel-group configuration for the interface.

- CSCsc60249

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

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254

  - Real-time Transport Protocol (RTP)
  - Facsimile reception

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

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

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

- CSCsc72722

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

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

  Workaround: There is no workaround.

- 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.

- CSCsd81407

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

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

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

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

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

- CSCsd92405

  Symptoms: A router crashes when receiving multiple malformed TLS and/or SSL3 finished messages. A valid username and password are not required for the crash to occur.

  Conditions: This symptom is observed when a router has HTTP secure server enabled and has an open, unprotected HTTP port.

  Workaround: There is no workaround. Minimize the chances of the symptom occurring by permitting only legitimate hosts to access HTTP on the router.

- CSCsd95616

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

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

- CSCse56501

  Symptoms: When two sockets are bound to the same port, the first File Descriptor always receives the requests.

  Conditions: This symptom is observed on a Cisco router when two sockets such as one IPv4 socket and one IPv6 socket are connected to the same UDP port.

  Workaround: Use different UDP ports for different sockets.

- CSCse68138

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

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

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

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

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

- CSCsg16908

  This bug documents the deprecation and removal of the Cisco IOS FTP Server feature.

- CSCsg40567

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

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

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

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.

- CSCse05736

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

  Conditions: This symptom is seen under the following conditions:

  – The router must have RCP enabled.

  – The packet must come from the source address of the designated system configured to send RCP packets to the router.

  – The packet must have a specific data content.

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

Resolved Caveats—Cisco IOS Release 12.2(14)S17

Cisco IOS Release 12.2(14)S17 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S17 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCeb85136

  Symptoms: An IP packet that is sent with an invalid IP checksum may not be dropped.

  Conditions: This symptom is observed if the IP checksum is calculated with a decreased time-to-live (TTL) value. For example, in the situation where the IP checksum must be 0x1134 with a TTL of 3, if the packet is sent with an IP checksum of 0x1234 that is calculated by using a TTL value of 2, the packet is not dropped. In all other cases, packets with incorrect checksums are dropped.

  Workaround: There is no workaround.

Miscellaneous

- CSCdz84963

  Symptoms: A VIP that is installed in a Cisco 7500 series runs out of memory after some time of operation. The output of the **show processes memory** command shows that the CEF IPC background process holds a lot of memory, and the output of the **show buffers** command on the VIP shows that many buffers are used by IPC.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(18)S8 after dCEF is enabled.

  Workaround: Disable dCEF. Note that the symptom does not occur in Release 12.2(14)S13.

- CSCec31206

  Symptoms: The amount of free memory on a router decreases as the memory that is held by the Simple Network Management Protocol (SNMP) engine process increases. The decrease in the amount of free memory can be verified by examining the output of the **show proc mem | i SNMP** privileged EXEC command.

  Conditions: This symptom is observed when SNMP is used to attempt to set values in the LDP-MIB, TE-MIB, or VPN-MIB.

  Workaround: Avoid using SNMP to set values in the MIBs. Use the CLI on the router to set the values needed.

- CSCed76109

  Symptoms: On a Cisco 7500 series that is equipped with Versatile Interface Processors (VIPs) with ATM port adapters, the ATM PVCs may not come back up after the ATM interface flaps. This occurs because the interfaces in the VIP do not transmit any packets but still process incoming traffic.

  Conditions: This symptom is observed in a dLFIoATM environment in which distributed Class Based Weighted Fair Queueing (dCBWFQ) is configured on PPPoATM virtual templates.

  Workaround: Apply any kind of distributed queueing on any interface or subinterface of the affected VIP. Doing so triggers all interfaces to start transmitting again, enabling the ATM PVCs to come back up.

- CSCef56327

  Symptoms: You may not be able to configure the **clock source line** command during the configuration of the SONET controller on a Cisco router in which a PA-MC-STM1 port adapter is installed.

  When you enter the **clock source line** command during the configuration of the SONET controller, the output of the **show running-config** command indicates that the clock source is set to line. However, the output of the **show controllers sonet** command indicates that the clock is set to internal, and when you enter the **show running-config** command again, the output indicates this time that the clock source is set to internal.

  Conditions: This symptom is observed when the PA-MC-STM1 port adapter is connected back-to-back via dark fiber to another PA-MC-STM1 port adapter.

  Workaround: Enter the **overhead s1byte ignore** command on the SONET controller before you configure the clock source.

- CSCin41510

  Symptoms: An output service policy with a police feature may be rejected, and the following error message may be generated:

  ```
  Cannot attach flat policy to pvc/sub-interface. Hierarchical policy with shape in
  class-default is recommended
  ```

  Conditions: This symptom is observed on a Cisco 7500 series when the output service policy is attached to multiple subinterfaces.

  Workaround: There is no workaround.

- CSCse56501

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

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml.

- CSCsi01470

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

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

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

Resolved Caveats—Cisco IOS Release 12.2(14)S16

Cisco IOS Release 12.2(14)S16 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S16 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCdv46906

  Symptoms: A router may send linkUp traps with the loclfReason attribute set as “Down” and linkDown traps with the loclfReason attribute set as “Up.”

  Conditions: This symptom is observed on a Cisco router that is configured for Simple Network Management Protocol (SNMP).

  Workaround: Query the link status using the command-line interface (CLI) or other SNMP methods.

Interfaces and Bridging

- CSCec87736

  Symptoms: TX Simple Network Management Protocol (SNMP) counters do not update on Fast Ethernet subinterfaces for distributed Cisco Express Forwarding (dCEF) traffic.

  Conditions: This symptom is observed on Cisco IOS Release 12.0(26)S and Release 12.3. The hardware is DEC21140A, and the interface receiving the traffic is not located on the same Versatile Interface Processor (VIP). The symptom may also occur in other releases.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCed60800

  Symptoms: The withdraw message of a multipath (not bestpath) from a BGP neighbor deletes the path from the BGP table but it does not uninstall the route from the IP routing table.

  Conditions: This symptom is observed when the **maximum-paths eibgp** command or **maximum-paths ibgp** command is configured along with **soft-reconfiguration inbound**.

  Workaround: Enter the **clear ip bgp *** or disable the **soft-reconfiguration inbound** or disable the **maximum-paths eibgp** command or **maximum-paths ibgp** command.

  Alternate Workaround: Ensure that the number of possible EBGP peers is less or equal to two. In this situation, the symptom is transient and not obviously noticeable.

ISO CLNS

- CSCdz61787

  Symptoms: A shortest path first (SPF) loop may occur on a router. The output of the **show isis spf-log** EXEC command shows that the loop is triggered by BACKUPOVFL:

  ```
  Level 2 SPF log
  0 18 1 BACKUPOVF
  0 18 1 BACKUPOVFL
  ```

  Conditions: This symptom is observed on a Cisco router that has the **ip fast-convergence** EXEC command enabled and that is configured with specific Intermediate System-to-Intermediate System (IS-IS) metrics.

  Workaround: Remove the **ip fast-convergence** command from all routers in the network by entering the **no ip fast-convergence** EXEC command.

  Alternate Workaround: Adjust the IS-IS metrics.

Miscellaneous

- CSCdz69000

  Symptoms: A Versatile Interface Processor 4-80 (VIP4-80) may reload during normal operation.

  Conditions: This symptom is observed on a Cisco 7500 series when Real-Time Transport Protocol (RTP) and distributed switching are enabled.

  Workaround: Disable distributed switching by entering the **no ip cef distributed** global configuration command.

- CSCea84736

  Symptoms: After you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface, pings may fail on this interface.

  Conditions: This symptom is observed on an interface that has both PPP and Intermediate System-to-Intermediate System (IS-IS) configured.

  Workaround: There is no workaround.

- CSCea87364

  Symptoms: Distributed Cisco Express Forwarding (DCEF) may become disabled on a Versatile Interface Processor (VIP) or Cisco 12000 series line card (LC), and the following error message may appear on the console:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 12: Window did not open, LC to RP IPC is
  non-operational
  ```

  Conditions: This symptom is observed on a Cisco 7500 series VIP2-50 and VIP4- 80 in which ATM OC-3 port adapters such as the PA-A1-OC3 or PA-A3-OC3 are installed when the Cisco 7500 series is upgraded to Cisco IOS Release 12.0(24) S or Release 12.0(24)S1. This symptom is also observed on a Cisco 12000 series LC during significant, prolonged routing table churn.

  Workaround: Reload CEF on the VIP or LC by entering the **clear cef linecard** *slot-number* EXEC command.

  Alternate Workaround: Restart the VIP by performing an online insertion and removal (OIR). Restart the LC by executing the **hw-module slot** *slot #* **reload** command.

- CSCed45746

  Symptoms: Several prefixes for nonredistributed and connected interfaces in different VRFs may be partially bound to the same MPLS VPN label, causing traffic that is bound for one or more of these VRFs to be disrupted.

  Conditions: This symptom is observed on a Cisco router after the VRF interfaces have flapped.

  Workaround: Clear the routes in the VRFs in sequence.

Wide-Area Networking

- CSCdz51400

  Symptoms: A router that is configured as a Home Gateway (HGW) may not correctly remove the per-user route.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.2(7c) or an earlier release and that is configured with per-user routes. The symptom may also occur in other releases.

  Workaround: Reload the HGW.

Resolved Caveats—Cisco IOS Release 12.2(14)S15

Cisco IOS Release 12.2(14)S15 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S15 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCei61732

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

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

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

IP Routing Protocols

- CSCdz41310

  Symptoms: Memory fragmentation may occur on a router.

  Conditions: This symptom is observed when a large number of Open Shortest Path First (OSPF) routes are flapped on a Cisco router.

  Workaround: There is no workaround.

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

ISO CLNS

- CSCeh61778

  Symptom: A Cisco device running IOS and enabled for Intermediate System-to- Intermediate System (IS-IS) routing protocol may reset with a SYS-2-WATCHDOG error from a specifically crafted malformed IS-IS packet. The IS-IS protocol is not enabled by default.

  Conditions: The IS-IS crafted malformed IS-IS Packet that requires processing will not be forwarded across a Level 1/Level 2 boundary. The specifically crafted malformed IS-IS packet would require local attachment to either a Level 1 or Level 2 router. A Cisco device receiving the malformed IS-IS packet will forward the malformed packet to its neighbors, and may reset.

  Workaround: There is no workaround. Enabling IS-IS Authentication is seen as a best practice, and can be leveraged as a mitigation technique.

Miscellaneous

- CSCin31767

  Symptoms: A Cisco router may reload when you enter the **show atm map** privileged EXEC command.

  Conditions: This symptom is observed on all Cisco routers after you have first deleted a subinterface on which a static map bundle was configured.

  Workaround: First remove the static map bundle; then, delete the subinterface.

Resolved Caveats—Cisco IOS Release 12.2(14)S14

Cisco IOS Release 12.2(14)S14 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S14 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsa81379

  NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of NetFlow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supersedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the NetFlow MIB (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

Miscellaneous

- CSCec86420

  Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

This bug is a complementary fix to CSCeb56909 which addresses this vulnerability.

More details can be found in the security advisory which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml.

- CSCef61610

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Resolved Caveats—Cisco IOS Release 12.2(14)S13

Cisco IOS Release 12.2(14)S13 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S13 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial-In User Service (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

IP Routing Protocols

- CSCeb77038

  Symptoms: A Cisco router may pause indefinitely because of a bus error, and the following error message may appear:

  ```
  System returned to ROM by bus error at PC 0x60B5F1C0, address 0xEF4321E5
  ```

  Conditions: This symptom is observed on a Multiprotocol Label Switching (MPLS) provider edge (PE) router.

  Workaround: There is no workaround.

- CSCee41172

  Symptoms: The **maximum-paths import** *number-of-paths* command enables a VRF to import additional paths in addition to the bestpath. If the original path of the import path is withdrawn, wrong import paths may be purged. This situation may cause traffic disruption up to 15 seconds.

  Conditions: This symptom is observed when the original path of the best import path is withdrawn and the import path is at the end of the path list (that is, the one learned the very first). In this situation, all import paths that are derived from other paths may be purged as well. If the imported net has only import paths, the net may not be reachable until other paths are reimported.

  Workaround: Ensure that the import path is at the top of the path list or use the same route descriptor (RD) for all import paths.

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Miscellaneous

- CSCdz45785

  Symptoms: The **protocol ppp virtual-template** *number* interface configuration command may not function.

  Conditions: This symptom is platform independent and is observed in an environment that uses permanent virtual circuits (PVCs) or switched virtual circuits (SVCs).

  Workaround: There is no workaround.

- CSCeb52181

  Symptoms: A Cisco platform that accesses the "system:/vfiles/tmstats_ascii" virtual file (for example, via "more system:/vfiles/tmstats_ascii") may crash because of bus error.

  Conditions: This symptom is observed under normal working conditions when no configuration changes are made on a Cisco platform that runs Cisco IOS Release 12.0S, 12.1E, 12.2, 12.2S, or 12.3. When the "system:/vfiles/tmstats_ascii" virtual file is not used, the symptom does not occur.

  Workaround: There is no workaround.

- CSCed81317

  Symptoms: When an import map is configured on a VPN Routing/Forwarding (VRF) instance, the CE-learned routes are filtered out, preventing them from appearing in the VRF routing table.

  Conditions: This symptom is observed when the **import map** *word* command is configured as part of the VRF configuration. Note that eBGP routes are not filtered out.

  Workaround: There is no workaround.

- CSCed95499

  Symptoms: A Cisco router may crash if a PA driver attempts to convert an uncached iomem address to a cached iomem address.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

  Workaround: There is no workaround.

- CSCef10863

  Symptoms: A router may reload when NBAR protocol discovery statistics are displayed or when the NBAR protocol discovery is disabled on a serial interface.

  Conditions: This symptom is observed on a Cisco 1800 series and Cisco 3745 that run Cisco IOS interim Release 12.3(9.10)T. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

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

Resolved Caveats—Cisco IOS Release 12.2(14)S12

Cisco IOS Release 12.2(14)S12 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S12 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml.

Interfaces and Bridging

- CSCeb45429

  Symptoms: A channelized interface of a PA-MC-T3 port adaptor on a Cisco 7500 series may fail to bring up its line protocol.

  Conditions: This symptom is observed when keepalives are configured.

  Workaround: There is no workaround. Note that reloading the router does not solve the problem.

IP Routing Protocols

- CSCin31057

  Symptoms: A router may reload when a subinterface with a certain configuration is deleted.

  Conditions: This symptom is observed on a Cisco router that has multicast and the Hot Standby Routing Protocol (HSRP) configured.

  Workaround: Remove the multicast configuration before deleting the subinterface.

Miscellaneous

- CSCdz45785

  Symptoms: The **protocol ppp virtual-template** *number* interface configuration command may not function.

  Conditions: This symptom is platform-independent and is observed in an environment that uses permanent virtual circuits (PVCs) or switched virtual circuits (SVCs).

  Workaround: There is no workaround.

- CSCea74331

  Symptoms: A Cisco 7200 series or Cisco uBR7200 series may reload unexpectedly when you perform an online insertion and removal (OIR) of a 2-port multichannel T3 port adapter (PA-MC-2T3).

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco uBR7200 series that run Cisco IOS Release 12.2 when the interfaces of the PA-MC-2T3 are configured for PPP encapsulation. The symptom may occur also in other releases.

  Workaround: There is no workaround.

- CSCec06146

  Symptoms: A serial interface of a channelized port adapter may fail to enter the “up/up” state when you initially configure the interface or after a number of reconfigurations.

  Conditions: This symptom is observed on a channelized port adapter that is installed in a Cisco 7500 series or Cisco 7600 series when the following sequence of events occurs:

  1. You configure an interface by entering the **controller e3** *slot/port* global configuration command followed by the **e1** *line-number* **channel-group** *channel* **timeslots** *range* controller configuration command.

2. You delete the interface by entering the **controller e3** *slot/port* global configuration command followed by the **no e1** *line-number* **channel-group** *channel* controller configuration command.
3. You reconfigure the interface by entering the commands listed in Step 1.

Although the symptom may occur when you initially configure the interface, it is more likely to occur when you configure, delete, and reconfigure the interface several times. In addition, the symptom may also occur after a link flap of an interface of one of the channelized cards.

The symptom may occur on any of the following channelized port adapters: PA-MC-T3, PA-MC-2T3, PA-MC-xT1 (x = 2,4,8), PA-MC-xE1 (x = 2,4,8), and PA-MCX-xTE1 (x = 2,4,8).

Workaround: When the interface does not enter the "up/up" state, configure the interface again.

- CSCin39446

  Symptoms: Traffic may stall on a few channels of certain port adapters.

  Conditions: This symptom is observed on the following Cisco port adapters:

  - PA-MC-xT1
  - PA-MC-xE1
  - PA-MC-xT3
  - PA-MCX-xTE1
  - PA-MC-xE3 where x = number of ports

  Workaround: Reprovision the affected channels on the port adapters.

- CSCin66542

  Symptoms: The line protocol on a T1 of a T3 controller in a PA-MC-2T3+ port adapter may stay in the down state even when looped.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(14)S10

Cisco IOS Release 12.2(14)S10 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S10 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCea70296

  Symptoms: A router may crash when an ARP entry ages out.

  Conditions: This symptom is observed when the ARP entry is internally rearranged during the ARP table lookup process and when a race condition occurs between the ARP table lookup process and other processes on the router.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb56909

  Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

  The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

  More details can be found in the security advisory which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml.

Wide-Area Networking

- CSCee57544

  Symptoms: An IP ping may only go through for 60 percent across a multipoint Frame Relay link on a Cisco 7500 series that is configured for dCEF.

  Conditions: This symptom is observed on a Cisco 7500 series that runs the rsp-jsv-mz image of Cisco IOS Release 12.2(14)S9.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(14)S9

Cisco IOS Release 12.2(14)S9 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S9 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCdw65342

  Symptoms: CyBus error 10 and QA zero link errors may occur some time after a switchover.

  Conditions: This symptom is observed on a Cisco 7500 series when a VIP reads an invalid “bufhdr” pointer and attempt to write it to MEMD.

  Workaround: There is no workaround.

- CSCea58795

  Symptoms: Border Gateway Protocol (BGP) Virtual Private Network (VPN) labels may not be released to free up the available pool of labels in a router when a prefix that has a local label assigned to it is withdrawn. When a very large number of such prefixes is withdrawn, the router may eventually run out of available labels.

  Conditions: This symptom is observed on a Cisco router that functions as a provider edge (PE) router and that has VPN routing/forwarding (VRF) instances configured.

  Workaround: Increase the number of available labels, that is, configure a larger label range.

- CSCee03112

  Symptoms: Downloading to an ATA flash disk may fail and the following error may appear:

  ```
  %Error writing disk2:/c7200-js-mz.122-14.S7.bin (TF I/O failed in data-out phase)
  ATA_Status time out waiting for card ready.
  ATA_Status time out waiting for card ready.
  ```

```
ATA_Status time out waiting for card ready.
```

The image size on the flash disk is 0 bytes.

Conditions: This problem is seen on a Cisco 7200 series NPE-G1 that runs Cisco IOS Release 12.2(14)S5 or Release 12.2(14)S7.

Workaround: Attempt a second time; the second attempt may be successful, but you will need to check the image size, even if there were no errors.

- CSCed40933

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory, which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml.

Resolved Caveats—Cisco IOS Release 12.2(14)S7

Cisco IOS Release 12.2(14)S7 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S7 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCea42500

  Symptoms: If the **default-information originate** router configuration command is entered on the Virtual Private Network (VPN) routing/forwarding (VRF) instance of a Cisco router that has the **address-family ipv4 vrf** command configured using the Border Gateway Protocol (BGP), the default route is learned correctly but the default route is entered incorrectly in the BGP routing table. This behavior may result in unexpected behavior on the other router if the other router does not have a correct default route.

  The default static route of the VRF is not advertised by BGP after the default static route is configured under the VRF, and BGP may advertise the incorrect default route that is in the BGP routing table.

  Conditions: This symptom is observed on a Cisco router that is running BGP.

  Workaround: Perform either of the following steps:

  - Enter a static default route under the VRF configuration.
  - Configure an access control list (ACL).

- CSCeb32598

  Symptoms: A Cisco router may reload when you enter the **show ip bgp regexp** EXEC command repeatedly. The router may also reload when you enter the **show ip bgp** EXEC command after you enter the **show ip bgp regexp** EXEC command.

  Conditions: This symptom is observed on a Cisco router that is configured with inbound policies that contain prefix lists, autonomous system path filter lists, and so on.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb22276

  Symptoms: Some Simple Network Management Protocol (SNMP) packets may linger in the input queue while they are processed. However, the packets do exit the queue on their own without any intervention from the user. This fix allows these packets to be removed from the queue more quickly.

  Conditions: This symptom is observed on a device that runs Cisco IOS software and that supports SNMP operations. In addition, the SNMP request must contain a valid community string.

  Workaround: Protect the SNMP community strings with good password management. Permit SNMP traffic only from trusted devices.

- CSCec37143

  Symptoms: Operation, Administration, and Maintenance (OAM) cells may be dropped from an ATM interface.

  Conditions: This symptom is observed when an input service policy is applied.

  Workaround: Disable OAM.

  Alternate Workaround: Remove the service policy.

- CSCed20042

  Symptoms: A Cisco router may unexpectedly reload if IPv6 encounters a routing loop, and IPv6 CEF is enabled.

  Conditions: This symptom occurs under the following conditions:

  - IPv6 must be enabled
  - IPv6 CEF must be enabled
  - The IPv6 RIB must have recursive entries that form a loop, for example:

```
Router# show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
B   ::/0 [200/0]
     via 2::2
C   1::/64 [0/0]
     via ::, Ethernet0/0
L   1::2/128 [0/0]
     via ::, Ethernet0/0
C   2::/64 [0/0]
     via ::, Ethernet1/0
L   2::1/128 [0/0]
     via ::, Ethernet1/0
B   2001::/16 [200/0]
     via 2002::1
B   2002::/16 [200/0]
     via 2001::1
L   FE80::/10 [0/0]
```

```
     via ::, Null0
L    FF00::/8 [0/0]
     via ::, Null0
```

Note that 2001::/16 and 2002::/16 results in a recursion loop because 2001::/16 is accessible via 2002::/16 and 2002::/16 is accessible via 2001::/16.

Workaround: Disable IPv6 CEF using the global configuration command **no ipv6 cef**.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed45698

  Symptoms: Unused ports on a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may flap even when they are not processing any traffic.

Conditions: This symptom is observed when there is congestion on used ports of the PA-MC-STM-1 and when a committed access rate (CAR) is configured on these used ports.

Workaround: There is no workaround.

- CSCed51664

  Symptoms: Gigabit Ethernet interfaces on a Network Processing Engine G-1 (NPE-G1) may not accept packets with long MPLS headers. This situation may decrease the performance of some network environment such as an Ethernet over MPLS (EoMPLS) environment.

  Packets with a size that exceeds the maximum MTU in the output of the **show controller gigabitethernet 0/x** command may be dropped.

  Conditions: This symptom is observed on a Cisco 7200 series.

  Workaround: Increase the MTU at the interface level.

- CSCed68575

  Cisco Internetwork Operating System (IOS) Software releases trains 12.0 S, 12.1 E, 12.2, 12.2 S, 12.3, 12.3 B and 12.3 T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

Resolved Caveats—Cisco IOS Release 12.2(14)S5

Cisco IOS Release 12.2(14)S5 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S5 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCea15963

  Symptoms: In a setup that has two redundant provider edge (PE) routers that are connected to a Virtual Private Network (VPN), both of the PE routers may originate Multicast Distribution Tree (MDT) updates for the VPN source.

  In a worst case scenario, both PE routers may send a different mapping than the mapping that would cause the receivers to toggle between the different MDT data groups. In this situation, an immediate loss of data may be observed on the receivers.

  Conditions: This symptom is observed in a setup that has two redundant PE routers that are connected to a VPN source.

  Workaround: There is no workaround.

- CSCea20948

  Symptoms: Bridging and PPP are configurable on the same interface, but they will not work together.

  Conditions: This symptom occurs on a Cisco 7500 series router that is running the rsp-pv-mz image.

  Workaround: There is no workaround.

- CSCea27138

  Symptoms: Data Multicast Distribution Tree (MDT) mappings may be deleted too soon, causing a loss of data, or may not be deleted at all, causing unnecessary data to be transferred.

  Conditions: These symptoms are observed on a receiving provider edge (PE) router.

  Workaround: There is no workaround.

- CSCea84931

  Symptoms: Label Distribution Protocol (LDP) does not send a label release message in response to a label withdraw message.

  Conditions: This symptom is observed in an Any Transport over Multiprotocol Label Switching (AToM) configuration.

  Workaround: There is no workaround.

- CSCeb26389

  Symptoms: The same local label may be allocated to two different prefixes, which may be learned via two different routing protocols.

  The Cisco Express Forwarding (CEF) entry for these two prefixes shows the same local label. Depending on how the route was learned, the local label in the Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP) database may show the same label or two different labels for the two prefixes.

  The Multiprotocol Label Switching (MPLS) forwarding table has only one entry that matches the last prefix that used the local label, and there is no entry for the other prefix. This situation may lead to a connectivity failure for the prefix that does not have an entry in the MPLS forwarding table.

  Conditions: These symptoms are observed on a Cisco router that is configured with the MPLS VPN Carrier Supporting Carrier—IPv4 BGP Label Distribution feature and that has both BGP IP version 4 (IPv4) label distribution entries and LDP entries in the Routing Information Base (RIB).

  The symptoms occur when a route is learned via both BGP IPv4 label distribution and Interior Gateway Protocol (IGP) (for example via Open Shortest Path First [OSPF] or Intermediate System-to-Intermediate System [IS-IS]), and the route that is learned via BGP IPv4 label distribution replaces the route that is learned via IGP in the RIB.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdx74321. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Ensure that the local label is reallocated for the first prefix that does not have an entry in the MPLS forwarding table:

  - If the first prefix is learned via BGP IPv4 label distribution, enter the **clear ip bgp** *neighbor-address* or **clear ip bgp *** privileged EXEC command.
  - If the first prefix is learned via IGP and allocated by LDP, enter the **no mpls ip** global configuration command followed by the **mpls ip** global configuration command in order to restart LDP. If the route can be removed from IGP and then relearned via BGP IPv4 label distribution, LDP reallocates a local label.

- CSCeb47812

  Symptoms: A Cisco 7500 series or Cisco 7600 series may generate the following error message on its console:

  ```
  Invalid memory action (malloc) at interrupt level
  ```

Conditions: This symptom is observed when you enter the **clear counters** EXEC command.

Workaround: There is no workaround.

- CSCeb52270

  Symptoms: An interface of a Cisco 7200 series may not be able to receive traffic that is destined for an address that is configured on the router.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(14)S1.

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

- CSCeb53438

  Symptoms: When you manually set the value of the *ring-limit* argument in the **tx-ring-limit** *ring-limit* interface configuration command, the value is lost when you reload the router, even though the value is properly saved in the running configuration and in the startup configuration.

  Conditions: This symptom is observed only when you manually set the value of the *ring-limit* argument for an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) and you reload the router.

  Workaround: There is no workaround.

- CSCeb54536

  Symptoms: Memory allocation failure (MALLOCFAIL) errors may occur when you apply configuration changes to an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) or when traffic passes through the PA-MC-8TE1+.

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 65556 bytes failed from
  Pool: I/O  Free: 12976  Cause: Not enough free memory
  Alternate Pool: None  Free: 0  Cause: No Alternate pool

  -Process= "Pool Manager", ipl= 0, pid= 5
  -Traceback= 606377A4 60638FC0 606332A8 6060F7B0 606451C8 6064530C
  ```

  Unexpected drops in the Weighted Random Early Detection (WRED) system may also occur.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(14)S, Release 12.2(14)S1, Release 12.2(14)S2, or Release 12.2(14)S3 and that is configured with a Network Processing Engine G-1 (NPE-G1) in which a PA-MC-8TE1+ is installed. The symptom does not occur when the PA-MC-8TE1+ is enabled in the NPE-G1 but no configuration is applied or traffic is not processed in the PA-MC-8TE1+.

  Workaround: There is no workaround.

- CSCeb65671

  Symptoms: An incorrect virtual circuit (VC) disposition label may be generated, causing packets to drop.

  Conditions: This symptom is observed when VC label attributes, such as a control word setting or a VC type, do not match on a pseudowire.

  Workaround: Toggle the interface on which the pseudowire is configured by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCeb76341

  Symptoms: A label may not be assigned for a peer provider edge (PE) router.

  Conditions: This symptom is observed on a Cisco 7500 series and a Cisco 12000 series in a Virtual Private Network (VPN) configuration with multiple route reflectors (RRs) and label controlled ATM (LC-ATM) links between PE routers. The symptom may also occur on other platforms.

  Workaround: There is no workaround.

- CSCec08434

  Symptoms: The Cisco 7200 series boothelper image for Cisco IOS Release 12.2(14)S2 may reload unexpectedly, and the router may return to the ROM monitor (ROMmon) mode.

  Conditions: This symptom is observed when you install a 2-port Token Ring Inter-Switch Link 100BASE-TX port adapter (PA-2FEISL-TX) or a 1-port ATM Enhanced OC-3 Packet-over-SONET (POS) port adapter in a Cisco 7200 series Network Processing Engine G-1 (NPE-G1) and you reload, reset, or power up the router with the boothelper image.

  Workaround: Remove the PA-2FEISL-TX or 1-port ATM Enhanced OC-3 POS port adapter when you reload, reset, or power up the router with the boothelper image. Once the router has booted up, you can reinstall the port adapters.

- CSCec26643

  Symptoms: Packet over SONET (POS) interfaces on a 1-port Packet-over-SONET OC-3c/STM-1 port adapter (PA-POS-OC3) installed in a Cisco 7200 series router that is running Cisco IOS Release 12.2(14)S3 may stop transmitting packets. The output packets counter stops incrementing.

  Conditions: This symptom occurs when the router is reloaded with queueing configuration on POS interfaces.

  Workaround: Remove queueing configuration before reload and apply it later when the router is up and running.

- CSCin33783

  Symptoms: Entering the **shutdown** command followed by the **no shutdown** command on the Gigabit Ethernet interface prevents customer edge-to-customer edge (CE-to-CE) pings from going through.

  Conditions: This symptom is observed when Ethernet over Multiprotocol Label Switching (EoMPLS) is configured in VLAN mode on the Gigabit Ethernet interface of a Network Processing Engine G1 (NPE-G1) on a Cisco 7200 series router.

  Workaround: Configure EoMPLS in VLAN mode on a port adapter (for example, Gigabit Ethernet or Fast Ethernet).

- CSCin39123

  Symptoms: A Cisco router that is configured for Any Transport over Multiprotocol Label Switching (AToM) may send AToM packets that are missing control words, even though control-word imposition is enabled. When another Cisco router receives such malformed packets, the router does not handle these packets properly during disposition.

  Conditions: This symptom may occur on all Cisco routers that employ software switching with AToM enabled. This symptom has specifically been observed on a Cisco 7200 series, Cisco 7400 series, and Cisco 7500 series that are configured for AToM.

  On a Cisco 7200 series router that is processing a heavy traffic load, the reception of malformed packets may cause the router to pause indefinitely.

  Workaround: There is no workaround.

- CSCin49458

  Symptoms: Pings between two customer edge (CE) routers may fail.

  Conditions: This symptom is observed after a high traffic load has occurred for a short period of time on Any Transport over Multiprotocol Label Switching (AToM) Layer 2 Tunneling Protocol version 3 (L2TPv3) virtual circuits (VCs). The VCs stay up, but pings may fail.

  Workaround: Reload the microcode onto the line card on which the VCs are configured.

- CSCin55053

  Symptoms: The interface output rate counter of a 1-port E3 serial port adapter (PA-E3) may reset and remain at zero, even though traffic is leaving the interface.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(14)S when the PA-E3 is configured with a service policy and is subjected to a high traffic load.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(14)S3

Cisco IOS Release 12.2(14)S3 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S3 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCea51200

  Symptoms: Subinterface counters may increment more slowly than expected when the **show interface atm** EXEC command is entered on a subinterface.

  Conditions: This symptom is observed when a user enters the **show interface atm** EXEC command on the subinterface of a Cisco router while traffic is going through the interface.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCea66323

  Symptoms: A Cisco router may reload when the tunnel bandwidth is changed at the ingress point of a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel.

  Conditions: This symptom is observed in a multivendor environment. Another Cisco router serves as the ingress point of the MPLS TE tunnel.

  Workaround: There is no workaround.

Miscellaneous

- CSCdz66770

  Symptoms: Tag Distribution Protocol (TDP) may not convey the label change information for a prefix that is learned via an exterior Border Gateway Protocol plus (EBGP+) label to its TDP peers.

Conditions: This symptom is observed on a Cisco 7500 series when TDP is used. The symptom does not occur when Label Distribution Protocol (LDP) is used.

Workaround: There is no workaround.

- CSCea25265

  Symptoms: A Parallel Express Forwarding (PXF) network processor may reload and generate the following error messages:

  ```
  %PXF-2-EXCEPTION: PXF exception on unit tmc.
  %PXF-2-RESTARTED: PXF tmc restarted.
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a Network Service Engine-1 (NSE-1) and on a Cisco 7400 series. The symptom occurs when the router receives a large number of streaming video feeds.

  Workaround: Disable PXF by entering the **no ip pxf** global configuration command.

- CSCea25707

  Symptoms: A Cisco router may reload because of a software condition when running the LDP-MIB MIB. The router reloads because of a process watchdog timeout in the "SNMP ENGINE" process and logs an entry similar to the following one and logs a traceback:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SNMP ENGINE.
  %Software-forced reload
  Unexpected exception, CPU signal 23, PC = 0x606F1FC4 ... Cause 00000024 (Code 0x9):
  Breakpoint exception
  ```

  Conditions: This symptom is observed after the router ID has been changed and when Label Distribution Protocol (LDP) sessions have been added or removed.

  Workaround: Do not change the router ID. If the router ID has been changed, do not run the LDP-MIB MIB.

- CSCea84387

  Symptoms: A user session may pause indefinitely, causing a Cisco router to become unresponsive.

  Conditions: This symptom is observed when multiple simultaneous users enter modular QoS CLI (MQC) commands on the same router via separate vty sessions.

  Workaround: Allow only one user at a time to enter MQC commands.

- CSCeb05672

  Symptoms: Cisco IOS Server Load Balancing (SLB) packets that are switched at the process level instead of at the Forwarding Information Base (FIB) level may be dropped by a Cisco router.

  Conditions: This symptom is observed when the virtual IP destination address is a dynamic alias, which occurs when the virtual IP destination address is a member of a subnet on the interface of a router.

  Workaround: Enable Cisco Express Forwarding (CEF) switching by entering the **ip cef** global configuration command, and enter the **ip route-cache cef** interface configuration command on the destination interface.

- CSCeb11203

  Symptoms: A Route Reflector (RR) that receives a prefix for a customer edge (CE) router may advertise this prefix to one of its clients, causing an erroneous route to be established.

Conditions: This symptom is observed on a Cisco 7200 VXR series and a Cisco 7500 series that are running Cisco IOS Release 12.2(14)S1, that function as provider edge (PE) routers that are running IP version 6 (IPv6) in a Multiprotocol Label Switching (MPLS) environment (also referred to as 6PE routers), and that also function as RRs.

Workaround: There is no workaround.

- CSCeb19074

  Symptoms: The following message may be generated when a Response Time Reporter (RTR) HTTP probe runs:

  ```
  IDMGR-3-INVALID_ID: bad id in id_to_ptr.
  ```

  Conditions: This symptom is observed when Cisco IOS Server Load Balancing (SLB) is configured.

  Workaround: Do not run an RTR HTTP probe when Cisco IOS SLB is configured.

- CSCin40363

  Symptoms: A Cisco platform may reload when you enter the **no tag-switching mtu** interface configuration command.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series, Cisco 7600 series, and Cisco Catalyst 8540 MSR.

  Workaround: There is no workaround. Note that the fix for this caveat is generic in nature and also applies to platforms other than the ones stated in the conditions.

Resolved Caveats—Cisco IOS Release 12.2(14)S2

Cisco IOS Release 12.2(14)S2 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S2 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCin26599

  Symptoms: An enhanced ATM port adapter (PA-A3) may display an increasing “rx_no_buffer” counter in the output of the **show controllers atm** privileged EXEC command, and the PA-A3 port adapter may subsequently pause indefinitely and stop receiving traffic.

  Conditions: This symptom is observed when there is a high-traffic load on the PA-A3. Only the PA-A3 with a specific third-party vendor Segmentation and Reassembly (SAR) chip is affected. Contact your Cisco representative for information about the third-party vendor chip. You can verify the SAR chip revision from the output of the **show controllers atm** privileged EXEC command.

  To verify the SAR chip revision on a Cisco 7500 series, connect to the Versatile Interface Processor (VIP) in which the PA-A3 is installed.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the PA-A3.

- CSCin40163

  Symptoms: An ATM interface may remain administratively down.

  Conditions: This symptom is observed when commands do not have any effect because the command-line interface (CLI) does not function. The symptoms are platform independent.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdu53656

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please see this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCea28131

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please see this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

Miscellaneous

- CSCdy47789

  Symptoms: Directly-connected neighbors may be displayed in the “Targeted Hellos” field in the output of the **show mpls ldp discovery** privileged EXEC, which is incorrect behavior. This situation does not impact routing functionality.

  Conditions: This symptom is observed in an Any Transport over Multiprotocol Label Switching (AToM) environment and is platform independent.

  Workaround: There is no workaround.

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCdz50199

  Symptoms: When the **service-policy** interface configuration command has been configured on any of its interfaces, a Cisco router may reload during the bootup process, and the following error message is logged on the console of the router:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0xABCD, ra=0xFJHK, sp=0xLMNOPQRS
  ```

  Note Pc represents the program counter; ra represents the return address; sp represents the stack pointer.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(15) or Release 12.2(15)T, but may also occur in other releases.

  Workaround: Disable the configuration of the service policy before you reload the router and reapply the configuration of the service policy after the router has been booted up.

- CSCdz51865

  Symptoms: A router may reload when more than two Telnet sessions are established on a router and all sessions try to modify the same class map or policy map, or one session tries to modify the class map or policy map while another session tries to display the policy map by using a **show class-map** or **show policy-map** EXEC command.

  Conditions: This symptom is observed on a router when more than two Telnet sessions have been established.

  Workaround: Do not modify or remove the policy map while you use a **show class-map** or **show policy-map** EXEC command.

- CSCdz56072

  Symptoms: When a 2-port Fast Ethernet 100BASE-TX port adapter (PA-2FE-TX) that is installed in a Versatile Interface Processor (VIP) on a Cisco 7500 series is configured for InterSwitch Link (ISL), the port adapter may send 4 extra bytes at the end of an Ethernet frame, causing frames that are larger than 1496 bytes to be dropped as giant frames by directly-connected devices.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.1(14)E or Release 12.1(14)E1, but may also occur in other releases. The symptom occurs only when ISL is configured.

  Workaround: Use dot1q encapsulation for trunking.

- CSCdz63050

  Symptoms: Outdrops may occur on a native Gigabit Ethernet interface of a Network Processing Engine G1 (NPE-G1), and the “bad length” counter in the output of the **show controllers gigabitethernet** privileged EXEC command may increase.

  This situation may prevent a customer premises equipment (CPE) from using FTP and HTTP communication when the CPE is connected to the Internet via a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) and an L2TP network server (LNS).

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1, that is functioning as an LNS, and that has Cisco Express Forwarding (CEF) enabled.

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

- CSCdz81658

  Symptoms: The interface receive ring of a native Gigabit Ethernet (GE) interface (gig0/1, gig0/2, or gig0/3) on a Network Processing Engine G1 (NPE- G1) may lock up.

  Conditions: This symptom is observed on a Cisco 7200 series router when the maximum transmission unit (MTU) is increased above the value of 2006 and the interface is subjected to stress traffic. (An MTU value of 2006 works fine, but a value of 2007 does not.)

  Workaround: There is no workaround.

- CSCea21064

  Symptoms: The following error message may be generated every minute:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_to_ptr
  -Traceback= 413DD97C 405C4C08 405CB12C 40E387E8 40E34DF0 401DAD1C 401DAD08
  %IDMGR-3-INVALID_ID: bad id in id_to_ptr
  -Traceback= 413DD97C 405C4C08 405CB12C 40E387E8 40E34DF0 401DAD1C 401DAD08
  ```

  Conditions: This symptom is observed when the Cisco IOS Server Load Balancing (SLB) feature is enabled and real time reporter (RTR) entries are created via Simple Network Management Protocol (SNMP).

  Workaround: Ensure that no RTR entries are created via SNMP when the Cisco IOS SLB feature is enabled. Note that the symptom does not occur when RTR entries are created via a command-line interface (CLI) command.

- CSCea25622

  Symptoms: A Network Processing Engine G1 (NPE-G1) may reload unexpectedly and report the following message:

  ```
  System was restarted by reload
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1 and that is running Cisco IOS Release 12.1(14)E; however, this symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea32437

  Symptoms: Quality of service (QoS) policing and QoS marking may not function on a Cisco 7200 series Network Service Engine-1 (NSE-1).

Conditions: This symptom is observed when QoS policing and QoS marking are configured on the main interface of the NSE-1, but traffic is switched on the subinterfaces of this main interface.

Workaround: If this is an option, switch traffic on the main interface instead of on the subinterfaces.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea38945

  Symptoms: A Cisco router that is configured with a 2-port Token Ring InterSwitch Link 100BASE-TX port adapter (PA-2FEISL-TX) and a Network Processing Engine G1 (NPE-G1) may reload upon bootup or when you enter the **no shutdown** interface configuration command.

  Conditions: This symptom is observed in Cisco IOS Release 12.1 E, Release 12.2(4)BW, Release 12.2 S, and Release 12.2 T because support for the PA-2FEISL-TX is missing from these releases.

  Workaround: Instead of a PA-2FEISL-TX, use a 2-port Fast Ethernet 100BASE-TX port adapter (PA-2FE-TX).

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCuk40771

  Symptoms: When IP version 6 (IPv6) packets are switched by using distributed switching, a Versatile Interface Processors (VIP) may reload because of an internal software error.

Conditions: This symptom is observed on a Cisco 7500 series when Distributed Cisco Express Forwarding version 6 (DCEFv6) is enabled.

Workaround: Disable dCEFv6 on the interfaces of the VIP.

TCP/IP Host-Mode Services

- CSCea60379

  Symptoms: High-memory utilization may occur gradually on a router that is running Label Distribution Protocol (LDP), resulting in gradual reduction of the available memory; applications that use TCP as the transport protocol may leak memory.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(23)S and later 12.0 S releases, but may also occur in other releases.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCdz78099

  Symptoms: Multilink Frame Relay (MFR) may not function.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(14)S and Release 12.2(14)S1.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(14)S1

Cisco IOS Release 12.2(14)S1 is a rebuild release for Cisco IOS Release 12.2(14)S. The caveats in this section are resolved in Cisco IOS Release 12.2(14)S1 but may be open in previous Cisco IOS releases.

- CSCdy57048

  Symptoms: TCP transmit packets that are sent from a router in some configurations may be corrupted. This behavior may cause a TCP session to pause indefinitely in one direction.

  Conditions: These symptoms are observed with protocols that use TCP transport (Border Gateway Protocol [BGP] and Telnet are known to be affected). Configurations that may exhibit these symptoms include interfaces that are configured with Multiprotocol Label Switching (MPLS) or Multilink PPP (MLP) encapsulation.

  Workaround: There is no workaround.

- CSCdy81947

  Symptoms: When debug traces are logged to a memory buffer, some debug messages may be missing from the trace, making it difficult to diagnose system problems.

  Conditions: This symptom is observed when there is a heavy traffic load.

  Workaround: There is no workaround.

- CSCdz43747

  Symptoms: A provider edge (PE) router may fail to bind a label for a route.

  Conditions: This symptom is observed after the route has flapped and recovered.

  Workaround: There is no workaround. To recover from the situation, enter the **no mpls ip** global configuration command followed by the **mpls ip** global configuration command.

- CSCdz45760

  Symptoms: A useless partial Shortest Path First (SPF) calculation may occur.

  Conditions: This symptom is observed when an Open Shortest Path First (OSPF) link-state advertisement (LSA) for a 0.0.0.0 destination is refreshed.

  Workaround: Use a static default route.

- CSCdz51138

  Symptoms: An incorrect value is displayed for the ifOperStatus object for High-Speed Serial Interfaces (HSSIs) that are running PPP or propPointToPointSerial encapsulation. A value of “6” (not present) is returned.

  Conditions: This symptom is observed when a Simple Network Management Protocol (SNMP) query is performed on the ifOperStatus object or the propPointToPointSerial encapsulation.

  Workaround: There is no workaround.

- CSCdz53696

  Symptoms: A router may reload or report spurious memory access at the Resource Reservation Protocol (RSVP) process when certain functions are used.

  Conditions: These symptoms may occur when RSVP sends a ResvError or ResvConfirm request from a router that is acting as an RSVP endpoint.

  Workaround: There is no workaround.

- CSCdz67483

  Symptoms: You may not be able to configure the **encapsulation aal0** interface-ATM-VC configuration command for raw cell encapsulation on an ATM permanent virtual circuit (PVC).

  Conditions: This symptom is observed when the **pvc** *vpi*/*vci* **l2transport** interface-ATM-VC configuration command for ATM subinterfaces is configured on the PVC.

  Workaround: There is no workaround.

- CSCdz69161

  Symptoms: When you attempt to enter the **service single-slot-reload-enable** global configuration command, the following error message is generated:

  ```
  % Ambiguous command: "service single-slot-reload-enable"
  ```

  The command appears to be unavailable.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: There is no workaround.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at the following location:

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCdz73574

  Symptoms: Super frame (SF), single domain (SD), and threshold crossing alarms B1, B2, and B3 (TCA_B1, TCA_B2, and TCA_B3) defects may not clear on a Packet-over-SONET (POS) port adapter (PA). This situation may cause the interface of the POS PA to pause permanently.

  Conditions: These symptoms are observed on a POS PA that is installed in a Cisco 7200 series when SF, SD, TCA_B1, TCA_B2, and TCA_B3 defects are asserted and deasserted very quickly.

  Workaround: There is no workaround.

- CSCdz74130

  Symptoms: A bad magic number in the chunk header may lead to a memory corruption and may cause a router to reload.

  Conditions: This symptom is observed after a Resource Reservation Protocol (RSVP) path message is received on a Cisco router that is running Cisco IOS Release 12.2(13)T or Release 12.2 S and RSVP.

  Workaround: There is no workaround.

- CSCdz87238

  Symptoms: Spurious detection of real server failures may occur when Cisco IOS Server Load Balancing (SLB) HTTP probes are active.

  Conditions: This symptom is observed in Cisco IOS Release 12.2 S when probes do not send the configured URL or headers in the request.

  Workaround: Ensure that the request “GET / HTTP/1.0” does return the status that is configured in the **expect** HTTP probe configuration command (which defaults to “200, OK”).

- CSCdz90090

  Symptoms: A Fast Ethernet port may stop receiving unicast packets, causing pings and certain routing protocols to fail. The output of the **show interfaces** privileged EXEC command shows these unicast packets as “ignores.”

  Conditions: This symptom is observed a 2-port Fast Ethernet port adapter (PA-2FE) that is installed in a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCea02355

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at the following location:

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea02713

  Symptoms: A router may unexpectedly reload if it is unable to allocate enough memory for Weighted Random Early Detection (WRED). This unexpected reload may also be seen when the interface is already configured for WRED by using modular quality of service (QoS) and when an access group is added to the interface.

Conditions: This symptom is observed on a router that is running Cisco IOS software that is being configured for WRED on a Frame Relay interface via the modular QoS.

Workaround: There is no workaround.

- CSCea06563

  Symptoms: It may take up to 5 minutes for a traffic engineering (TE) label switched path (LSP) tunnel to come up.

  Conditions: This symptom is observed when you change the encapsulation from High-Level Data Link Control (HDLC) to PPP or when you shut down an interface on which PPP encapsulation is configured.

  Workaround: To enable the TE LSP tunnel to come up immediately, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that functions as the TE LSP tunnel head.

- CSCea07020

  Symptoms: A Cisco router that is configured with Frame Relay subinterfaces may leak memory if those subinterfaces are configured with Random Early Detection (RED). If the subinterfaces are configured with RED, other changes to the configuration may cause the router to leak memory as well. For instance, adding an IP access list to a Frame Relay subinterface that is configured with RED will cause the router to leak memory.

  Conditions: This symptom is observed when traffic shaping is configured with RED, which is configured in the subclass in the service policy.

  Workaround: There is no workaround.

- CSCea09270

  Symptoms: A Cisco router that is functioning in a Multiprotocol Label Switching (MPLS) environment may reload.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2 S when a static recursive route to an IP version 4 (IPv4) internal Border Gateway Protocol (iBGP) peer exists.

  Workaround: Do not configure static recursive routes to the IPv4 iBGP peer.

- CSCea17870

  Symptoms: When Parallel Express Forwarding (PXF) is enabled, a variety of symptoms may occur depending on the Cisco router or switch:

  - A router may reload.
  - A router may not forward packets correctly.
  - The “IPFAST-2-PAKSTICK: Corrupted pak header” error message may be generated.

  Conditions: This symptom is observed when a packet is punted to the Route Processor (RP) and occurs because the paktype was not properly scrubbed after its last use.

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

- CSCea24313

  Symptoms: A router may incorrectly move a default static route from one upstream router to another upstream router and then back again, and may continue to flap the route every 60 seconds.

Conditions: This symptom is observed in the following configuration:

A Cisco router (referred to as router A) is connected to two upstream routers (referred to as router B and router C) via a common interface. Router A is configured with two default recursive static routes, one via an address that is advertised by router B, the other one via an address that is advertised by router C.

The administrative distances of the static routes are set in such a way that if both router B and router C are reachable, router A installs the default static route via router B. If router B becomes unreachable, router A installs the default static route via router C.

Router B is advertising X::1. Router C is advertising X::2. Router A is configured in the following way:

```
ipv6 route ::/0 X::1
ipv6 route ::/0 X::2 2
```

When router B stops advertising X::1, router A removes the default static route via router B and installs the default static via router C. This is correct behavior. However, 60 seconds after the transition, router A incorrectly reinstalls the default static route via router B and removes the default static route via router C. Another 60 seconds later, router A removes the static route via router B and reinstalls the static route via router C. This route flap occurs every 60 seconds.

Possible Workaround: Do not rely on recursive static routes for the default route. For example, configure Interior Gateway Protocol (IGP) on routers B and C to advertise the default route. Appropriate configuration of metrics may ensure that the default route via router B is preferred to the one via router C, providing the same preference as the one that is obtained via static routes.

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page*:

  http://www.cisco.com/warp/public/108/index.shtml

- *Troubleshooting Bus Error Exceptions*:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

- *Why Does My Router Lose Its Configuration During Reboot?*:

  http://www.cisco.com/warp/public/63/lose_config_6201.html

- *Troubleshooting Router Hangs*:

  http://www.cisco.com/warp/public/63/why_hang.html

- *Troubleshooting Memory Problems*:

  http://www.cisco.com/warp/public/63/mallocfail.shtml

- *Troubleshooting High CPU Utilization on Cisco Routers*:

  http://www.cisco.com/warp/public/63/highcpu.html

- *Troubleshooting Router Crashes*:

  http://www.cisco.com/warp/public/122/crashes_router_troubleshooting.shtml

- *Using CAR During DOS Attacks*:

  http://www.cisco.com/warp/public/63/car_rate_limit_icmp.html

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2S. 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 537
- Platform-Specific Documents, page 538
- Feature Modules, page 540
- Cisco Feature Navigator, page 540
- Cisco IOS Software Documentation Set, page 540

Release-Specific Documents

This section provides information about release-specific documents.

Cisco IOS Release 12.2S

The following documents are specific to Cisco IOS Release 12.2S and are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2S*

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Release Notes**

- New Feature Documentation

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**: **Feature Guides**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **New Feature Documentation**: **Cisco IOS Release 12.2 S**: **New Feature Documentation**

- Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **New Feature Documentation**: **Cisco IOS Release 12.2 S**: **System Messages for 12.2S**

Cisco IOS Release 12.2

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 **Technical Support & Documentation > 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.)

Platform-Specific Documents

Platform-specific information and documents for the platforms that are supported in Cisco IOS Release 12.2S are available at the locations listed below:

- Cisco 7200 Series Routers
  - Cisco 7200 series home page on Cisco.com at

    Products & Solutions > Products > Routers and Routing Systems > 7200 Series Routers

  - Cisco 7200 series technical documentation on Cisco.com at

    Products & Solutions > Products > Routers and Routing Systems > 7200 Series Routers > in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7200 Series Routers**

    For Cisco 7200 series technical documentation on http://www.cisco.com/univercd/home/index.htm, select a Cisco 7200 series router from the **Routers** pull-down menu on the top left of the page.

- Cisco 7301 Router and 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**

  - For Cisco 7300 series technical documentation on http://www.cisco.com/univercd/home/index.htm, select a Cisco 7300 series router from the **Routers** pull-down menu on the top left of the page.

- Cisco 7400 Series Routers
  - Cisco 7400 series home page on Cisco.com at

    Products & Solution > Routers & Routing Systems > All Routers & Routing Systems > End-of-Sale and End-of-Life Products > Cisco 7400 Series Routers

  - Cisco 7400 series technical documentation on Cisco.com at

    Products & Solutions > Routers & Routing Systems > All Routers & Routing Systems > End-of-Sale and End-of-Life Products > Cisco 7400 Series Routers > in the "Technical Documentation & Tools" box on the right of page, **Cisco 7400 Series Routers**

  - Cisco 7400 series technical documentation on http://www.cisco.com/univercd/home/index.htm at

    Routers > Cisco 7401

- Cisco 7500 Series Routers
  - Cisco 7500 series home page on Cisco.com at

    Products & Solutions > Routers & Routing Systems > All Routers & Routing Systems > Cisco 7500 Series Routers

  - Cisco 7500 series technical documentation on Cisco.com at

    Products & Solution > Routers & Routing System > All Routers & Routing Systems > Cisco 7500 Series Routers > in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7500 Series Routers**

  - For Cisco 7500 series technical documentation on http://www.cisco.com/univercd/home/index.htm, select a Cisco 7500 series router from the **Routers** pull-down menu on the top left of the page.

- Cisco ONS 15530 and Cisco ONS 15540
  - Cisco ONS 15500 series home page on Cisco.com at

    Products & Solutions > Optical Networking > ONS 15500 Series
  - Cisco ONS 15500 series technical documentation on Cisco.com at

    Products & Solutions > Optical Networking > ONS 15500 Series > in the "Technical Documentation & Tools" box on the right of the page, **Cisco ONS 15500 Series**
  - For Cisco ONS 15500 series technical documentation on http://www.cisco.com/univercd/home/index.htm, select a Cisco ONS platform from the **Optical Networking** pull-down menu on the top left of the page.

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2S 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 12.2S are available at the following location:

On Cisco.com at:

Support > 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 > Cisco IOS Release 12.2 > New Feature Documentation > Cisco IOS Release 12.2 S > New Feature Documentation > 12.2 S New Features by Release

Cisco Feature Navigator

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

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

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

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

Cisco IOS Software Documentation Set

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

Documentation Modules

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

- Configuration guides on Cisco.com at

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

- Command references on Cisco.com at

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

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

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

Cisco IOS Release 12.2 Documentation Set Contents

Table 35 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

Note You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at

Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**

On http://www.cisco.com/univercd/home/index.htm at

Cisco IOS Software: **Release 12.2**

Table 35 Cisco IOS Release 12.2 Documentation Set

Modules	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM N2etworking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing IP Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX

Table 35 Cisco IOS Release 12.2 Documentation Set (continued)

Modules	Major Topics
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service

Table 35 Cisco IOS Release 12.2 Documentation Set (continued)

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

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

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Copyright © 2003–2010 Cisco Systems, Inc. All rights reserved.