Release Notes for Cisco 7000 Family for Cisco IOS Release 12.4XD

April 30, 2009

Cisco IOS Release 12.4(4)XD12

OL-10395-13

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.4 (4)XD12. Cisco IOS Release 12.4 (4)XD supports Cisco 7200 VXR series routers on the NPE-G2, and beginning with Cisco IOS Release 12.4 (4) XD7, also supports the Cisco 7201 router. These release notes are updated as needed.

Note Prior to Cisco IOS Release 12.4 (4)XD7, Cisco IOS Release 12.4 (4)XD supports Cisco 7200 VXR series routers on the NPE-G2 only. Beginning with Cisco IOS Release 12.4 (4) XD7, Cisco IOS Release 12.4(4)XD also supports the Cisco 7201 router.

For a list of the software caveats that apply to Cisco IOS Release 12.4(4)XD12, see the "Caveats for Cisco IOS Release 12.4XD" section on page 24 and *Caveats for Cisco IOS Release 12.4T*. The caveats document is updated for every maintenance release and is located on Cisco.com.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.4T* located on Cisco.com.

Cisco recommends 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

©2008 Cisco Systems, Inc. All rights reserved.

Contents

These release notes describe the following topics:

Inheritance Information

Cisco IOS Release 12.4(4)XD12 is based on Cisco IOS Release 12.4(4)T5. All features in Cisco IOS Release 12.4(4)T5 are in Cisco IOS Release 12.4(4)XD12.

Cisco IOS Release 12.4(4)XD11 is based on Cisco IOS Release 12.4(4)T5. All features in Cisco IOS Release 12.4(4)T5 are in Cisco IOS Release 12.4(4)XD11.

Cisco IOS Release 12.4(4)XD10 is based on Cisco IOS Release 12.4(4)T5. All features in Cisco IOS Release 12.4(4)T5 are in Cisco IOS Release 12.4(4)XD10.

Cisco IOS Release 12.4(4)XD9 is based on Cisco IOS Release 12.4(4)T5. All features in Cisco IOS Release 12.4(4)T5 are in Cisco IOS Release 12.4(4)XD9.

Cisco IOS Release 12.4(4)XD8 is based on Cisco IOS Release 12.4(4)T5. All features in Cisco IOS Release 12.4(4)T5 are in Cisco IOS Release 12.4(4)XD8.

Cisco IOS Release 12.4(4)XD7 is based on Cisco IOS Release 12.4(4)T5. All features in Cisco IOS Release 12.4(4)T5 are in Cisco IOS Release 12.4(4)XD7.

Cisco IOS Release 12.4(4)XD6 is based on Cisco IOS Release 12.4(4)T5. All features in Cisco IOS Release 12.4(4)T5 are in Cisco IOS Release 12.4(4)XD6.

Cisco IOS Release 12.4(4)XD5 is based on Cisco IOS Release 12.4(4)T5. All features in Cisco IOS Release 12.4(4)T5 are in Cisco IOS Release 12.4(4)XD5.

Note Cisco IOS Release 12.4(4)XD4 is based on Cisco IOS Release 12.4(4)T5, label: SYNC_V1244XDT_061009. Only caveats resolved in 12.4(4)T5 before this label are also resolved in Cisco IOS Release 12.4(4)XD4.

Cisco IOS Release 12.4(4)XD3 is based on Cisco IOS Release 12.4(4)T3. All features in Cisco IOS Release 12.4(4)T3 are in Cisco IOS Release 12.4(4)XD3

Cisco IOS Release 12.4(4)XD2 is based on Cisco IOS Release 12.4(4)T3. All features in Cisco IOS Release 12.4(4)T3 are in Cisco IOS Release 12.4(4)XD2.

Cisco IOS Release 12.4(4)XD1 is based on Cisco IOS Release 12.4(4)T1. All features in Cisco IOS Release 12.4(4)T1 are in Cisco IOS Release 12.4(4)XD1.

Cisco IOS Release 12.4(4)XD is based on Cisco IOS Release 12.4(4)T1. All features in Cisco IOS Release 12.4(4)T1 are in Cisco IOS Release 12.4(4)XD.

Table 1 lists sections of the *Cross-Platform Release Notes for Cisco IOS Release* 12.4T that apply to Cisco IOS Release 12.4(4)XD.

Table 1 References for the Cross-Platform Release Notes for Cisco IOS Release 12.4T

Topic	Location
• Introductory information about the Cisco 7000 family of routers • Hardware Supported • Feature Set Tables	On Cisco.com at: **Product Support> Cisco IOS Software > Cisco IOS Software Releases 12.4T > General Information> Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 2: Platform-Specific Information** Or at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/xprn124t/124tfeat.htm
• Determining the Software Version • Upgrading to a New Software Release	On Cisco.com at: **Product Support> Cisco IOS Software > Cisco IOS Software Releases 12.4T > General Information> Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 1: System Requirements** Or at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/xprn124t/124treqs.htm
• Feature Descriptions (New and Changed Information) • MIBs • Important Notes	On Cisco.com at: **Product Support> Cisco IOS Software > Cisco IOS Software Releases 12.4T > General Information> Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 3: New Features and Important Notes** Or at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/xprn124t/124tnewf.htm
• Related Documentation • Obtaining Documentation • Obtaining Technical Assistance	On Cisco.com at: **Product Support> Cisco IOS Software > Cisco IOS Software Releases 12.4T > General Information > Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 4: Related Documentation** Or at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/xprn124t/124tdocs.htm

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(4)XD and includes the following sections:

Memory Recommendations

Warning **Unlike other network processing engines, the Cisco NPE-G2 has its own Cisco IOS software images with the prefix of "c7200p-" in the software image file names. All other network processing engines such as NPE-225, NPE-400 and NPE-G1 are compatible with images with the prefix of "c7200-." The Cisco NPE-G2 does not boot up with a software image with the prefix of "c7200-". Conversely, the other network processing engines such as NPE-225, NPE-400, and NPE-G1 do not boot up with the software image with the prefix of "c7200p-".**

Table 2 Memory Recommendations for the Cisco 7200 VXR Routers on the NPE-G2 and Cisco 7201 Router

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Routers and Cisco 7201 Router	ADVANCED ENTERPRISE SERVICES Feature Set	c7200p-adventerprisek9-mz	256 MB Flash	1 GB DRAM	RAM
	ADVANCED ENTERPRISE SERVICES WITH SNA SWITCHING Feature Set	c7200p-adventerprisek9_sna-mz	256 MB Flash	1 GB DRAM	RAM
	ADVANCED IP SERVICES Feature Set	c7200p-advipservicesk9-mz	256 MB Flash	1 GB DRAM	RAM
	ADVANCED IP SERVICES W/LAWFUL INTERCEPT Feature Set	c7200p-advipservicesk9_li-mz	256 MB Flash	1 GB DRAM	RAM
	ADVANCED SECURITY Feature Set	c7200p-advsecurityk9-mz	256 MB Flash	1 GB DRAM	RAM
	IP BASE W/O CRYPTO Feature Set	c7200p-ipbase-mz	48 MB Flash	1 GB DRAM	RAM
	IP BASE Feature Set	c7200p-ipbasek9-mz	48 MB Flash	1 GB DRAM	RAM
	SP SERVICES Feature Set	c7200p-spservicesk9-mz	256 MB Flash	1 GB DRAM	RAM

Supported Hardware

Cisco IOS Release 12.4(4)XD supports the following Cisco 7000 platforms:

- Cisco 7200 VXR routers on the NPE-G2
- Cisco 7201 router, beginning with Cisco IOS Release 12.4(4)XD7

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 13.

Cisco 7201 Router ROMMON Requirement

The Cisco 7201 router requires ROMMON version 12.4(12.2r)T or later.

C7200 VSA Hardware Requirements

Note Beginning with Cisco IOS Release 12.4(4)XD7, the C7200 VSA and VAM2+ are no longer supported on the Cisco IOS Release12.4XD. Customers who require C7200 VSA or VAM2+ support should migrate to Cisco IOS Release 12.4(15)Tx.

The hardware required to ensure proper operation of the C7200 VSA is as follows:

- The C7200 VSA is compatible with the Cisco NPE-G2 processor on the Cisco 7204VXR or Cisco 7206VXR routers.
- ROMMON requirement: 12.4(4r)XD5 or later
- I/O FPGA requirement: 0x25 (decimal 0.37) or later
- VSA FPGA requirement: 0x13 (decimal 0.19) or later

Determining the ROMMON Version

To determine the ROM monitor (ROMMON) version, enter the show version command as follows. The following sample show version command output is from a router running a Cisco 7200 series software image with Cisco IOS Release 12.4(4)XD12:

```
Router> show version | inc Boot

ROM: System Bootstrap, Version 12.4(4r)XD12, RELEASE SOFTWARE (fc1)
```

Upgrading ROMMON on the NPE-G2

Upgrading the re-writeable ROM monitor (ROMMON) allows you to download a new ROMMON image instead of having to replace hardware (NPE-G2) to get a new image.

For information about upgrading ROMMON on the NPE-G2, refer to the "Upgrading ROMMON on the NPE-G1 or NPE-G2" subsection in the "NPE-G1 and NPE-G2 Installation and Configuration Information" chapter of the *Network Processing Engine and Network Services Engine Installation and Configuration* guide at:

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

Determining the I/O and VSA FPGA Versions

To determine the I/O and VSA FPGA versions, enter the show upgrade fpd file command as follows. The following sample show upgrade fpd file command output is from a router running a Cisco 7200 series software image with Cisco IOS Release 12.4(4)XD6:

```
Router# show upgrade fpd file disk2:c7200p-fpd-pkg.124-4.XD6

============================================================
    Bundled FPD Image Version Matrix
    ================================
                                                 Min. Req.
Supported Card TypesID   Image Name   Version   H/W Ver.
==================== === ============ ======= ===========
    NPEG2 IOFPGA     1   NPEG2 IOFPGA 0.37       0.0
-------------------- --- ------------ ------- -----------
    VSA              1   VSA          0.19       0.0
============================================================
```

Note Beginning with Cisco IOS Release 12.4(4)XD7, the C7200 VSA and VAM2+ are no longer supported on the Cisco IOS Release12.4XD. Customers who require C7200 VSA or VAM2+ support should migrate to Cisco IOS Release 12.4(15)Tx.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the Cisco 7000 family router and enter the **show version** EXEC command. The following sample **show version** command output is from a router running a Cisco 7200 series software image with Cisco IOS Release 12.4(4)XD12:

```
Router> show version
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(4)XD12,
RELEASE SOFTWARE 9 (fc1)
```

Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, refer to *How to Choose a Cisco IOS Software Release* at:

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

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

- Cisco 7200 Series, 7300 Series, 7400 Series, and 7500 Series Routers

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

For *Cisco IOS Upgrade Ordering Instructions*, refer to 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:

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

FPD Image Packages for Cisco 7200 VXR Routers on the NPE-G2

Field Programmable Device (FPD) image packages are used to update FPD images.

FPD Image Package for Cisco IOS Release 12.4(4)XD12

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD12 is the c7200p-fpd-pkg.124-4.XD12.pkg file. This 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 3 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD12

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37 or later	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD11

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD11 is the c7200p-fpd-pkg.124-4.XD11.pkg file. This 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 4 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD11

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37 or later	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD10

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD10 is the c7200p-fpd-pkg.124-4.XD10.pkg file. This 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 5 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD10

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37 or later	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD9

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD9 is the c7200p-fpd-pkg.124-4.XD9.pkg file. This 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 6 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD9

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37 or later	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD8

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD8 is the c7200p-fpd-pkg.124-4.XD8.pkg file. This 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 7 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD8

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37 or later	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD7

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD7 is the c7200p-fpd-pkg.124-4.XD7.pkg file. This 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 8 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD7

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37 or later	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD6

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD6 is the c7200p-fpd-pkg.124-4.XD6.pkg file. This 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 9 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD6

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37 or later	0.0
VSA	1	VSA	0.19 or later	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD5

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD5 is the c7200p-fpd-pkg.124-4.XD5.pkg file. This 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 10 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD5

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37 or later	0.0
VSA	1	VSA	0.19 or later	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD4

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD4 is the c7200-fpd-pkg.124-4.XD4.pkg file. This 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 11 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD4

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37	0.0
VSA	1	VSA	0.19	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD3

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD3 is the c7200-fpd-pkg.124-4.XD3.pkg file. This 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 12 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD3

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.37	0.0
VSA	1	VSA	0.19	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD2

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD is the c7200-fpd-pkg.124-4.XD2.pkg file. This 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 13 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD2

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.36	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD1

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD is the c7200-fpd-pkg.124-4.XD1.pkg file. This 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 14 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD1

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.36	0.0

FPD Image Package for Cisco IOS Release 12.4(4)XD

The FPD image package that is used to upgrade an FPD image that runs Cisco IOS Release 12.4(4)XD is the c7200-fpd-pkg.124-4.XD.pkg file. This 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 15 Cisco 7000 Series FPD Image Package Contents for Release 12.4(4)XD

Supported Card	ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
NPE-G2	1	NPEG2 I/O FPGA	0.36	0.0

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.4(4)XD supports the same feature sets as Cisco IOS Release 12.4(4)T, but Cisco IOS Release 12.4(4)XD can include new features supported by the Cisco 7200 VXR routers on the NPE-G2 or the Cisco 7201 router.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States 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 United

States government regulations. When applicable, purchaser and 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.

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

Table 16, Table 17, Table 18, andTable 19 list the features and feature sets supported by Cisco 7200 VXR routers on the NPE-G 2 and the Cisco 7201 router in Cisco IOS Release 12.4(4)XD and use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, (4) means a feature was introduced in 12.4 (4)XD4. If a cell in this column is empty, the feature was included in the initial base release.

Note These release notes are not cumulative and list only features that are new to Cisco IOS Release 12.4(4)XD. The parent release for Cisco IOS Release 12.4(4)XD is Cisco IOS Release 12.4(4)T. 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 **Product Support> Cisco 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.

Table 16 Feature List by Feature Set for Cisco *7200 VXR Routers on the NPE-G2 and the Cisco 7201 Router*

Features	In	Software Images by Feature Sets	
		c7200p-adventerprisek9-mz	c7200p-adventerprisek9_sna-mz
Support for the 2GB Memory Module (MEM-NPE-G2-2GB)	3	Yes	Yes
Cisco Quality ID		Yes	Yes
Field-Programmable Device Upgrades		Yes	Yes
NPE-G2 Support for the show environment Command		Yes	Yes
USB Storage and USB Storage PKI Enhancements		Yes	Yes

Table 17 Feature List by Feature Set for Cisco *7200 VXR Routers on the NPE-G2 and the Cisco 7201 Router (continued)*

Features	In	Software Images by Feature Sets	
		c7200p-advipservicesk9-mz	c7200p-advipservicesk9_li-mz
Support for the 2GB Memory Module (MEM-NPE-G2-2GB)	3	Yes	Yes
Cisco Quality ID		Yes	Yes

Table 17 Feature List by Feature Set for Cisco *7200 VXR Routers on the NPE-G2 and the Cisco 7201 Router (continued)*

Features	In	Software Images by Feature Sets	
		c7200p-advipservicesk9-mz	c7200p-advipservicesk9_li-mz
Field-Programmable Device Upgrades		Yes	Yes
NPE-G2 Support for the show environment Command		Yes	Yes
USB Storage and USB Storage PKI Enhancements		Yes	Yes

Table 18 Feature List by Feature Set for Cisco *7200 VXR Routers on the NPE-G2 and the Cisco 7201 Router (continued)*

Features	In	Software Images by Feature Sets	
		c7200p-advsecurityk9-mz	c7200p-ipbase-mz
Support for the 2GB Memory Module (MEM-NPE-G2-2GB)	3	Yes	Yes
Cisco Quality ID		Yes	Yes
Field-Programmable Device Upgrades		Yes	Yes
NPE-G2 Support for the show environment Command		Yes	Yes
USB Storage and USB Storage PKI Enhancements		Yes	Yes

Table 19 Feature List by Feature Set for Cisco *7200 VXR Routers on the NPE-G2 and the Cisco 7201 Router (continued)*

Features	In	Software Images by Feature Sets	
		c7200p-ipbasek9-mz	c7200p-spservicesk9-mz
Support for the 2GB Memory Module (MEM-NPE-G2-2GB)		Yes	Yes
Cisco Quality ID		Yes	Yes
Field-Programmable Device Upgrades		Yes	Yes
NPE-G2 Support for the show environment Command		Yes	Yes
USB Storage and USB Storage PKI Enhancements		Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by Cisco 7200 VXR routers on the NPE-G2 and the Cisco 7201 router for Cisco IOS Release 12.4XD:

New Hardware Features in Cisco IOS Release 12.4(4)XD12

There are no new hardware features supported in Cisco IOS Release 12.4(4)XD12.

New Software Features in Cisco IOS Release 12.4(4)XD12

There are no new software features supported in Cisco IOS Release 12.4(4)XD12.

New Hardware Features in Cisco IOS Release 12.4(4)XD11

There are no new hardware features supported in Cisco IOS Release 12.4(4)XD11.

New Software Features in Cisco IOS Release 12.4(4)XD11

There are no new software features supported in Cisco IOS Release 12.4(4)XD11.

New Hardware Features in Cisco IOS Release 12.4(4)XD10

There are no new hardware features supported in Cisco IOS Release 12.4(4)XD10.

New Software Features in Cisco IOS Release 12.4(4)XD10

There are no new software features supported in Cisco IOS Release 12.4(4)XD10.

New Hardware Features in Cisco IOS Release 12.4(4)XD9

There are no new hardware features supported in Cisco IOS Release 12.4(4)XD9.

New Software Features in Cisco IOS Release 12.4(4)XD9

There are no new software features supported in Cisco IOS Release 12.4(4)XD9.

New Hardware Features in Cisco IOS Release 12.4(4)XD8

There are no new hardware features supported in Cisco IOS Release 12.4(4)XD8.

New Software Features in Cisco IOS Release 12.4(4)XD8

There are no new software features supported in Cisco IOS Release 12.4(4)XD8.

New Hardware Features in Cisco IOS Release 12.4(4)XD7

The following new hardware features are supported in Cisco IOS Release 12.4(4)XD7:

Note Beginning with Cisco IOS Release 12.4(4)XD7, the C7200 VSA and VAM2+ are no longer supported on the Cisco IOS Release12.4XD. Customers who require C7200 VSA or VAM2+ support should migrate to Cisco IOS Release 12.4(15)Tx.

Cisco 7201 Router

The Cisco 7201 router provides application-specific features for broadband subscriber aggregation and network application services with high processing performance. The Cisco 7201 is a compact one-rack-unit router that offers four built-in Gigabit Ethernet ports, pluggable Gigabit Ethernet optics (small form-factor pluggable [SFP] optics) one dedicated 10/100-Mbps copper Ethernet Management port, one USB port for general storage and security token storage, one port adapter slot, one CompactFlash Disk slot, 1 GB SDRAM DIMM (upgradable to 2 GB), plus console and auxiliary ports.

For more information about the Cisco 7201 router, refer to the following URL:

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

New Software Features in Cisco IOS Release 12.4(4)XD7

There are no new software features supported in Cisco IOS Release 12.4(4)XD7.

New Hardware Features in Cisco IOS Release 12.4(4)XD6

There are no new hardware features supported in Cisco IOS Release 12.4(4)XD6.

New Software Features in Cisco IOS Release 12.4(4)XD6

There are no new software features supported in Cisco IOS Release 12.4(4)XD6.

New Hardware Features in Cisco IOS Release 12.4(4)XD5

There are no new hardware features supported in Cisco IOS Release 12.4(4)XD5.

New Software Features in Cisco IOS Release 12.4(4)XD5

There are no new software features supported in Cisco IOS Release 12.4(4)XD5.

New Hardware Features in Cisco IOS Release 12.4(4)XD4

There are no new hardware features supported in Cisco IOS Release 12.4(4)XD4.

New Software Features in Cisco IOS Release 12.4(4)XD4

There are no new software features supported in Cisco IOS Release 12.4(4)XD4.

New Hardware Features in Cisco IOS Release 12.4(4)XD3

The following new hardware features are supported by the Cisco 7200 VXR routers on the NPE-G2 for Cisco IOS Release 12.4(4)XD3:

C7200 VSA (VPN Services Adapter) 1.0

Note Beginning with Cisco IOS Release 12.4(4)XD7, the C7200 VSA and VAM2+ are no longer supported on the Cisco IOS Release12.4XD. Customers who require C7200 VSA or VAM2+ support should migrate to Cisco IOS Release 12.4(15)Tx.

The C7200 VSA (VPN Services Adapter) is a full-width service adapter supported in the I/O slot (slot 0) of the Cisco 7204VXR and Cisco 7206VXR routers with the NPE-G2 processor.

Table 20 summarizes the features provided by the VSA.

Table 20 VSA Features

Feature	Description/Benefit
Throughput[1]	Performance to 960 Mbps encrypted throughput using 3DES or AES on the Cisco 7204VXR and Cisco 7206VXR routers
Number of IPSec protected tunnels[2]	Up to 5000 tunnels
Number of tunnels per second	Up to 85 tunnels per second
Hardware-based encryption	Data protection: IPSec DES, 3DES, and AES Authentication: RSA and Diffie-Hellman Data integrity: SHA-1 and Message Digest 5 (MD5)
VPN tunneling	IPsec tunnel mode; Generic Routing Encapsulation (GRE) and Layer 2 Tunneling Protocol (L2TP) protected by IPSec
Minimum Cisco IOS software release supported	12.4(11)Tx
Standards supported	IPSec/IKE: RFCs 2401-2411, 2451

1. As measured with IPSec 3DES HMAC-SHA1 on 1400 byte packets.
2. Number of tunnels supported varies dependent of traffic throughput and the actual deployment topology.

Table 21 lists the performance information for the VSA.

.

Table 21 Performance for VSA

Cisco Router	Throughput[1]	Description
Cisco 7200VXR series routers with the NPE-G2 processor	Performance to 960 Mbps encrypted throughput	Cisco IOS release: 12.4(11)Tx 7200VXR/NPE-G2/VSA, 1GB system memory 3DES/HMAC-SHA or AES/HMAC-SHA, preshared with no IKE-keepalive configured

1. As measured with IPSec 3DES or AES Hashed Message Authentication Code (HMAC)-SHA-1 on 1400-byte packets. Performance varies depending on bandwidth, traffic volume, Cisco IOS software release, and so forth.

For more information about the C7200 VSA, refer to the following Cisco documents:

- *C7200 VSA (VPN Services Adapter) feature module at:*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/index.htm
- *C7200 VSA (VPN Services Adapter) Installation and Configuration Guide at:*

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

New Software Features in Cisco IOS Release 12.4(4)XD3

The following new software features are supported by the Cisco 7200 VXR routers on the NPE-G2 for Cisco IOS Release 12.4(4)XD3:

Support for the 2GB Memory Module (MEM-NPE-G2-2GB)

Beginning with the Cisco IOS Release 12.4(4)XD3, support is included for the 2GB Memory Module (MEM- NPE-G2-2GB).

New Hardware Features in Cisco IOS Release 12.4(4)XD2

The following new hardware features are supported by the Cisco 7200 VXR routers on the NPE-G2 for Cisco IOS Release 12.4(4)XD2:

Cisco 7200 VXR Port Adapter Jacket Card

The Cisco 7200 VXR Port Adapter Jacket Card addresses the demand for additional slot density and flexibility by enabling the I/O slot to hold a single port adapter for additional capacity on systems with the Cisco 7200 VXR NPE-G1 Network Processing Engine and above. Benefits of the jacket card include the following:

- Provides one additional slot for single port adapter (selected port adapter)
- Allows a high-bandwidth port adapter-such as the hardware-based security encryption module SA-VAM2+ and the 2-Port Packet/SONET OC3c/STM1 Port Adapter-to be moved onto a dedicated Peripheral Component Interconnect (PCI) bus that the Cisco NPE-G1 or NPE-G2 provides
- Reduces PCI contention among other port adapters

- Provides a cost-effective way to increase the slot density in parallel to the increased switching capacity of the newest engine of the platform-the Cisco NPE-G2.

For more information about the Port Adapter Jacket Card, refer to the following Cisco document:

- *Port Adapter Jacket Card Installation Guide* at:

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

New Software Features in Cisco IOS Release 12.4(4)XD2

There are no new software features supported in Cisco IOS Release 12.4(4)XD2.

New Hardware Features in Cisco IOS Release 12.4(4)XD1

The following new hardware features are supported by the Cisco 7200 VXR routers on the NPE-G2 for Cisco IOS Release 12.4(4)XD1.

VPN Acceleration Module 2+ (VAM2+)

Note Beginning with Cisco IOS Release 12.4(4)XD7, the C7200 VSA and VAM2+ are no longer supported on the Cisco IOS Release12.4XD. Customers who require C7200 VSA or VAM2+ support should migrate to Cisco IOS Release 12.4(15)Tx.

As of Cisco IOS Release 12.4(4)XD1, support has been included for the VPN Acceleration Module 2+ (VAM2+) on the NPE-G2. VAM2+ is a single-width port adapter that features 128/192/256-bit Advanced Encryption Standard (AES) in hardware, Data Encryption Standard (DES), Triple DES (3DES), and IPv6 IPSec, providing increased performance for site-to-site and remote-access IPSec VPN services. The Cisco VAM2+ provides hardware-assisted Layer 3 compression services with its encryption services, conserving bandwidth and lowering network connection costs over secured links, as well as full Layer 3 routing, quality of service (QoS), multicast and multiprotocol traffic, and broad support of integrated LAN/WAN media.

Note Although VAM2 and VAM2+ are both supported on the NPE-G1, Cisco IOS Release 12.4 (4)XD supports Cisco 7200 VXR series routers on the NPE-G2 only, and has not been tested against the NPE-G1.

For more information about VAM2+, refer to the following Cisco documents:

- VPN Acceleration Module 2+ (VAM2+) feature module at:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/ft_vam2p.htm

- VAM2+ Installation and Configuration Guide at:

  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/portadpt/accelmod/vam2p/index.htm

New Software Features in Cisco IOS Release 12.4(4)XD1

There are no new software features supported in Cisco IOS Release 12.4(4)XD1.

New Hardware Features in Cisco IOS Release 12.4(4)XD

The following new hardware features are supported by the Cisco 7200 VXR routers on the NPE-G2 for Cisco IOS Release 12.4(4)XD:

NPE-G2

Like the NPE-G1, the NPE-G2 provides 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 supported in the Cisco 7200 VXR routers. The NPE-G2, when installed with an I/O controller, provides the bootflash and NVRAM that the Cisco IOS software uses to boot.

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

The NPE-G2 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-G2 consists of one board with multiple interfaces. It can be used only in the Cisco 7200 VXR routers.

The NPE-G2 can be used with the Port Adapter Jacket Card installed in the I/O controller slot. If you are upgrading to an NPE-G2 and Port Adapter Jacket Card at the same time, refer to the *Port Adapter Jacket Card Installation Guide* at the following URL for information about the order of installation of both the NPE-G2 and the Port Adapter Jacket Card:

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

New Software Features in Cisco IOS Release 12.4(4)XD

The following new software features are supported by the Cisco 7200 VXR routers on the NPE-G2 for Cisco IOS Release 12.4(4)XD:

Cisco Quality ID

Cisco IOS Release 12.4(4)XD supports the Cisco Quality ID feature in Cisco transceivers (Gigabit Interface Converter [GBIC] or small form factor pluggables [SFP]).

The Cisco Quality ID feature primarily consists of the following components: 1) a unique encrypted code in the GBIC module or SFP module which enables Cisco IOS to identify Cisco-pluggable parts, and 2) the ability of Cisco IOS to enable only those ports populated with Cisco parts. The Cisco Quality ID feature allows customers to have confidence that the GBIC modules or SFP modules being deployed are certified to be compatible with the Cisco network device in which they are being deployed.

Field-Programmable Device Upgrades

Field-programmable devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. A field-programmable gate array (FPGA) is a type of programmable memory device that exists on some cards in Cisco routers. The term “FPD” in general describes any type of programmable hardware device, including FPGAs.

An FPD image package is used to upgrade FPD images. Whenever a Cisco IOS image is released that supports the FPD feature, a companion FPD image package is also released for that Cisco IOS software release. The FPD image package is available from Cisco.com and is accessible from the Cisco Software Center page where you also go to download your Cisco IOS software image.

For information about how to upgrade FPD versions in the Cisco 7200 VXR router on the NPE-G2 Network Processing Engine and the VPN Services Adapter (VSA), including the information that you need to determine whether an FPD upgrade is necessary and how to verify the FPD upgrade process, refer to the feature guide at the following URL:

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

NPE-G2 Support for the show environment Command

The output of the **show environment** command has been modified to support the NPE-G2 network processing engine on the Cisco 7200 VXR in Cisco IOS Release 12.4(4)XD. No other changes to the Cisco IOS software were made. Refer to the *NPE-G2 Support for the show environment Command* feature module at the following URL for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xd4/showenv2.htm

USB Storage and USB Storage PKI Enhancements

Cisco IOS Release 12.4(4)XD supports the following features on the NPE-G2 network processing engine:

- USB Storage— Enables the NPE-G2 to support USB flash modules and USB eTokens.

  USB flash drives allow users to store images and configurations external to the router.

  The NPE-G2 supports smart card technology in a USB key form factor (also known as an Aladdin USB eToken Pro key). USB tokens provide secure configuration distribution and allow users to store Virtual Private Network (VPN) credentials for deployment.
- USB Storage PKI Enhancements—Enhances the USB token PIN security for automatic login, and increases the flexibility of USB token configuration and storage of public key infrastructure (PKI) credentials, such as Rivest, Shamir, and Adelman (RSA) keys on the NPE-G2.

USB Storage

Storing on USB Flash Memory Modules

The NPE-G2 provides two USB ports that can be used with USB Flash memory modules as secondary storage, similar to CompactFlash Disks. The USB Flash memory modules can be used to store Cisco IOS images, data, and configuration files. The Cisco USB Flash memory module is nonsecure, compared to the USB eToken, which is a secure memory module.

Storing on a USB eToken

A USB token is a smart card, containing a microprocessor and memory, with a USB interface. The NPE-G2 uses the USB eToken Pro key by Aladdin Knowledge Systems to securely store up to 32 KB of information, such as a bootstrap configuration or VPN credentials, separate from the router chassis. The USB eToken uses smart card technology to protect a small area of memory and grants access using a personal identification number (PIN). When IP Security (IPSec) VPN credentials are stored on the USB eToken, they are safely external to the router. When the USB eToken is inserted in a USB port, the router can pass the PIN and unlock it, retrieving the credentials and copying them into running memory. When the USB eToken is removed, the router erases the credentials from running memory, ensuring that they cannot be retrieved from the router itself.

One of the feature benefits is that it secures a VPN connection. The router may have access to the Internet at all times. However, the router can only use the VPN when the token is present because the RSA keys on the eToken are used to set up the tunnel, and the tunnel is torn down when the eToken is removed.

For more information on USB Storage and the commands used, refer to the following:

- "NPE-G2 Overview" chapter in the *Network Processing Engine and Network Services Engine Installation and Configuration* guide at:

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

- *USB Storage* feature module, Cisco IOS Release 12.3(14)T, at:

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

- *Cisco IOS Security Configuration Guide, Release 12.4T*, "Part 5: Implementing and Managing a PKI," "Storing PKI Credentials" chapter at:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part20/index.htm

  or the *USB Storage PKI Enhancements* configuration module, Cisco IOS Release 12.4(4)T at:

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

The C7200 VSA supports the following MIBs:

- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB

Limitations and Restrictions

The following limitations and restrictions apply to the Cisco 7200 VXR routers on the NPE-G2 for Cisco IOS Release 12.4(4)XD:

C7200 VSA Limitations and Restrictions

Note Beginning with Cisco IOS Release 12.4(4)XD7, the C7200 VSA and VAM2+ are no longer supported on the Cisco IOS Release12.4XD. Customers who require C7200 VSA or VAM2+ support should migrate to Cisco IOS Release 12.4(15)Tx.

The C7200 VSA has the following restrictions:

- The VSA does not interoperate with other ISA or VAM/VAM2/VAM2+ crypto cards in the same router. The VAM/VAM2/VAM2+ crypto cards are disabled when the VSA is active in the Cisco 7200VXR series routers with the NPE-G2 processor.
- Only a single VSA card is supported on the Cisco 7200VXR series routers with the NPE-G2 processor.

Note Only Cisco 7200VXR series routers with the NPE-G2 processor are supported.

- The VSA module does not support Online Insertion and Removal (OIR).

  The VSA boots only during system initialization. The VSA will not work if it is inserted after the system is up and running. The VSA can be shut down by a disabling CLI command. The VSA is ready for removal after the disabling CLI command is executed.
- No per packet show access-list packet count details for crypto map ACL are displayed when the **show access-list** command is entered.

  Use other counters, such as the output from the **show crypto ipsec sa**, **show crypto engine accelerator statistics 0,** and **show crypto engine conn act** commands, to determine if the VSA is processing the packets.
- VSA does not support IPPCP compression.
- VSA supports a maximum anti-replay window size of 512.

VAM2+ Limitations and Restrictions

Note Beginning with Cisco IOS Release 12.4(4)XD7, the C7200 VSA and VAM2+ are no longer supported on the Cisco IOS Release12.4XD. Customers who require C7200 VSA or VAM2+ support should migrate to Cisco IOS Release 12.4(15)Tx.

The VAM2+ crypto card has the following restriction:

- VAM2+ does not interoperate with other crypto cards, such as ISA, VAM, or VAM2, in a single Cisco 7204VXR or Cisco 7206VXR.

Caveats for Cisco IOS Release 12.4XD

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 the caveats document.

This section contains open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.4(4)T that apply to the Cisco 7000 family of routers are also in Cisco IOS Release 12.4(4)XD.

For information on caveats in Cisco IOS Release 12.4(4)T, see *Caveats for Cisco IOS Release 12.4T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com.

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, l**og in** to Cisco.com and click **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.2 Mainline> Troubleshoot and Alerts > Bug Toolkit**. 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.

Table 22 Caveats Reference for 12.4XD

	Software Release	
	12.4(4)XD	
DDTS Number	**Caveat Resolved**	**Caveat Open**
CSCdy80322	12.4(4)XD8	12.4(4)XD8
CSCea58000	12.4(4)XD6	12.4(4)XD6
CSCec10149	12.4(4)XD11	No
CSCec12299	12.4(4)XD7	12.4(4)XD7
CSCec77703	12.4(4)XD12	
CSCed57504	12.4(4)XD7	12.4(4)XD7
CSCef93594	12.4(4)XD12	
CSCeg87396	12.4(4)XD8	12.4(4)XD8
CSCeh52502	12.4(4)XD3	12.4(4)XD3
CSCej21681	12.4(4)XD3	12.4(4)XD3
CSCej27827	12.4(4)XD10	12.4(4)XD10
CSCej44509	12.4(4)XD7	12.4(4)XD
CSCej83614	12.4(4)XD8	12.4(4)XD8
CSCek26492	12.4(4)XD2	12.2(4)XD2
CSCek28689	No	12.4(4)XD3

Table 22 Caveats Reference for 12.4XD (Continued)

	Software Release	
	12.4(4)XD	
DDTS Number	Caveat Resolved	Caveat Open
CSCek34097	12.4(4)XD11	No
CSCek40085	12.4(4)XD2	12.4(4)XD
CSCek42751	12.4(4)XD11	No
CSCek43101	12.4(4)XD2	12.4(4)XD1
CSCek43732	12.4(4)XD8	12.4(4)XD8
CSCek44895	No	12.4(4)XD2
CSCek46234	12.4(4)XD11	No
CSCek48252	No	12.4(4)XD3
CSCek50177	12.4(4)XD8	12.4(4)XD8
CSCek50994	No	12.4(4)XD3
CSCek51696	No	12.4(4)XD3
CSCek51702	12.4(4)XD5	12.2(4)XD5
CSCek52673	12.4(4)XD11	No
CSCek53837	No	12.4(4)XD3
CSCek53865	No	12.4(4)XD3
CSCek53980	No	12.4(4)XD3
CSCek54071	No	12.4(4)XD3
CSCek54073	No	12.4(4)XD3
CSCek54331	No	12.4(4)XD3
CSCek55486	12.4(4)XD7	12.4(4)XD7
CSCek56991	12.4(4)XD4	12.4(4)XD3
CSCek58542	12.4(4)XD8	12.4(4)XD8
CSCek61276	12.4(4)XD8	12.4(4)XD8
CSCek68014	12.4(4)XD6	12.4(4)XD6
CSCek71805	12.4(4)XD8	12.4(4)XD8
CSCek73386	12.4(4)XD8	12.4(4)XD8
CSCek75633	12.4(4)XD8	12.4(4)XD8
CSCek75931	12.4(4)XD11	No
CSCek76933	No	12.4(4)XD8
CSCek77866	No	12.4(4)XD8
CSCir00018	12.4(4)XD5	12.4(4)XD5
CSCin78805	12.4(4)XD12	
CSCsa55031	12.4(4)XD11	No
CSCsa86801	12.4(4)XD12	

Table 22 Caveats Reference for 12.4XD (Continued)

	Software Release	
	12.4(4)XD	
DDTS Number	Caveat Resolved	Caveat Open
CSCsb08386	12.4(4)XD10	12.4(4)XD10
CSCsb15164	12.4(4)XD11	No
CSCsb25337	12.4(4)XD2	12.4(4)XD2
CSCsb40304	12.4(4)XD5	12.4(4)XD5
CSCsb42470	12.4(4)XD3	12.4(4)XD3
CSCsb52717	12.4(4)XD3	12.4(4)XD3
CSCsb55483	12.4(4)XD4	12.4(4)XD4
CSCsb58590	12.4(4)XD3	12.4(4)XD3
CSCsb78345	12.4(4)XD10	12.4(4)XD10
CSCsb82123	12.4(4)XD4	12.4(4)XD4
CSCsb93407	12.4(4)XD3	12.4(4)XD3
CSCsc22696	No	12.4(4)XD3
CSCsc64217	12.4(4)XD10	12.4(4)XD10
CSCsc70114	12.4(4)XD11	No
CSCsc72722	No	12.4(4)XD3
CSCsc77704	12.4(4)XD12	
CSCsc86307	12.4(4)XD11	No
CSCsc97727	12.4(4)XD10	12.4(4)XD10
CSCsc98725	12.4(4)XD3	12.4(4)XD3
CSCsd13899	No	12.4(4)XD3
CSCsd24183	12.4(4)XD7	12.4(4)XD7
CSCsd24814	No	12.4(4)XD1
CSCsd28214	12.4(4)XD8	12.4(4)XD8
CSCsd38693	No	12.4(4)XD8
CSCsd39684	No	12.4(4)XD1
CSCsd42053	12.4(4)XD8	12.4(4)XD8
CSCsd42073	No	12.4(4)XD
CSCsd44501	12.4(4)XD3	12.4(4)XD2
CSCsd53289	No	12.4(4)XD1
CSCsd58381	12.2(4)XD2	12.2(4)XD2
CSCsd59381	12.4(4)XD12	
CSCsd62214	No	12.4(4)XD1
CSCsd75854	12.4(4)XD8	12.4(4)XD8
CSCsd89790	No	12.4(4)XD2

Table 22 Caveats Reference for 12.4XD (Continued)

	Software Release	
	12.4(4)XD	
DDTS Number	Caveat Resolved	Caveat Open
CSCsd91454	12.4(4)XD5	12.4(4)XD5
CSCsd92405	12.4(4)XD5	12.4(4)XD5
CSCse05642	12.4(4)XD4	12.4(4)XD4
CSCse07013	No	12.4(4)XD3
CSCse09256	No	12.4(4)XD5/12.4(4)XD6
CSCse17976	No	12.4(4)XD2
CSCse18854	No	12.4(4)XD2
CSCse19109	No	12.4(4)XD2
CSCse23502	No	12.4(4)XD3
CSCse24889	12.4(4)XD8	12.4(4)XD8
CSCse51820	12.4(4)XD3	12.4(4)XD3
CSCse53002	12.4(4)XD3	12.4(4)XD3
CSCse56501	12.4(4)XD7	12.4(4)XD7
CSCse56800	12.4(4)XD10	No
CSCse58419	12.4(4)XD8	12.4(4)XD8
CSCse66625	12.4(4)XD6	12.4(4)XD6
CSCse68138	12.4(4)XD4	12.4(4)XD4
CSCse69102	12.4(4)XD3	12.4(4)XD3
CSCse73065	No	12.4(4)XD3
CSCse79443	No	12.4(4)XD1
CSCse81609	No	12.4(4)XD2
CSCse85068	No	12.4(4)XD2
CSCse85329	12.4(4)XD8	12.4(4)XD8
CSCse93621	12.4(4)XD11	No
CSCsf04754	12.4(4)XD3	12.4(4)XD3
CSCsf05474	No	12.4(4)XD3
CSCsf05718	No	12.4(4)XD3
CSCsf06323	12.4(4)XD3	12.4(4)XD3
CSCsf12577	No	12.4(4)XD3
CSCsf16469	No	12.4(4)XD8
CSCsf25106	12.4(4)XD4	12.4(4)XD4
CSCsf28840	12.4(4)XD5	12.4(4)XD5
CSCsf32623	12.4(4)XD4	12.4(4)XD4
CSCsf33015	12.4(4)XD5	12.4(4)XD3

Table 22 Caveats Reference for 12.4XD (Continued)

	Software Release	
	12.4(4)XD	
DDTS Number	Caveat Resolved	Caveat Open
CSCsf97252	No	12.4(4)XD3
CSCsg00102	12.4(4)XD11	No
CSCsg01964	12.4(4)XD4	12.4(4)XD3
CSCsg05375	12.4(4)XD4	12.4(4)XD4
CSCsg06794	No	12.4(4)XD4
CSCsg11150	No	12.4(4)XD5/12.4(4)XD6
CSCsg16186	12.4(4)XD5	12.4(4)XD4
CSCsg16908	12.4(4)XD4	12.4(4)XD4
CSCsg18075	12.4(4)XD5	12.4(4)XD5
CSCsg23462	12.4(4)XD5	12.4(4)XD5
CSCsg31742	12.4(4)XD4	12.4(4)XD4
CSCsg38143	No	12.4(4)XD4
CSCsg40482	12.4(4)XD7	12.4(4)XD7
CSCsg43916	12.4(4)XD9	12.4(4)XD8
CSCsg48725	12.4(4)XD8	12.4(4)XD8
CSCsg51538	12.4(4)XD7	12.4(4)XD7
CSCsg55591	12.4(4)XD8	12.4(4)XD8
CSCsg58391	12.4(4)XD8	12.4(4)XD8
CSCsg59037	12.4(4)XD8	12.4(4)XD8
CSCsg65169	12.4(4)XD11	No
CSCsg69458	12.4(4)XD7	12.4(4)XD7
CSCsg76715	12.4(4)XD7	12.4(4)XD7
CSCsg81961	12.4(4)XD8	12.4(4)XD8
CSCsg84732	12.4(4)XD8	12.4(4)XD8
CSCsg86048	12.4(4)XD6	12.4(4)XD5
CSCsg89647	12.4(4)XD6	12.4(4)XD5
CSCsg91306	12.4(4)XD10	No
CSCsg92743	12.4(4)XD8	12.4(4)XD8
CSCsg95813	12.4(4)XD7	12.4(4)XD7
CSCsh02315	12.4(4)XD8	12.4(4)XD8
CSCsh30855	12.4(4)XD7	12.4(4)XD7
CSCsh30863	12.4(4)XD8	12.4(4)XD8
CSCsh48919	12.4(4)XD11	No
CSCsh70906	12.4(4)XD8	12.4(4)XD8

Table 22 Caveats Reference for 12.4XD (Continued)

	Software Release	
	12.4(4)XD	
DDTS Number	Caveat Resolved	Caveat Open
CSCsh71247	12.4(4)XD8	12.4(4)XD8
CSCsh89164	12.4(4)XD12	
CSCsh90413	12.4(4)XD7	12.4(4)XD7
CSCsi09530	12.4(4)XD8	12.4(4)XD8
CSCsi13344	12.4(4)XD12	
CSCsi15195	12.4(4)XD7	12.4(4)XD7
CSCsi17113	No	12.4(4)XD7
CSCsi20225	12.4(4)XD8	12.4(4)XD8
CSCsi25540	No	12.4(4)XD7
CSCsi27015	No	12.4(4)XD8
CSCsi32334	No	12.4(4)XD8
CSCsi53716	12.4(4)XD8	12.4(4)XD8
CSCsi53827	12.4(4)XD10	12.4(4)XD8
CSCsi54780	12.4(4)XD8	12.4(4)XD8
CSCsi56413	12.4(4)XD10	12.4(4)XD10
CSCsi58461	12.4(4)XD12	
CSCsi62406	12.4(4)XD9	12.4(4)XD8
CSCsi68543	12.4(4)XD12	
CSCsi78118	12.4(4)XD8	12.4(4)XD8
CSCsi82427	12.4(4)XD8	12.4(4)XD8
CSCsi90974	12.4(4)XD11	No
CSCsi96149	12.4(4)XD8	12.4(4)XD8
CSCsi98120	12.4(4)XD9	12.4(4)XD9
CSCsi99217	12.4(4)XD8	12.4(4)XD8
CSCsj07936	12.4(4)XD8	12.4(4)XD8
CSCsj13380	12.4(4)XD8	12.4(4)XD8
CSCsj17304	No	12.4(4)XD8
CSCsj25395	12.4(4)XD9	12.4(4)XD9
CSCsj27963	12.4(4)XD11	No
CSCsj52491	No	12.4(4)XD8
CSCsj68052	12.4(4)XD9	12.4(4)XD9
CSCsj85065	12.4(4)XD11	No
CSCsj99980	12.4(4)XD10	12.4(4)XD10
CSCsk02368	No	12.4(4)XD8

Table 22 Caveats Reference for 12.4XD (Continued)

	Software Release	
	12.4(4)XD	
DDTS Number	Caveat Resolved	Caveat Open
CSCsk04350	12.4(4)XD11	No
CSCsk09735	12.4(4)XD11	No
CSCsk19565	12.4(4)XD11	No
CSCsk23972	12.4(4)XD11	No
CSCsk25697	12.4(4)XD11	No
CSCsk32150	12.4(4)XD10	12.4(4)XD10
CSCsk40413	12.4(4)XD9	12.4(4)XD9
CSCsk62253	12.4(4)XD11	
CSCsk65796	12.4(4)XD9	12.4(4)XD9
CSCsk66240	12.4(4)XD11	No
CSCsk73104	12.4(4)XD10	12.4(4)XD10
CSCsk88637	12.4(4)XD10	12.4(4)XD10
CSCsl34280	12.4(4)XD10	12.4(4)XD10
CSCsl34481	12.4(4)XD11	No
CSCsl47915	12.4(4)XD11	No
CSCsl59294	12.4(4)XD11	No
CSCsl62609	12.4(4)XD11	No
CSCsl69445	12.4(4)XD11	No
CSCsl96254	12.4(4)XD11	No
CSCsm34361	12.4(4)XD11	No
CSCsm61105	12.4(4)XD11	No
CSCsm66688	12.4(4)XD11	No
CSCsm77199	12.4(4)XD11	No
CSCso21611	12.4(4)XD11	No
CSCso97927	12.4(4)XD12	
CSCsq13348	12.4(4)XD11	No
CSCsq44013	12.4(4)XD11	No
CSCsq50944	12.4(4)XD12	
CSCsq62976	12.4(4)XD11	No
CSCsq88866	12.4(4)XD12	
CSCsr08094	12.4(4)XD12	
CSCsr15607	12.4(4)XD11	No
CSCsr27960	12.4(4)XD12	
CSCsr53390	12.4(4)XD12	

Table 22 Caveats Reference for 12.4XD (Continued)

	Software Release	
	12.4(4)XD	
DDTS Number	Caveat Resolved	Caveat Open
CSCsr70035	12.4(4)XD11	No
CSCsr73973	12.4(4)XD12	
CSCsr74835	12.4(4)XD12	
CSCsr97753	12.4(4)XD11	No
CSCsu35475	12.4(4)XD12	
CSCsu47128	12.4(4)XD12	
CSCsu97934	12.4(4)XD12	
CSCsv04836	12.4(4)XD12	
CSCsv67618	12.4(4)XD12	
CSCsv75974	12.4(4)XD12	
CSCsv91602	12.4(4)XD12	
CSCsx44223	12.4(4)XD12	

Open Caveats—Cisco IOS Release 12.4(4)XD12

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD12 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new open caveats for Cisco IOS Release 12.4(4)XD12.

Resolved Caveats—Cisco IOS Release 12.4(4)XD12

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD12. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec77703

  Disk corruption in the router.

  This condition is observed when simultaneously multiple disk operations are performed. These operations can be:

  - Two vty sessions as a result of CLI commands
  - A router application and a SNMP application accessing the disk
  - Two different router applications accessing a disk.

  Workaround: There is no known workaround. Use **fsck** command to fix the corruption.

- CSCef93594

  A Cisco router acting as a L2TP Network Server (LNS) may transmit all LCP packets with the L2TP priority bit set. This may cause negotiation failures or data loss at the end of a PPP session.

This condition is observed when the LNS sets the Priority bit for all the LCP packets using l2tp_fixup_l2tp_header. The Priority bit should only be set if the packet has been marked as PAK_PRIORITY_CRUCIAL.

Workaround: There is no known workaround.

- CSCin78805

  The VCs are made INACTIVE.

  This condition is observed when the Auto VC is configured as part of range on point-to-point sub-interface.

  Workaround: There is no known workaround.

- CSCsa86801

  Alignment errors or a crash may occur while changing route-map configuration.

  This condition is observed when the route-map command is configured in the global configurations mode resulting in traceback messages.

  Workaround: There is no known workaround.

- CSCsc77704

  A Cisco router may become inaccessible via console or telnet. Router must be reloaded to recover.

  Workaround: There is no known workaround.

- CSCsd59381

  Accessing the secondary disk or disk2 device by IOS results in the following error message:

  ```
  %Error opening disk2:/ (No such device)
  ```

  This condition is observed on c7200 platform with an NPE-G2 processor card that is running an IOS image with the fix for CSCec77703.

  Workaround: There is no known workaround.

- CSCsh89164

  ARP table is accessed at interrupt level which is forbidden resulting in an error message on the console.

  This condition is observed when **shutdown** and **no shutdown** command is issued on serial interface with lapb encapsulation.

  Workaround: There is no known workaround.

- CSCsi58461

  A router may crash in an IOS boot helper image during system bootup.

  This condition is observed when the router with a dedicated PPP connection (a leased line) to another active system is loading and booting up its regular image.

  The router must be configured to autoboot with a "boot helper" image. Additionally, the system must have an active serial line, configured for PPP encapsulation, with Multilink enabled. The Multilink connected to a remote system that actively attempts to negotiate PPP (with Multilink) while the local router is booting. This issue has only been observed on a 7200VXR NPE-G2 system (the "c7200p" series of routers)

  Workaround: You can use one of the following two methods:

  – Deactivate the serial connection to router while the bootup is performed.

  - Delete the **boot bootldr** command from the configuration if there is no some special requirement to use custom boot helper image. This will allow the router boot using its default boot image (the image contained in its boot ROM) and avoid this issue.

- CSCsi68543

  If TLS is deconfigured and reactivated, the corresponding ethernet interface fails to set to promiscuous mode.

  This condition is observed when an originally configured TLS is deconfigured and reactivated.

  Workaround: Do not disable the TLS once it is enabled.

- CSCso97927

  The performance of Cisco 7200 router is affected during OIR operation due to high CPU utilization.

  This condition is observed when OIR operation is performed on Cisco 7200 router.

  Workaround: There is no known workaround.

- CSCsq50944

  Traceback message is displayed when a user enters a password greater than the max limit while performing filesystem operations.

  This condition is observed when a password of more than 16 characters long is entered due to incorrect handling of password field.

  Workaround: There is no known workaround.

- CSCsq88866

  Following a crash, the Cisco 7200 router prints junk on the console. Power cycle is required to reboot the router to working state.

  This condition is observed on NPE-G2 if the crash occurs while console logging enabled.

  Workaround: Disable console logging.

- CSCsr08094

  The L2TP control packets that should be dropped as "udp checksum error" are dropped with some other reason. The VPDN process is ignoring udp checksum configuration of the L2TP control packet.

  This condition is observed when L2TP control packets are configured using **vpdn ip udp ignore checksum** command.

  Workaround: There is no known workaround.

- CSCsr27960

  Traceback messages is displayed while configuring the credentials CLI.

  This condition is observed when the user configures a username with more than 32 characters in the credentials CLI.

  Workaround: There is no known workaround.

- CSCsr53390

  The onboard Gigabit ethernet ports on the NPE-G2, with flow control enabled, fails to send pause frames on experiencing a resource problem. However, the ethernet ports continue to receive pause frames and function accordingly.

  This condition is observed when flow control is enabled on the NPE-G2 Gigabit ethernet ports.

  Workaround: There is no known workaround.

- CSCsr73973

  The output of Show controller gig0/<x> command returns negative value in the tx_end_count counter.

  This condition is observed in Native gig ports in Cisco 7200 router with NPE-G2 processor due to continuous traffic flow.

  Workaround: There is no known workaround.

- CSCsr74835

  Potential overflow of the destination buffer due to unspecified bounding length.

  Workaround: There is no known workaround.

- CSCsu35475

  The output queue of a gigabit interface on a NPE-G1 hangs after removing a two level policy-map.

  This condition is observed on a NPE-G1 after removing a two level service policy where the first level was shaping the traffic and at the second level it had LLQ and CBWFQ.

  Workaround: Perform shut/no shut operation on the physical interface using **shutdown** and **no shutdown** command to solve this issue.

- CSCsu47128

  The following error message appears repeatedly in the logs:

  %SYS-2-INTSCHED: 'idle' at level 4 -Process= "Virtual Exec"

  This condition is observed when a user run **reload** command in IOS.

  Workaround: There is no known workaround.

- CSCsu97934

  The NPE-G1 is crashing after pppoe_sss_holdq_enqueue function.

  Workaround: Enter the **deb pppoe error** command to solve this issue.

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website 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-20090908-tcp24.shtml.

- CSCsv67618

  The **sh ip bgp vpnv4 all** command does not show all the routes in routing table.

  This condition is observed on c7200 with 12.4(15)T8.fc2 image.

  Workaround: There is no known workaround.

- CSCsv75974

  The show atm int atm command does not show increments in out drop when packets are dropped due to traffic shaping.

  This condition is observed due to high traffic rate on an ATM interface with traffic shaping enabled.

  Workaround: There is no known workaround.

- CSCsv91602

  Cisco 7201 router with Gi0/3 experiences communication failure.

  Workaround: Perform a shut/no shut operation on the Gi0/3 using **shutdown** and **no shutdown** command. This may solve the problem.

- CSCsx44223

  Packet loss occurs due to IP checksum error if MPF supported image is used.

  This condition is observed if a lot of IPv6 Multicast Packets are received and MPF supported image is in use.

  Workaround: Use non MPF supported image.

Open Caveats—Cisco IOS Release 12.4(4)XD11

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD11 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new open caveats for Cisco IOS Release 12.4(4)XD11.

Resolved Caveats—Cisco IOS Release 12.4(4)XD11

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD11. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec10149

  Router crashes on executing **delete /recursive** command.

  This condition is observed when multiple sub-directories exist with same name recursively.

  Workaround: Perform **del** or **dir** command on individual directories.

- CSCek34097

  The router displays CPUHOG errors and/or reloads on executing **no ipv6 multicast-routing** global configuration command.

  This condition is observed in router with configurations that include large numbers of dot1q subinterfaces.

  Workaround: There is no known workaround.

- CSCek42751

  The running configuration on a router becomes inaccessible when a small file is copied to it.

  This condition is observed on a Cisco router that has an ATA file system after you reboot the router.

  Workaround: Reboot the router again.

- CSCek46234

Deconfiguring a member interface from a multilink bundle and adding it to another multilink bundle results in continuos error message.

Workaround: There is no known workaround.

- CSCek52673

  A single UDP packet sent to port 67 caused the router to reload.

  This condition is observed when a router that has DHCP server enabled receives a malformed UDP packet.

  Workaround: There is no known workaround.

- CSCek75931

  The router may experience CPUHOG condition.

  This condition is observed when more than 2000 sessions are established on the router.

  Workaround: There is no known workaround.

- CSCsa55031

  The router shows high CPU utilization resulting in impact on router performance.

  This condition is observed when Turbo ACL is enabled resulting in repeated Turbo ACL compilations.

  Workaround: There is no known workaround.

- CSCsb15164

  The router permits unauthorized packets even when these packets are denied in the standard Access List.

  This condition is observed when the order of ACL entries for permitting and denying packets are reordered. As a result, the permit entry may be placed above the deny entry.

  Workaround: Use extended ACLs.

- CSCsc70114

  Router crashes when NAT entries time out.

  This condition is observed on routers running 12.4(3) configured with VRF and NAT using route-map.

  Workaround: There is no known workaround.

- CSCsc86307

  The router crashes due to bus error.

  This condition is observed on executing **show interface** command.

  Workaround: There is no known workaround.

- CSCse93621

  ISDN B-channel is not brought to in-service state after sending restart acknowledgement (RESTART ACK).

  Workaround: Use BCAC feature to bring channel service state in sync with peer.

- CSCsg65169

  The router gives data path error.

  The reason for this condition is not known.

  Workaround: There is no known workaround.

- CSCsh48919

  A router with an ATA flash card failed when the **dir disk_name0:** command was executed.

  This condition is observed when the router has a removable flash card (such as an ATA flash car or CF card) that is formatted to use DOSFS and the file or directory name stored on disk contains embedded spaces.

  Workaround: Remove or rename all files and directories having names with embedded spaces.

- CSCsi90974

  MPF drops all traffic for a particular client on the network while the traffic for other clients remains consistent.

  This condition is observed due to incorrect MPF RPF and adjancency entries.

  Workaround: You can implement the following workarounds:

  - Unload/reload MPF software module.
  - Reboot the system
  - Execute **clear adjacency** command to purge old MPF adjacencies and reinstall the current existing ones.

- CSCsj27963

  A router running Cisco IOS may show the following error when performing a "write memory" operation:

  ```
  %SYS-4-NV_BLOCK_INITFAIL: Unable to initialize the geometry of nvram
  ```

  This condition is observed when the size of configuration is greater than the size of NVRAM.

  Workaround: You can implement one of the following workarounds:

  - Use **service compress-config** command to compress the configuration before 'write memory' operation.
  - Erase the nvram, unconfigure configurations to fit them into nvram, and issue write memory operation. Repeat these steps until this error is resolved.
  - Save the configuration to another file system other than nvram.
  - If the router is reloaded, use write erase command to reinitialise nvram and allow write memory operation.

- CSCsj85065

  The router crashes while processing an SSL packet.

  This condition is observed during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

  Workaround: Cisco has released free software updates that address this vulnerability. Apart from disabling affected services, there are no available workaround to resolve problem.

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

- CSCsk04350

  The router takes too many CPU cycles to print the syslog messages to the system console.

  This condition is observed when burst L2TP LNS session authentication fails and the **vpdn logging** global configuration is enabled.

Workaround: Disable system console logging using the **no logging console** global configuration command.

- CSCsk09735

  A router crashes when the **mkdir .../.../** *EXEC* command is executed, followed by **reload** *EXEC* and **show file system** *EXEC* command.

  This condition is observed on a router that runs Cisco IOS software using a storage device that is formatted with the DOS file system.

  Workaround: Avoid creating a subdirectory with "." characters.

- CSCsk19565

  The **ipv6 traffic-filter** command may not work on multiple subinterfaces on a router.

  This condition is observer when **ipv6 traffic-filter** command is used to deny multicast packets out of multiple subinterfaces under the same physical interface.

  Workaround: Disable and re-enable ipv6 cef.

- CSCsk23972

  A router running an IOS image may stop accepting incoming TELNET connections.

  This condition is observed when 20 or more VRFs are configured on a router and each VRF has incoming TCP connection requests arriving at the host for non-existing services from different VRFs.

  Workaround: Follow the following steps to resolve this problem:

  – Use **show tcp brief all** command to view TCB that have local and foreign addresses as "*.*", and

  – Clear those entries using the **clear tcp tcb** *address of the TCB* command.

- CSCsk25697

  A router with DNS server configured may show CPUHOG tracebacks when it receives repeated crafted UDP packets to its port 53.

  This condition is observed when DNS server is not configured on the router to listen to UDP port 53.

  Workaround: Apply rate limit to port 53 to interfaces facing untrusted networks using the following commands:

```
access-list 100 permit udp any any eq domain
access-list 100 deny   ip any any
interface GigabitEthernet0/0
 ip address 10.2.2.2 255.255.255.0
 rate-limit input access-group 100 8000 1500 2000 conform-action transmit
exceed-action drop
```

- CSCsk62253

  Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

  1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
  2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

  Cisco has released free software updates that address these vulnerabilities. There is no known workaround that mitigate these vulnerabilities. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml

- CSCsk66240

  An error message is received on the ingress PE. Sample message:

  ```
  *Mar 10 23:48:12.395: %BGP-3-INVALID_MPLS: Invalid MPLS label (3)
              received in update for prefix 1:1:10.254.5.0/24 from 10.100.1.5
  *Mar 10 23:48:51.743: %BGP-3-INVALID_MPLS:  Invalid MPLS label (3)
              received in update for prefix 1:1:10.254.2.1/32 from 10.100.1.5
  ```

  This condition is observed with the following network configuration:

  - A CE (CE1) is connected to an ingress PE (PE1), and
  - The ingress PE is connected to a router reflector, and
  - The router reflector is connected to other two (egress) PEs (PE2a and PE2b), and
  - Both the egresses PEs are connected to the same CE (CE2).

  When the link flaps between one of these two PEs and the CE (CE2) the error message is generated.
  Workaround: There is no known workaround.

- CSCsl34481

  Router crashes due to IPv6 multicast routing.

  This condition is observed on applying/removing multicast routing configurations.

  Workaround: There is no known workaround.

- CSCsl47915

  Redistribution from OSPF into RIP using a route map based on a prefix list may not work for some routes. The **show ip route** *network* command shows that a network is not advertised by RIP.

  This condition is observed when the prefix list is changed. The RIP database is not updated with the new network that was added to the prefix list.

  Workaround: Issue the **clear ip route** *network* command.

- CSCsl59294

  A Cisco router may see the following error shortly after bootup:

  ```
  *Nov 21 15:16:28 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error,  -PC=
  0x416DE178 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE178
  0x416DE650 0x423E303C 0x423E3020 *Nov 21 15:16:28 CDT:
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error,  -PC= 0x416DE188
  -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE188 0x416DE650
  0x423E303C 0x423E3020
  ```

  This condition is observed Cisco router running Cisco IOS Release 12.4(13d).

  Workaround: Use the following commands to disable configuration on the router:

  - **voice hpi capture buffer** *size*
  - **voice hpi capture destination** *filename*

- CSCsl62609

  The Session Initiation Protocol (SIP) implementation in Cisco IOS could be exploited remotely to trigger a memory leak or reload the IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software versions and fixes section contains fixes for all vulnerabilities addressed in this advisory.

  Workaround: There are no known workaround.

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

- CSCsl69445

  The attribute, containedIn, returns zero as value for chassis and module components.

  This condition is observed only on Cisco 7201 routers.

  Workaround: There is no known workaround.

- CSCsl96254

  If an EIGRP distribute-list applied to an interface allows a route, the route will be installed into the routing table without verifying the global distribute-list.

  This condition is observed when a router has a running EIGRP with interface distribute lists and a global distribute list.

  Workaround: Apply the global distribute list to each interface distribute list.

- CSCsm34361

  TCP ports may not show open during port scanning using NMAP.

  This condition is observed on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsm61105

  The router crashes due to bus error on removing virtual-template interfaces under ATM.

  This condition is observed when there are approximately 3000 PPPoE and PPPoEoA sessions open and the **no interface virtual-template** *number* command is executed repeatedly under ATM interfaces:

  Workaround: There is no workaround.

- CSCsm66688

  The router crashes due to watchdog timeout or hangs.

  This condition is observed when:

  – The turbo-ACL is enabled. (indicating that **ip access-list compiled** or **ip access-list compiled reuse** commands are enabled)

  – The QoS and/or ACL configuration is modified.

  Workaround: Disable turbo-ACL using either **ip access-list compiled** or **ip access-list compiled reuse** command.

- CSCsm77199

  For a router with HTTP secure server capability, the switch shows the following error message:

  ```
  "%DATACORRUPTION-1-DATAINCONSISTENCY: copy error"
  ```

  This condition is observed when **ip http server** is configured.

  Workaround: Use the **no ip http server** command to disable HTTP server.

- CSCso21611

  The router crashes due to memory allocation issue.

  This conditions is observed on Cisco 7200 routers.

  Workaround: There is no known workaround.

- CSCsq13348

The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

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

Note This vulnerability is not related in any way to CVE-2008-1447 - Cache poisoning attacks. Cisco Systems has published a Cisco Security Advisory for that vulnerability, which can be found at http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml.

- CSCsq44013

  The CPE does not reply to the DNS query from the client for the first attempt, the first response is being dropped.

  This condition is observed on a router running 12.4T IOS image configured with Split DNS.

  Workaround: There is no known workaround.

- CSCsq62976

  The Router may crash when clearing vpdn l2tp tunnels.

  This condition is observed in a 7301 router which is acting as LAC in a multiple LNS env with load balancing.

  Workaround: There is no known workaround.

- CSCsr15607

  The Cisco 7201 router running 12.2(31)SB9/SB12 has the following issues when any MQC QoS is applied to Gig0/3:

  - Unable to send traffic out
  - Output queue gradually fills above maximum
  - The I/O memory is slowly depleted in HQF pool

  This condition is observed on Cisco 7201 routers running 12.2(31)SB9 or 12.2(31)SB12 IOS version.

  Workaround: Use 12.2(33)SRC1 IOS version.

- CSCsr70035

  The $_info_syslog_hist_msg_32 variable returned extraset of caracters, ^Z.

  This condition is observed when

  Workaround: There is no known workaround.

- CSCsr97753

  The router becomes inaccessible via all its subinterfaces on executing **no xconnect** *10.0.0.51 1435* **encapsulation** *mpls* command. In addition, the router looses routing connectivity and LDP connectivity.

  This condition is observed when xconnect is unconfigured.

  Workaround: Perform shutdown and no shutdown operation using **shut** and **no shut** commands.

Open Caveats—Cisco IOS Release 12.4(4)XD10

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD10 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new open caveats for Cisco IOS Release 12.4(4)XD10.

Resolved Caveats—Cisco IOS Release 12.4(4)XD10

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD10. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCej27827

  When Network Address Translation (NAT) is configured and an access-list is configured later, the router crashes because of insufficient memory allocation.

  This condition does not occur on a router with 512 MB RAM or more.

  There are no known workarounds.

- CSCsb08386

  A router crashes when you enter the **show ip bgp regexp** command.

  This condition occurs on a Cisco router when Border Gateway Protocol (BGP) is being updated.

  Workaround: Enable the new deterministic regular expression engine by entering the **bgp regexp deterministic** command and then enter the **show ip regexp** command. Note that enabling the new deterministic regular expression engine may impact the performance speed of the router.

- CSCsb78345

  A software-forced crash occurs when you execute the **show ipv6 cef** command after an OSPFv3 cost change is made to a GE link.

  Workaround: Use the s**how mls cef ipv6** command, or wait 60 seconds after making the cost change before entering the **show ipv6 cef** command.

- CSCsc64217

  A Cisco router with **ip inspect sip** configured crashes after experiencing excessive CPU usage and an eventual Watchdog Timeout in the Inspect Timer process.

  This condition is platform and software independent.

  Workaround: Disable **ip inspect sip**.

- CSCsc97727

  An access point may crash when you add or remove Terminal Access Controller Access Control System (TACACS) servers using the CLI.

  This condition is observed on a Cisco router that has the **aaa accounting commands** *level* **default** *list-name* **group** *groupname* command enabled.

  Workaround: Disable the **aaa accounting commands** *level* **default** *list-name* **group** *groupname* command.

  Alternate Workaround: Use Remote Authentication Dial-In User Service (RADIUS) instead of TACACS.

- CSCse56800

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed 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, if administrators do not require the Cisco IOS device to provide voice over IP services.

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

- CSCsg91306

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed 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, if administrators do not require the Cisco IOS device to provide voice over IP services.

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

- CSCsi53827

  A bogus source IP address occurs in replicated packets when using Service Independent Intercept (SII) to do lawful intercept.

  This condition occurs on a Cisco 7200 router with an NPE-G2. Typically, the source IP address matches the loopback address for the router, the IP address, or the interface actually used to connect to network with path to mediation device.

  There are no known workarounds.

- CSCsi56413

  The output may be stuck on a POS interface that is configured for Frame Relay encapsulation. When this situation occurs, the output queue is not emptied, and the Local Management Interface (LMI) remains down.

  This condition occurs on a Cisco router that runs Cisco IOS Release 12.4(12) or later, and occurs only with very specific hardware configurations including an NPE-G1 and PA-POS-OC3SMI. The issue has been observed when the PA-POS-OC3SMI is located in slot 4 and has not been seen with other hardware configurations.

  Workaround: Place the POS PA in one of the other slot(s). PA location reconfiguration in chassis should fix the problem.

- CSCsj99980

  The user is not able to configure Any Transport over MPLS (AToM) Xconnects on interfaces that use PA-POS-1OC3 cards. The following error message is displayed:

  ```
  MPLS encap is not supported on this circuit
  ```
  There are no known workarounds.

- CSCsk32150

  A Cisco 7200 series router running c7200-advipservicesk9_mpf-mz.124-4.XD8 with configuration for virtual private dialup network (VPDN) and virtual template may produce the following log message with additional tracebacks:

  ```
  %FF-4-MSGAWOL: mp_send_msg(module) at IPL-0
  ```

  There are no known workarounds.

- 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

- CSCsk88637

  Operation, Administration, and Maintenance (OAM) cells are not generated when a new Asynchronous Transfer Mode (ATM) subinterface and permanent virtual circuit (PVC) are configured.

  To diagnose this problem, check the subinterface and PVC status and enable the debug **atm oam interface atmx/x.xxx** command. Although the subinterface shows as up/up, the PVC is down, and no debug output is seen.

  This condition occurs in various Cisco IOS 12.4 images.

  Workaround: Perform the **shut/no shut** commands on the ATM subinterface.

- CSCsl34280

  Excessive TX underruns are observed on GigabitEthernet Interfaces 0/1 and 0/2 of a Cisco 7301 router causing substantial packet loss. A symptom of this problem is an increasing number of CRC errors reported by the GigabitEthernet interfaces of a switch connecting the respective interfaces of the Cisco 7301 router.

  This condition occurs when the router is configured as an L2TP network server (LNS) and runs Cisco IOS release 12.4(4)XD6. The GigabitEthernet Interface 0/0 used to terminate the Layer 2 Tunneling Protocol (L2TP) tunnels is not affected by the TX underruns.

  Workaround: There are no known workarounds.

  Further Information: A trigger for this issue is not known currently. There are also Cisco 7301 routers having the same configuration and similar load as well as the same IOS release, which are not impacted. Although currently only Cisco 7301 routers are impacted by this issue, other platforms with other Cisco IOS releases may be impacted as well.

Open Caveats—Cisco IOS Release 12.4(4)XD9

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD9 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new open caveats for Cisco IOS Release 12.4(4)XD9.

Resolved Caveats—Cisco IOS Release 12.4(4)XD9

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD9. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsg43916

  When configuring Xconnect on the PA-MC-E3 and PA-MC-T3 port adapters on a Cisco 7200 (NPEG1) router, the following error occurs:

  ```
  MPLS encap is not supported on this circuit error
  ```

  There are no known workarounds.

- CSCsi62406

  An NPE-G2 AUX port may encounter line resets and traceback errors every 10 minutes. This condition occurs when the following command is configured under the AYX port: **modem InOut**.

  There are no known workarounds.

- CSCsi98120

  A router crashes because of a bus error. Spurious accesses might also be observed.

  This condition occurs on a Cisco 7200 series router that has an NPE-G1. The router is configured as a Provider Edge (PE) router and uses Modular QoS CLI (MQC) hierarchical policies for some subinterfaces and the legacy **rate-limit** command for other subinterfaces.

  There are no known workarounds.

- CSCsj25395

  If you remove the Dialer interface configuration when Internet Protocol Header Compression (IPHC) is configured on the interface, the Cisco 7200 platform crashes.

  Workaround: Remove any IIPHC commands from the Dialer interface before you delete the Dialer interface from the configuration.

- CSCsj68052

  A platform crash occurs when either the **no frame-relay ip rtp header-compression** command or the **no frame-relay map ip** *ipadd dlci* command is entered.

  This condition occurs when there is more than one IP map configured for the same data-link connection identifier (DLCI) and IP header compression is configured.

  There are no known workarounds other than to not configure more than one IP map on the same DLCI at the same time as IP header compression.

- CSCsk40413

  The **control-plane** command does not work for some feature sets of the Cisco IOS Release 12.4(4)XD train.

  This condition occurs when Cisco7201/12.4(4)XD7/IPBASE feature sets are used, and the customer tries to set control plane policing (CoPP). This condition can also occur on devices equipped with the NPE-G2.

  Workaround: Use either of following feature sets for the Cisco IOS Release 12.4(4)XD train, ADVSECURITYK9, ADVIPSERVICESK9, or ADVENTERPRISEK9, or, use another train (such as, the Cisco IOS Release 12.4(15)T train.)

- CSCsk65796

  All frames received on a Gigabit Ethernet interface are dropped. All drops are reported as overruns in the output of **show interfaces** and **show controllers** commands.

  This condition occurs on Gigabit Ethernet interfaces on the NPE-G2 network processor of Cisco 7200 series routers. All IOS trains that support NPE-G2 are affected. The symptom occurs only when the Gigabit Ethernet controller is in promiscuous mode with a moderate traffic rate. The line protocol on the interface remains up when the error condition is present.

  Workaround: There are no known workarounds. When the Gigabit Ethernet controller falls into this condition, the only way to recover is to power-cycle the router as a soft reload will not clear the problem.

  Further Problem Description: The Gigabit Ethernet controller can go into promiscuous mode under the following two conditions:

  - When bridging is configured on the interface.
  - When the number of MAC addresses that have to be stored in the MAC address filter table exceed the capacity of the table. This situation can happen when a large number of Hot Standby Router Protocol (HSRP) groups are configured, or a large number of IP multicast groups are to be received on the interface.

Open Caveats—Cisco IOS Release 12.4(4)XD8

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD8 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek76933

  The router might crash when you configure an Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) for an ATM subinterface which is already configured with a bundle.

  Workaround: Use the ATM Multipoint subinterface.

- CSCek77866

  The second B channel of a Basic Rate Interface (BRI) fails to come UP when load sharing is enabled between B1 and B2. Traffic continues to pass, but B1 forwards all the traffic.

  This conditions occurs on the NPE-G2 processor only.

  There are no known workarounds.

- CSCsd38693

  Renaming a file to a string that contains multiple trailing dots ("." characters) corrupts the file system on Analog Telephone Adaptor (ATA), Compact Flash (CF), and Universal Serial Bus (USB) flash storage devices.

  This condition occurs when you enter the following commands to rename the file: **rename disk0:file2 disk0:file3...**

  Workaround: Avoid renaming a file that contains multiple trailing "." characters. After the condition has occurred, and the file system is no longer accessible, you must reformat the disk by entering the **format disk0:** command.

- CSCsf16469

  When executing a scalability test case for a dynamic crypto map for 2000 tunnels, tracebacks appear on the responder after applying the crypto map.

  There are no known workarounds.

- CSCsg43916

  When configuring Xconnect on the PA-MC-E3 and PA-MC-T3 port adapters on a Cisco 7200 (NPEG1) router, the following error occurs:

  ```
  MPLS encap is not supported on this circuit error
  ```

  There are no known workarounds.

- CSCsi27015

  If a **show run** or **write memory** command is issued with for an Layer 2 Tunneling Protocol Version 3 (L2TPv3) Ethernet configuration, it takes approximately 6 minutes for the task to complete. During this interval, the router does not respond to any other commands.

  This condition occurs on both the NPE-G2 and the Cisco 7201 router.

  There are no known workarounds.

- CSCsi32334

  `%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (91/62),process = TurboACL` messages appear on an NPE-G1 router running the MPF code for Cisco IOS Release 12.4(4)XD6.

  This condition appears to be related to service-policies on GE interfaces.

  There are no known workarounds.

- CSCsi53827

  A bogus source IP address occurs in replicated packets when using Service Independent Intercept (SII) to do lawful intercept.

  This condition occurs on a Cisco 7200 router with an NPE-G2. Typically, the source IP address matches the loopback address for the router, the IP address, or the interface actually used to connect to network with path to mediation device.

  There are no known workarounds.

- CSCsi62406

  An NPE-G2 AUX port may encounter line resets and traceback errors every 10 minutes. This condition occurs when the following command is configured under the AYX port: **modem InOut**.

  There are no known workarounds.

- CSCsj17304

  A multicast source address may not get translated if the Network Address Translation (NAT) outside interface is a Generic Routing Encapsulation (GRE) tunnel.

  Workarounds: 1. Turn off Cisco Express Forwarding (CEF) globally on the router. 2. Turn off the mroute-cache on the NAT inside interface.

- CSCsj52491

  A memory leak occurs when configuring quality of service (Qos) on a Cisco 7301 router.

  There are no known workarounds.

- CSCsk02368

  Traceback occurs after the interface is shut on a Cisco 7200 router.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(4)XD8

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD8. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy80322

  A CPUHOG error occurs when the **show ipv6 mld group summary** command is executed.

  This condition occurs during IPv6 Multicast when a large number of multicast routing states are present.

  There are no known workarounds.

- CSCeg87396

  A Cisco Router acting as a virtual private dialup network (VPDN) L2TP network server (LNS) or VPDN Multihop node can crash when Layer 2 Tunneling Protocol (L2TP) sessions are being terminated on this node.

  This condition occurs when memory allocation is failing due to memory unavailable, or other errors.

  There are no known workarounds.

- CSCej83614

  Multicast packets are punted to the Route Processor (RP) instead of being fast-dropped.

  This condition occurs on a Cisco router when an access control list is configured on the egress interface to deny all IP packets.

  There are no known workarounds.

- CSCek43732

  All packets are dropped from a 1-port OC-3/STM-1 POS port adapter (PA-POS-1OC3) or 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) that is configured for Class-Based Weighted Fair Queueing (CBWFQ).

  This condition occurs on a Cisco 7200 series router that has an NPE-G1.

  There are no known workarounds.

- CSCek50177

  A large blank space displays in the output of s**how vpn history failure** command.

  This condition occurs when the failure entry is the result of an AAA Authentication failure.

  There are no known workarounds.

- CSCek58542

  Following a cache error exception, a Cisco 7200 NPE-G1 router reloads, self-decompresses the image to boot, crashes again due to a bus error exception, and may eventually hang.

  There are no known workarounds.

- CSCek61276

  When you first disable and then re-enable IPv6 on an interface, IPv6 traffic stops on the Cisco router.

  Workaround: Enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface configuration command on the affected interface.

- CSCek71805

  The following two conditions occur on a Cisco 7200 series router that is configured with an NPE-G2 and a PA-8B-ST port adapter. These conditions do not occur with an NPE-G1:

  Condition 1: A PA-8B-ST port adapter powers down when you boot the router.

  Workaround 1: Perform a software online insertion and removal (OIR) to bring up the port adapter.

  Condition 2: The ISDN layers do not come up.

  Workaround 2: Enter the **debug bri-interface** command to bring up the ISDN layers.

- CSCek73386

  A Cisco 7200 series router running an 12.4XD image crashes if a ESCORT jacket card is present.

  There are no known workarounds.

- CSCek75633

  A router may crash when you attach a virtual circuit (VC) class to an Asynchronous Transfer Mode (ATM) bundle.

  This condition has been observed on a Cisco 7200 series router, but is platform-independent.

  There are no known workarounds.

- CSCsd28214

  A Cisco router may crash because of a watch dog timeout while running the Routing Information Protocol (RIP).

  This condition occurs on a router when an interface changes state at the exact same time that a RIP route that was learned on this interface is being replaced with a better metric redistributed route. For example, when RIP has learned the 192.168.1.0 network from Fast Ethernet 1/0 interface and then RIP learns the 192.168.1.0 network from a redistributed protocol that has a better metric, the RIP route is removed. If, during this interval, the Fast Ethernet 1/0 interface goes down, the router may crash because of a watch dog timeout.

  There are no known workarounds.

- CSCsd42053

  The **show run** command displays the **resource policy** command in the global configuration even though you do not want to configure any resource policy. In addition, the **resource policy** command can not be removed from the configuration.

  There are no known workarounds.

- CSCsd75854

  A router generates a malformed PPPoE Active Discovery Offer (PADO) packet with two 802.1q tags. The first 802.1q tag contains the correct VLAN ID.

  This condition occurs on a Cisco router when the Service-Name field in the PPPoE Active Discovery Initiation (PADI) packet is empty and not equal to the one that is configured on the router.

  Workaround: Ensure that a correct Service-Name field in used in the PADI packet.

- CSCse24889

  Malformed Secure Shell (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.

  This condition occurs 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
  ```

  For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:
  http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a0080716ec2.html

  For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

  http://www.cisco.com/warp/public/707/ssh.shtml

- CSCse58419

  Memory consumption by the Chunk Manager process increases over time.

  This condition can occur when Network Address Translation (NAT) is configured. When NAT Virtual Interface (NVI) with virtual routing/forwarding (VRF) is set in the system, the memory leaks rapidly. When NAT with VRF is set in the system, plus there is embedded address translation needed or Skinny protocol traffic, the memory leaks at a slow pace.

  There are no known workarounds.

- CSCse85329

  When you re-insert a PA-MC-8TE1+ port adapter into the same slot of a Cisco 7200 series router during an online insertion and removal (OIR), the serial interface may enter the Down/Down state. When you enter the **shutdown** command followed by the **no shutdown** command on the T1 or E1 controller, the serial interface may transition to the Up/Down state, still preventing traffic from passing.

  Workaround: Reload the router.

- CSCsg48725

  A Translational Bridging (TLB) exception occurs on a Cisco platform that functions as a Provider Edge (PE) router in an Multiprotocol Label Switching (MPLS) environment. The following error message is generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  This condition occurs on a Cisco platform when Terminal Access Controller Access Control System (TACACS) accounting and authorization is enabled, and the TACACs server is reachable through the global routing table.

  Workaround: Disable Authentication, Authorization, and Accounting (AAA). If disabling AAA is not an option, there are no known workarounds.

- CSCsg55591

  When there are link flaps in the network, various Provider Edge (PE) routers receive the error message:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (1) received in update for prefix
  155:14344:10.150.3.22/32 from 10.2.2.1 OR Local label is not programmed into
  forwarding table for a sourced BGP VPNv4 network
  ```

  This condition occurs when an internal BGP (iBGP) path for a VPNv4 Border Gateway Protocol (BGP) network is present, and then a sourced path for the same route distinguisher (RD) and prefix is brought up afterwards.

  Workarounds: (1) Remove the iBGP path. If the sourced path comes up first, the problem does not occur. (2) Use different RDs with the different PEs. If the RD+ prefix does not exactly match between the iBGP path and the sourced path, the problem does not occur.

- CSCsg58391

  When the **clear interface** command is issued for a Hot Standby Router Protocol (HSRP) router, the the HSRP does not resume.

  There are no known workarounds.

- CSCsg81961

  SYS-3-BADLIST_DESTROY error messages with tracebacks appear on the console relating to File Transfer Protocol (FTP). The router may also crash.

  This condition occurs when the router has **ip inspect** *name* **ftp** configured to an attached ios firewall inspection policy, and FTP traffic is passing through the router.

  Workaround: Disable FTP inspection with the **no ip inspect** *name* **ftp** command. If your clients are on the protected side of the firewall, and you are connecting to servers running active FTP, you can try specifying an access-list to permit source port 20 for certain FTP servers in your inbound security access-list. Note that specifying source port 20 is only an option if your security policy allows this port to be added.

- CSCsg84732

  %IPRT-4-IPROUTING_INT_ERR displays when reverse Telnet is executed on a peer router that is busy.

  There are no known workarounds.

- CSCsg92743

  The router reloads after repeatedly issuing the **show buffers usage** command.

  There are no known workarounds.

- CSCsh02315

  Selective client traffic may be dropped on a Multi-Processor Forwarding (MPF) system or all traffic for one client may be dropped. Traffic for other clients will be fine.

  This condition occurs when an Layer 2 Tunneling Protocol (L2TP) network server (LNS) with MPF functionality is used with an NPE-G1, and access control lists (ACLs) are used on the system.

  Workaround: Unloading/reloading the MPF software module can help. Reboot the system to clear the problem.

- CSCsh30863

  A Cisco 7206VXR (NPE-G1) router crashes during the boot-up process. After the crash, the router has to be reloaded using the **reload** command. Sometimes the router has to be power-cycled, and sometimes the router goes into ROMMON after the crash.

  All of the routers that experienced this crash had PA-POS-OC3SMI and/or PA-A3-OC3SMI installed on them.

  Workaround: Disable malloclite using the global configuration **no memory lite** command. When the router is reloaded the next time, the boot loader image will not use malloclite and the crash can be avoided. Note that disabling malloclite can have a negative impact on the memory utilization of a Cisco IOS device so ample testing of the affects of this change is advised.

  Another possible workaround is to use a bootloader image that does not have malloclite support. Malloclite was introduced into Cisco IOS release 12.3(8)T.

  Further Problem Description The following message can be seen in crashinfo file:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address TLB (store) exception, CPU signal 10.
  ```

- CSCsh70906

  The **debug pppoe events** command displays the wrong VLAN ID.

  This condition occurs when there are a lot of session establish requests of PPP over Ethernet (PPPoE).

  There are no known workarounds.

- CSCsh71247

  Cisco Express Forwarding (CEF) may not function correctly over Point-to-Point (PPP) sessions, and the output of the **show adjacency** command shows information similar to the following:

  ```
  Protocol Interface Address IP Virtual-Access3 point2point(8) (incomplete)
  ```
  This condition occurs on a Cisco router when PPP is used on a full virtual-access interface or multilink bundle.

  Workaround: Disable CEF.

- CSCsi09530

  When the **authenticate register** command is configured under the **voice register global** command, the Communications Manager Express (CME) Session Initiation Protocol (SIP) fails to register.

  This condition occurs when the CME is acting as a registrar.

  Workaround: Disable the **authenticate register** command under the **voice register global** command.

  Further Problem Description: In registrar functionality, CME challenges an inbound register request with a 401 response. If the **authenticate register** command is configured under the **voice register global** command, the Registering Endpoint ends a Register Request with Credentials. As a result, the gateway stack is not processing this request and is dropping it.

- CSCsi20225

  Continuous trace backs are seen on an L2TP network server (LNS) on a Cisco 7201 router when running Cisco IOS Release 12.4(4) XD7. These trace backs occur continuously when bringing up (PPP over Ethernet or PPP over ATM)/Layer 2 Tunneling Protocol (L2TP) sessions over multiple tunnels.

  This issue does not seem to impact the performance.

  There are no known workarounds.

- CSCsi53716

  When a named IPv6 access control list (ACL) is used, the following entries are logged by Cisco IOS:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61BCF2BC reading 0x8
  %ALIGN-3-TRACE: -Traceback= 0x61BCF2BC 0x61BCF6B4 0x61BF0720 0x60A49E84 0x60A65E98
  0x617689AC 0x61768990 0x0
  ```

  Workaround: Where possible, consider using a route-map name instead of a named IPv6 ACL.

- CSCsi54780

  An MV64460 interface flaps when a service-policy is applied or removed.

  There are no known workarounds.

- CSCsi78118

  A traceback may be generated at the iphc_decompress function.

  This condition occurs on Cisco routers configured for Internet Protocol Header Compression (IPHC).

  There are no known workarounds.

- CSCsi82427

  Ping fails when a native Gigabit Ethernet (GigE) interface is configured with speed auto/duplex auto/ no neg auto and its peer is configured for fixed speed/duplex with media type rj45.

  Workaround: Configure the same speed /duplex on both sides.

- CSCsi96149

  The build breaks as a result of CSCek71805.

  There are no known workarounds.

- CSCsi99217

  When 6000 Layer 2 Tunneling Protocol (L2TP) sessions are disconnected, a Cisco IOS L2TP network server (LNS) router gets stuck on High CPU Utilization (99% or 100%) for the PPP IP route process for 5 minutes.

  There are no known workarounds.

- CSCsj07936

  On a Cisco 7200 router with an NPE-G2 engine, packets may be forwarded even if they are not destined for the router. This condition only occurs when the interface controller is in Promiscuous mode ON. (For example, configuring the Hot Standby Routing Protocol (HSRP) would cause the interface controller to go into Promiscuous mode ON.)

  Workaround: If HSRP is used, use the **standby use-bia** command as a workaround. You might also need to enter **shut/no-shut** to change the controller state.

- CSCsj13380

  Data corruption messages are displayed, and the **show isdn active** command displays incorrect information for the calling number on outgoing calls.

  The occurrence of this problem is inconsistent, however it shows up most frequently when the **isdn test call** command is used.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.4(4)XD7

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD7 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsi17113

  Under certain circumstances, some process-switched packets (such as Open Shortest Path First (OSPF) updates) can be corrupted as they are transmitted by a Cisco 7200 series router. The neighboring router may receive an error message similar to the following:

  ```
  %OSPF-4-ERRRCV: Received invalid packet: Bad Checksum from 10.2.3.4, POS5/2
  ```

  The OSPF update is retransmitted by the Cisco 7200 series router; there is no operational impact.

  This condition occurs only with NPE-G2 and PA-POS-OC3 when the POS link is busy (over 100Mbps), and there are many OSPF packets to be sent. This condition does not seem to occur when the packets are small, but as the packets get larger, it is more noticeable.

  Workaround: Use the newer PA-POS-1OC3 or PA-POS-2OC3 port adapter, instead of PA-POS-OC3. This problem does not occur when using these newer port adapters.

- CSCsi25540

  A Cisco 7200 VXR router with an NPE-G2 and a Port Adapter Jacket Card crashes continuously.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(4)XD7

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD7. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec12299

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

  Workarounds are available to help mitigate this vulnerability.

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

  This issue cannot be deterministically exploited by an attacker.

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

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml.
- CSCed57504

A router that is configured with a virtual template reloads unexpectedly.

This condition occurs on a Cisco router when a session that uses a virtual-template is terminated and the session is cleared from a Digital Subscriber Line (DSL) customer premises equipment (CPE) router that is the peer router for the connection.

There are no known workarounds.

- CSCej44509

  A memory leak occurs in chunks of AAA Authen DB allocated by aaa_authendb_alloc.

  This condition occurs during login authentication in both passed and failed cases.

  There are no known workarounds.

- CSCek55486

  The native Gigabit Ethernet (GE) interface on an NPE-G1 resets unexpectedly.

  This condition occurs on a Cisco 7200 series router when the underrun counter for the native GE interface increments continuously. You can verify the underrun counter in the output of the **show interfaces gigabitethernet** *slot*/*port* command.

  There are no known workarounds.

- CSCsd24183

  The router crashes on a user log-in.

  This condition occurs when the debug radius command is enabled and the T server supplies an unsupported attribute value. Debug is not enabled by default. The crash only occurs when troubleshooting Remote Authentication Dial-In User Service (RADIUS) issues.

  Workaround: Disable the **debug radius** command.

- 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.

- CSCsg40482

  An Integrated Services Digital Networks (ISDN) Layer 2 (L2) interface remains in the TEI_ASSIGNED state after you have performed a hard online insertion and removal (OIR) of a PA-MC-4T1 port adapter.

  Workaround: There are no known workarounds to prevent the condition from occurring. After the condition has occurred, reload the router.

- CSCsg51538

  On rare occasions, a router acting as a L2TP access concentrator (LAC) with remote end customer PCs running Cisco IOS 12.4(4)T4 crashes with a bus error.

  There are no known workarounds.

- CSCsg69458

  On a GigabitEthernet interface on an NPE-G2 on a Cisco 7200 series router, when a link goes down and comes up due to a cable being pulled, a burst of packets are seen coming out of the interface.

  There are no known workarounds.

- CSCsg76715

  A device crashes when you delete an access control entry (ACE) that was inserted in the middle of the access control list (ACL) rather than added at the end of the list.

  This condition occurs when all of the following preconditions are present:

  - The inserted ACE has a destination prefix length of 0, that is, it has an "any" statement instead of a destination address.
  - The ACL already has another ACE with the same SRC prefix length and an destination prefix length that is greater than 0 (that is, other than an "any" statement), and the inserted ACE has a lower sequence number than this other ACE.
  - The other ACE with a destination prefix length that is greater than 0 is deleted before you delete the inserted ACE.

  Workaround: First, delete the inserted ACE. Then, delete the other ACE with the same SRC prefix length and an destination prefix length that is greater than 0.

  Alternate Workaround: Delete the complete ACL.

- CSCsg95813

  The Layer 2 Tunneling Protocol Version 3 (L2TPv3) Xconnect interface does not work with IPv6 multicast. The L2TPv3 session will not send data packets.

  This condition occurs if you configure Xconnect and IPv6 under same physical interface but not under the same subinterface.

  Workaround: Configure **ipv6 multicast-routing** under global configuration.

- CSCsh30855

  A Cisco 7200 series router with an NPE-G2 crashes if the **test c7200 pci dum**p command is executed.

  Workaround: Refrain from using the **test c7200 pci dump** command.

- CSCsh90413

  The processor identifier (PID) for the Cisco 7201 router is missing from the s**how in**v command output.

  There are no known workarounds.

- CSCsi15195

  When a Cisco 7201 router is configured with 1K Layer 2 Tunneling Protocol Version 3 (L2TPv3) Ethernet sessions for any packet size, if the traffic is sent at a rate slightly higher than the No Drop Rate (NDR), the following message appears:

  ```
  ENVM-3-BLOWER: Fan 1 may have failed
  ```

  The **show environment all** command displays the following output:

  ```
  Fans: Fan 1 MAY HAVE FAILED !
  Fan 1 RPM is 0
  Fan 2 is believed to be working
  Fan 2 RPM is 10600
  Fan 3 is believed to be working
  Fan 3 RPM is 10600
  Fan 4 is believed to be working
  Fan 4 RPM is 10070
  ```

  If the chassis is opened with this condition, all the fans seem to be working fine. This message goes away only after reloading the box and reducing the traffic rate to the NDR. This condition has been seen intermittently for fan1 and fan3.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.4(4)XD6

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD6 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCse09256

  A Cisco 7200 series router with an NPE-G2 I/O card crashes with "memory-size iomem 256" during a PPP over ATM (PPPoA)/Layer 2 Tunnel Protocol (L2TP) test.

  This condition occurs when Ixia traffic of 1490 bytes is passed through the L2TP access concentrator (LAC) router running 8k PPPoA sessions, and L2TP is configured between the L2TP access concentrator (LAC) and the L2TP network server (LNS) router. The crash happens at the 1490 byte packet size, when performance measurements are increased incrementally for 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes, 1280 bytes, and 1490 bytes. To some extent, performance degradation on the PA-A6-OC3MM and PA-A3-OC3MM is expected. Memory allocation (malloc) failures can also happen in certain conditions.

  Workaround: Configure **memory-size iomem 128** on the LAC router. No other configuration changes are required.

- CSCsg11150

  The router crashes with traceback pointing to the parser.

  This condition occurs when the customer is issuing CLIs.

  Workaround: Use the XD5 version of ROMMON, which should avoid the detrimental crash.

Resolved Caveats—Cisco IOS Release 12.4(4)XD6

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD6. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea58000

  Large NVRAM sizes cause CPU intensive operations because of CPU intensive checksum calculations. An alternative method that yields CPU is needed.

  There are no known workarounds.

- CSCek68014

  A router running Cisco IOS Release 12.4(4)XD5 waits for an input character on the console if it is reloaded from a Telnet session using virtual type terminal (vty) lines.

  Workaround: Reload from the console, or upgrade to Cisco IOS Release 12.4(4)XD6.

- CSCse66625

  A router does not accept the **pppoe max-sessions** *number* command on a subinterface.

  Workaround: Configure the **pppoe max-sessions** *number* command on a broadband access (BBA) group, and then attach this BBA group to the subinterface.

- CSCsg86048

  When configuring an onboard GigabitEthernet interface with dot1q subinterfaces, one of which is an Multiprotocol Label Switching (MPLS)- enabled interface, traffic stops being received if an **xconnect** is configured on one of the subinterfaces.

  This condition occurs on a Cisco 7200 VXR router with an NPE-G2 running Cisco IOS release 12.4(4)XD4.

  Workaround: Unconfigure the **xconnect**.

- CSCsg89647

  When a **clear counters** command is issued on the f0/2 interface of an NPE-G2 / G0/3 interface on a Cisco 7200 VXR router, the CRC error, Alignment error, Broadcast RX, and RX undersize counters remain uncleared in the output.

  For example:

```
Router# clear counters
*May 14 07:13:24.975: %CLEAR-5-COUNTERS: Clear counter on all interfash controller
f0/2 | b Statist i82545 Statistics
CRC error 401 Symbol error 0 <------- CRC not cleared
Missed Packets 0 Single Collision 0
Excessive Coll 0 Multiple Coll 0
Late Coll 0 Collision 0
Defer  0 Receive Length 0
Alignment Error  200 XON RX 0 <------- Alignment error not cleared
XON TX  0 XOFF RX 0
XOFF TX  0 FC RX Unsupport 0
Packet RX (64)  0 Packet RX (127) 0
Packet RX (255)  0 Packet RX (511) 0
Packet RX (1023)  0 Packet RX (1522) 0
Good Packet RX  0 Broadcast RX  122 <----- Broadcast counter not cleared
Multicast RX  0 Good Packet TX 0
Good Octets RX.H 0 Good Octets RX.L 0
Good Octets TX.H 0 Good Octets TX.L 0
RX No Buff 0 RX Undersize  100 <----- undersize counter not cleared
```

This condition occurs on a Cisco 7200 VXR router with an NPE-G2.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.4(4)XD5

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCse09256

  A Cisco 7200 series router with an NPE-G2 I/O card crashes with "memory-size iomem 256" during a PPP over ATM (PPPoA)/Layer 2 Tunnel Protocol (L2TP) test.

  This condition occurs when Ixia traffic of 1490 bytes is passed through the L2TP access concentrator (LAC) router running 8k PPPoA sessions, and L2TP is configured between the L2TP access concentrator (LAC) and the L2TP network server (LNS) router. The crash happens at the 1490 byte packet size, when performance measurements are increased incrementally for 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes, 1280 bytes, and 1490 bytes. To some extent, performance degradation on the PA-A6-OC3MM and PA-A3-OC3MM is expected. Memory allocation (malloc) failures can also happen in certain conditions.

  Workaround: Configure **memory-size iomem 128** on the LAC router. No other configuration changes are required.

- CSCsg11150

  The router crashes with traceback pointing to the parser.

  This condition occurs when the customer is issuing CLIs.

  Workaround: Use the XD5 version of ROMMON, which should avoid the detrimental crash.

- CSCsg86048

  When configuring an onboard GigabitEthernet interface with dot1q subinterfaces, one of which is an Multiprotocol Label Switching (MPLS)- enabled interface, traffic stops being received if an **xconnect** is configured on one of the subinterfaces.

  This condition occurs on a Cisco 7200 VXR router with an NPE-G2 running Cisco IOS release 12.4(4)XD4.

  Workaround: Unconfigure the **xconnect**.

- CSCsg89647

  When a **clear counters** command is issued on the f0/2 interface of an NPE-G2 / G0/3 interface on a Cisco 7200 VXR router, the CRC error, Alignment error, Broadcast RX, and RX undersize counters remain uncleared in the output.

  For example:

```
Router# clear counters
*May 14 07:13:24.975: %CLEAR-5-COUNTERS: Clear counter on all interfash controller
f0/2 | b Statist i82545 Statistics
CRC error 401 Symbol error 0 <------- CRC not cleared
Missed Packets 0 Single Collision 0
Excessive Coll 0 Multiple Coll 0
Late Coll 0 Collision 0
Defer  0 Receive Length 0
Alignment Error  200 XON RX 0 <------- Alignment error not cleared
XON TX  0 XOFF RX 0
XOFF TX  0 FC RX Unsupport 0
Packet RX (64)  0 Packet RX (127) 0
```

```
Packet RX (255)  0 Packet RX (511) 0
Packet RX (1023)  0 Packet RX (1522) 0
Good Packet RX  0 Broadcast RX  122 <----- Broadcast counter not cleared
Multicast RX  0 Good Packet TX 0
Good Octets RX.H 0 Good Octets RX.L 0
Good Octets TX.H 0 Good Octets TX.L 0
RX No Buff 0 RX Undersize  100 <----- undersize counter not cleared
```

This condition occurs on a Cisco 7200 VXR router with an NPE-G2.

There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(4)XD5

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek51702

  The NPE-G2 crashes with a watchdog timeout after many SYS-3-CPUHOG messages.

  This condition usually occurs when a lot of messages appear on the console (generally, debugs).

  Workaround: To avoid this problem, use the following workarounds:

  1. Disable debugs, or

  2. Disable console logging, or

  3. Limit console logging to a minimum.

- CSCir00018

  The far end alarm is not asserted on a native GigabitEthernet port.

  This condition occurs when a **shut/no shut** is executed on the native GigabitEthernet interface on the near end router.

  There are no known workarounds.

- 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.

- CSCsd91454

  Voice traffic is dropped in one direction due to Internet Protocol Header Compression (IPHC) IPCRC error.

  This condition occurs some time after the voice call has been established. When the problem is occurring, the logs show IPHC error messages.

  Workaround: Use process switching.

- 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.

- 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

- CSCsf33015

  Line protocol up and down messages occur at three minutes intervals when NPE-G2 GigabitEthernet negotiation is disabled at an interface and the remote peer interface is in the shut state.

  Workaround: Enable negotiation.

- CSCsg16186

  When a PA-MCX-8TE1+ is in the system and 256MB I/O memory is configured, the system may crash during bootup. This condition will generate an SCM abort message in the crash info file.

  Workaround: Reduce the I/O memory in the configuration.

- CSCsg18075

  A Multi-Processor Forwarding (MPF) router crashes when the router is used as an L2TP access concentrator (LAC).

  This condition occurs when there are more than 3000 VLAN subinterfaces and PPP over Ethernet (PPPoE) sessions with some traffic.

  There are no known workarounds.

- CSCsg23462

  When the PPPoE Circuit ID Tag Processing feature is tested using the t**est pppoe** command for both the PPP over Ethernet (PPPoE) client and L2TP access concentrator (LAC), the debug looks clean. But with sniffer traces, PPPoE Active Discovery Requests (PADRs) and PPPoE Active Discovery Session-confirmations (PADSs) are found that contain duplicated circuit ID tags.

  This condition occurs in Cisco IOS releases 12.4(9)T1 and 12.4(4)T.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.4(4)XD4

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsf33015

  Line protocol up and down messages occur at three minutes intervals when NPE-G2 GigabitEthernet negotiation is disabled at an interface and the remote peer interface is in the shut state.

  Workaround: Enable negotiation.

- CSCsg06794

  When the VPN Service Adapter (VSA) and High Availability (HA) are configured, the system may not switch over properly when you use box-to-box redundancy. This condition also causes checksum errors when the system boots up.

  There are no known workarounds.

- CSCsg16186

  When a PA-MCX-8TE1+ is in the system and 256MB I/O memory is configured, the system may crash during bootup. This condition will generate an SCM abort message in the crash info file.

  Workaround: Reduce the I/O memory in the configuration.

- CSCsg38143

  If you remove a disk from a running system, a reload occurs. If the disk is reinserted it is recognized physically but cannot be read, and the reload fails until a power failure occurs.

  Workaround: Keep the disk in the system all the time.

Resolved Caveats—Cisco IOS Release 12.4(4)XD4

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek56991

  A Cisco 7200 series router may send a corrupted packet using a 2-port T3 serial enhanced port adapter (PA-2T3+). The rate of corrupted packets is very low.

  This condition occurs on a Cisco 7200 series router that runs Cisco IOS Release 12.2SB, 12.4T, or 12.4(4)XD3 and occurs when the router functions under high stress conditions, such as a high CPU load and an oversubscribed interface of the PA-2T3+.

  Workaround: Avoid a high CPU load and oversubscription of the interface of the PA-2T3+.

- CSCsb55483

  Traceback messages occur at ipfib_les_lookup_and_switch.

  There are no known workarounds.

- CSCsb82123

  The passive File Transfer Protocol (FTP) fails to work through Network Address Translation (NAT).

  When this condition occurs, the sniffer capture shows extra characters in the Passive FTP "Response 227" after the NAT translation is done.

  There are no known workarounds.

- CSCse05642

  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

- 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

- CSCsf25106

  After issuing a **loopback network payload** command on a PA-T3/PA-T3+, the remote end user sees cyclic redundancy check (CRC) and overrun errors.

  This condition only affects newer Cisco IOS 12.4/12.4T releases.

  Workaround: Issue the **no loopback network payload** command.

- CSCsf32623

  The on-board GigabitEthernet interfaces increase the ignored and input errors counters under normal, non-error circumstances.

  This condition occurs in Cisco IOS Release12.4(4)XD2 after the fix for CSCsd19400 has been added. The ignored counter increases if the GE controller drops a frame due to mac address filtering because the frame was not meant for that interface and was not a multicast/broadcast frame. The ignored counter can also increase if the controller does not have enough particles to copy the frame packet to the routers memory. Although dropping a frame because of mac address filtering is not an error condition, in 12.4(4)XD2 they are counted as input errors because the input errors counter is a compilation of multiple counters, including the ignored counter.

  There are no known workarounds.

- CSCsg01964

  A Cisco 7206VXR router with NPE-G2 running Cisco IOS Release 12.4(4)XD2 does not recognize SFP-GE-Z on the G0/2 and G0/3.

  There are no known workarounds.

- CSCsg05375

  An NPE-G2 running 12.4(4)XD2 reloads unexpectedly due to a SegV exception.

  There are no known workarounds.

- 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 Cisco IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the Cisco IOS FTP Client feature.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

- CSCsg31742

  False environment warnings about certain voltages are posted to the NPE-G2 console.

  There are no known workarounds. These false warnings can be ignored.

Open Caveats—Cisco IOS Release 12.4(4)XD3

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

This section describes the caveats for the C7200 VSA.

- CSCek28689

  Replay window size 1024 does not work.

  This condition occurs because the C7200 VSA does not support the anti-replay window size of 1024.

  Workaround: Use an anti-replay window size of 512 or lower.

- CSCek48252

  The Reverse Route Injection (RRI) current peer is not specifically set when a Quick Mode (QM) rekey retransmit failure occurs.

  This condition occurs when there is a QM rekey retransmit failure and the max retrans value is exceeded.When this condition occurs, IPsec sends deletes for its security associations (SAs), and if its has a dynamic map, that map is also cleaned-up. In this scenario, the peer (current peer) to which the SAs belong must be explicitly set, but several peers still appear in the dynamic map list even though their IPsec SAs are gone. In the current code, RRI is removing, or attempting to remove, routes for the oldest peer in the list; this must be changed to explicitly use the current peer.

  There are no known workarounds.

- CSCek50994

  IPSec security association (SA) lifetime changes made globally are not inherited by IPSec profiles. By default, all IPSec profiles have the default IPSec lifetime value of 3600 seconds. If the SA lifetime value is changed globally, this is not reflected in the individual IPSec profiles.

  This condition occurs when using the Cisco IOS router with IPSec profiles for Generic Routing Encapsulation (GRE) tunnel protection to IPSec virtual tunnel interfaces.

  Workaround: Use the CLI to edit each IPSec profile as necessary to change the IPSec SA lifetime value.

- CSCek51696

  Static Virtual Tunnel Interface (VTI) into Multiprotocol Label Switching (MPLS) does not work with the Border Gateway Protocol (BGP). A Cisco 7200 or 7300 router using BGP through IPSec Static Virtual Tunnel Interfaces (SVTI) for terminating IPSec traffic into MPLS does not forward packets from the MPLS side to the SVTI spoke.

  This condition occurs when a Cisco 7200 or 7300 router is using IPSec SVTI tunnels to terminate IPSec tunnels from remote spokes across the Internet into virtual routing/forwarding (VRF) instances, and thus, into an MPLS core. The problem exists when using BGP across the SVTI tunnel for dynamic routing between the spoke and 7200, and then distributing these routes into the MPLS core using multiprotocol BGP. End-to-end routing works fine. Traffic from the spoke reaches the 7200, is decrypted, and sent tag-switched to the MPLS network. However, traffic from the MPLS side is received by the 7200 and dropped, instead of being encrypted and forwarded to the spoke.

  Workaround: Use static routes or OSPF/EIGRP across the SVTI tunnel instead of BGP.

- CSCek53837

  Static Reverse Route Injection (RRI) routes are not deleted after stateless IPSec failover.

  This condition occurs when two Cisco 7200 series routers are being used for Hot Standby Router Protocol (HSRP) IPSec stateless failover at a VPN hub, and site-to-site IPSec tunnels have been configured with RRI static using the **reverse-route static command.** Only the active 7200 should have these static RRI routes installed; the standby 7200 should not have these routes. When a failover occurs, and the active 7200 becomes standby, it does not delete the static RRI routes. As a result, both 7200s can be advertising these routes to the hub LAN network. This can cause return traffic to get directed to the standby 7200 and be dropped.

  Workaround: If possible, avoid the **static** keyword and dynamic crypto maps.

- CSCek53865

  The RF_LAST_CLIENT should never give a timer expiration, but an RF-3-NOTIF-TMO message for the RF last client is displayed.

  If this message is followed by peer loss, it is not a problem because the Stream Control Transmission Protocol (SCTP) timer for the B2B is 50 seconds, while the RF timer is set for 30seconds, and under these circumstances this message is to be expected. However, if the message is received without a peer loss, it may indicate a problem.

  There are no known workarounds.

- CSCek53980

  When in VRF mode, if the user shuts down the High Availability (HA) primary router Hot Standby Router Protocol (HSRP) interface, it may trigger a new active router and incur an RF-Reload.

  This condition occurs because the HA primary router sends an HSRP coup message, which causes the secondary to reload.

  There are no known workarounds.

- CSCek54071

  When bringing up the High Availability (HA) active/standby router, the standby router may miss one or two IPSec security associations (SAs).

  There are no known workarounds.

- CSCek54073

  IPSec accounting is not accurate after a stateful failover.

  This condition occurs when a Cisco 7200 series router is acting as an IPSec hub in a Stateful Switchover (SSO) IPSec failover topology. If a failover occurs when using IPSec accounting, the resulting IPSec accounting logs may not reflect the correct values for packets or bytes encrypted and decrypted.

  There are no known workarounds.

- CSCek54331

  When a Cisco 7200 series router that is using the VSA encryption module and acting as an IPSec hub in a Stateful Switchover (SSO) IPSec failover topology reloads, a stream of the following error messages can appear on the console: %CHKPT-4-INVALID: Invalid checkpoint client ID.

  This condition occurs regardless of when the reload occurs manually or because of a failover-triggered reload.

  There are no known workarounds.

- CSCek56991

  A Cisco 7200 series router may send a corrupted packet via a 2-port T3 serial, enhanced port adapter (PA-2T3+). The rate of corrupted packets is very low.

  This condition is observed on a Cisco 7200 series router that runs Cisco IOS Release 12.2SB, Release 12.4T, or Release 12.4(4)XD3 and occurs when the router functions under high stress conditions such as a high CPU load and an oversubscribed interface of the PA-2T3+.

  Workaround: Avoid a high CPU load and oversubscription of the interface of the PA-2T3+.

- CSCsc22696

  High Availability (HA) + Stateful Switchover (SSO) IPSec security associations (SAs) are not cleared after synchronization verification. During the testing of security Security Association Database (SADB) synchronization, IPSec SAs are not cleared on both active and standby devices when they are cleared on the initiator.

  This condition occurs after a series of SADB synchronization tests.

  There are no known workarounds.

- CSCsc72722

  Transmission Control Protocol (TCP) connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  This condition occurs with the Cisco IOS Firewall (CBAC) enabled because the Transmission Control Protocol (TCP) idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This can lead to the TCP session not timing out.

  There are no known workarounds.

- CSCsd13899

  The fragment count displayed by the **show ip traffic** command has a delay of one packet if the packet is fragmented by the C7200 VSA. This counter is updated only when the next outbound packet is received. For example, if 50 packets are fragmented, the counters will show 49, until another packet is sent in the outbound direction.

  This condition occurs because the hardware does not give any output to indicate the packet was fragmented. It confirms that all the fragments are received and updates the fragment count only it receives the next packet. As a result, there is a delay of one packet in accounting for the outbound traffic in the case of fragmentation.

  Workaround: This behavior is as designed.

- CSCse07013

  Prefrag is not working on bundled security associations (SAs). If a transform set is configured with both Authentication Header (AH) and Encapsulating Security Payload (ESP) transforms, VSA always does fragmentation after encryption.

  This condition occurs because Prefrag is disabled for bundled SAs. When a transform set is configured with both AH and ESP transforms, VSA always does fragmentation after encryption.

  Workaround: This is a hardware limitation. If this is unacceptable, use ESP or AH.

- CSCse23502

  The **clear cry sa** command does not get an updated lifetime for a virtual tunnel interface (VTI). The **show crypto ipsec sa** command shows that the IPSec tunnel does not get the new configured lifetime.

  Workaround: To work around this issue:

  1. Bounce the tunnel interface, as in the following example:

     ```
     conf t
     int tunnel1
     shutdown
     no shut
     end
     ```

     When the tunnel comes back up, it will get the latest configured lifetime.

  2. Remove the configuration for **interface tunnel** and reconfigure it.

- CSCse73065

  Maximum transmission unit (MTU) values for the Dynamic Virtual Tunnel Interface (DVTI) IPSec tunnels are not set properly. The **show crypto ipsec sa** command shows the MTU value for DVTI tunnel as follows:

  ```
  path mtu 0, ip mtu -1, ip mtu idb
  ```

  Fragmentation is not working as expected. The **show crypto ipsec sa** command shows that the IPSec tunnel does not get the new configured lifetime.

  There are no known workarounds.

- CSCsf05474

  Memory leaks occur for Crypto Internet Key Management Protocol (IKMP), IPSec Key processes. These memory leaks can be seen with the tracebacks for the Crypto IKMP and IPSec Key Engine processes.

  This condition occurs in VRF-aware IPSec scenarios.

  There are no known workarounds.

- CSCsf05718

  When using a Cisco IOS software to Win2k setup with Layer 2 Tunnel Protocol (L2TP) and IPSec and port address translation (PAT) (Network Address Translation (NAT) overload) in between, only one client is able to connect at a given time. When a second client tries to connect, Internet Key Exchange (IKE) negotiation fails at MM_SA_SETUP.

  This condition only occurs with PAT; dynamic NAT works fine. Also, this condition only occurs when the second client is using the same username. If each client uses a different username to login, then the PAT setup also works.

  Workaround: Use a different username for each client machine.

- CSCsf12577

  A router configured with Static Virtual Tunnel Interface (SVTI) crashes when copying an SVTI configuration file from disk media into running-config.

  This condition occurs when a router has SVTI IPSec peers established to remote SVTI peers, its current running configuration is stored in disk media (for example, disk2:) rather than startup-config, and it is rebooted, while the remote SVTI IPSec peers are still sending inbound traffic. After the reload, a crash occurs when the SVTI configuration stored in disk media is copied into running-config.

  Workaround: Prior to copying the configuration file from disk media to running-config, shutdown all physical interfaces that receive traffic from the remote SVTI IPSec peers. Then, copy the configuration file into running-config. After the copy is complete, enter the **no shutdown** command on previously shut interfaces.

- CSCsf33015

  When NPEG2 Gigabit Ethernet negotiation is disabled and its peer interface is in the shut state, the line protocol up and down message can appear at three minutes intervals on the console.

  Workaround: Enable negotiation.

- CSCsf97252

  Packets in priority class are dropped by the VSA.

  This condition occurs when Low Latency Queuing (LLQ) for IPSec Encryption Engines is configured and there is over-subscription over the VSA.

  There are no known workarounds.

- CSCsg01964

  A Cisco 7206VXR router with NPE-G2 running Cisco IOS Release 12.4(4)XD2 does not recognize SFP-GE-Z on the G0/2 and G0/3.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(4)XD3

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeh52502

  Crypto conditional debug does not work properly for the **spi**, **connid**, and **username** options.

  There are no known workarounds.

- CSCej21681

  Traceback occurs while using a Point-to-Point Protocol (PPP) configuration with c7200-js-mz.

  There are no known workarounds.

- CSCsb42470

  The output of the **show interfaces sum** and the **show interfaces tunnel** commands is inconsistent. For example, the output of the **show interfaces tunnel** command displays incorrect values for the number of packets that are switched per second and the number of bytes that have been switched.

  This condition occurs when CEF switching is enabled, and when IPsec tunnel protection or a virtual interface (VTI) is applied to a tunnel interface.

  Workaround: Disable CEF switching, and use fast-switching or process-switching.

- CSCsb52717

  A Cisco router configured for multicast VPN may reload after receiving a malformed Multicast Distribution Tree (MDT) data group join packet.

  This condition affects all IOS versions that support mVPN MDT.

  Workaround: Filter out MDT Data Join messages from the router sending the malformed packet using the Receive Access Control List (rACL) feature. Note that by doing this, the offending router will not be able to participate within the mVPN data trees.

  The following example shows how to block malformed MDT Data Join messages that are sent from the device's IP addresses using a receive ACL:

```
!
ip receive access-list 111
!
access-list 111 deny udp host ip-address-of-router-sending-malformed-join-request host
224.0.0.13 eq 3232
access-list 111 permit ip any any
!
```

Note Ensure that the rACL does not filter critical traffic such as routing protocols or interactive access to the routers. Filtering necessary traffic could result in an inability to remotely access the router, thus requiring a console connection. For this reason, lab configurations should mimic the actual deployment as closely as possible. As always, Cisco recommends that you test this feature in the lab prior to deployment. For more information on rACLs, refer to "*Protecting Your Core: Infrastructure Protection Access Control Lists*" at: http://www.cisco.com/warp/public/707/racl.html.

- CSCsb58590

  The EzVPN server crashes when the **debug crypto isakmp detail** command is enabled on the EzVPN server and the client tries to establish a connection.

  There are no known workarounds.

- CSCsb93407

  With H323 call service stopped, the router still listens on tcp port 1720 and completes connection attempts.

  This condition occurs when H323 is disabled using the following configuration commands:

  ```
  voice service voip
  h323
  call service stop
  ```

  Workaround: Deploy an interface access list that blocks access to the Transmission Control Protocol (TCP) port 1720 for traffic that is destined for any of the IP addresses of the router.

- CSCsc98725

  Spurious memory access messages occur when keepalive is configured on a template.

  There are no known workarounds.

- CSCsd44501

  The line protocol flaps for PA CT3,CE3, MC-8TE1 with any serial encaps configuration.

  This condition occurs only with following midplane revision chassis:

  - CISCO7206VXR (midplane) hardware version less than 2.8 - 800-04667-11
  - CISCO7204VXR (midplane) hardware version less than 2.8 - 800-04766-11.

  There are no known workarounds.

- CSCse51820

  The PA-POS-2OC3 interface flaps after the interface is up.

  This condition always occurs on SB-related images.

  Workaround: After rebooting, enter the following commands at the CLI:

  ```
  test c7200 memory write F1000A18 002E0000
  test c7200 memory write F1000A20 002D0020
  ```

- CSCse53002

  Memory leaks occur at the IPSec key engine process.

  This condition occurs whenever there is traffic.

  There are no known workarounds.

- CSCse69102

  Spurious memory access occurs at ike_profile_remove.

  This condition occurs on a Cisco router that runs Cisco IOS 12.4(6)T3, when there is at least one Internet Key Exchange (IKE) or IPSec security association (SA), and the profile is removed using the CLI with debug crypto isakmp turned on.

  Workaround: Turn off crypto isakmp debugs or clear all the crypto sessions and then remove the isakmp profile.

- 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

- CSCsf06323

  When using IP inspection and process switching, the outbound crypto access-check ACL is only processed by the first packet, which also triggers the IP inspect session. For subsequent packets, the access-list is not processed at all.

  Workaround: Use CEF or fast switching with IP inspection.

Open Caveats—Cisco IOS Release 12.4(4)XD2

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek44895

  The global positioning service (GPS) device does not synchronize with the AUX port of NPE-G2.

  This condition occurs with the **sh ntp asso det** command and affects only the GPS/Network Time Protocol (NTP) connectivity with the AUX port. There is no problem with normal operation of the router.

  There are no known workarounds.

- CSCsd44501

  The line protocol flaps on serial interfaces configured with the following port adapters: CT3,CE3, and MC-8TE1.

  There are no known workarounds.

- CSCsd89790

  NPE-G2 hangs when the **reset** command is issued after the **send break** command.

  There are no known workarounds.

- CSCse17976

  NPE-G2 crashes when using MC-2T3+ in a port adapter jacket card.This does not occur on the regular slot.

  Workaround: Use the port adapter in the normal slot.

- CSCse18854

  Performance for VAM2+ is 14% lower in an Escort card slot than in normal port adapter slot.

  This condition occurs only when the CPU is near 100% utilization.

  There are no known workarounds.

- CSCse19109

  The router crashes when frequent start/stop of the traffic stream occurs for an MC-STM1 port adapter on an Escort slot.

  This condition occurs intermittently.

  There are no known workarounds.

- CSCse81609

  NPE-G2 crashes with a program exception error when the **reset** command is issued after jumping to ROMMON for a send break. NPE-G2 goes into a loop and can only recover by a power cycle.

  There are no known workarounds.

- CSCse85068

  A ping packet with a packet size greater than 1498 bytes cannot pass from the L2TP access concentrator (LAC) through the L2TP network server (LNS) to the client.

  Workaround: Enlarge the maximum transmission unit (MTU) of the LAC-facing physical interface on the client to be greater than or equal to1502.

Resolved Caveats—Cisco IOS Release 12.4(4)XD2

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsb25337

  Cisco devices running Cisco IOS, which support voice and are not configured for Session Initiated Protocol (SIP) are vulnerable to a crash under yet to be determined conditions, but isolated to traffic destined to User Datagram Protocol (UDP) 5060. SIP is enabled by default on all Advanced images which support voice and do not contain the fix for CSCsb25337. Devices which are properly configured for SIP processing are not vulnerable to this issue. Workarounds exist to mitigate the effects of this problem. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.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 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

- CSCsd58381

  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

Open Caveats—Cisco IOS Release 12.4(4)XD1

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek43101

  When running Multiprotocol Label Switching (MPLS) and MPLS VPN applications on native GE ports of NPE-G2, occasional data integrity errors can occur.

  Workaround: Reduce the data rate.

- CSCsd24814

  When applying an access list with 5000 access control entries (ACEs) to the crypto map, traceback can be seen at the Crypto access control list (ACL).

  There are no known workarounds.

- CSCsd62214

  When the IPsec packet gets fragmented after encryption and the traffic rate for the large packets is high, the decrypting side may drop some packets as a result of an output authentication error. The packet drop is minimal and should not impact performance.

  Workaround: Avoid fragmentation of IPsec packets either by path mtu discovery, or enable prefragmentation using the **crypto ipsec fragmentation before-encryption** command.

- CSCsd39684

  In process switching with crypto, a "Characters In" value is seen on the route-cache of the incoming interface when the traffic is coming from the other side on an IPsec tunnel. If traffic flows from the router side, this problem does not occur.

  Workaround: Use another switching method.

- CSCsd53289

  If you have a crypto card in one slot and remove it and insert the card in another slot, the **show crypto engine configuration** command shows the old slot number in the crypto engine *in slot:* field.

  There are no known workarounds.

- CSCse79443

  The VPN client does not connect to Cisco 7200 series routers with Remote Authentication Dial-In User Service (RADIUS).

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(4)XD1

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.4(4)XD1.

Open Caveats—Cisco IOS Release 12.4(4)XD

This section documents possible unexpected behavior by Cisco IOS Release 12.4(4)XD and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek40085

  Under high traffic rate conditions, packet drops can occur on NPE-G2 built-in Ethernet ports. As a result of this caveat, performance will appear lower than expected.

  Workaround: Allow a drop rate of 0.01% during testing, or stagger turning on the multiple data streams into the native GE ports.

- CSCsd42073

  Low NDR values are observed on NPE-G2 with 1483 Bridging (Transparent Bridging).

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(4)XD

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)XD. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.4(4)XD.

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family of routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and http://www.cisco.com/univercd/home/index.htm.

Use these release notes with these documents:

- Release-Specific Documents, page 76
- Platform-Specific Documents, page 76
- Feature Modules, page 77
- Cisco Feature Navigator, page 77
- Cisco IOS Software Documentation Set, page 77

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.4 T and are located on Cisco.com and http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.4 T*

  On Cisco.com at:

  Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4T > General Information> Release Notes

  On http://www.cisco.com/univercd/home/index.htm at:

  Cisco IOS Software > Cisco IOS Release 12.4T > Release Notes

- Product bulletins, field notices, and other release-specific documents at http://www.cisco.com/univercd/home/index.htm

- *Caveats for Cisco IOS Release 12.4 T*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.4XD" in these release notes, see *Caveats for Cisco IOS Release 12.4 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.4 T.

  On Cisco.com at:

  Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4T > General Information > Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 5: Caveats

  On http://www.cisco.com/univercd/home/index.htm at:

  Cisco IOS Software > Cisco IOS Release 12.4T > Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 5: Caveats

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, l**og in** to Cisco.com and click **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.2 Mainline> Troubleshoot and Alerts > Bug Toolkit**. 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

These documents are available for the Cisco 7000 family of routers on Cisco.com:

- *Cisco7200 VXR Installation and Configuration Guide*
- *Cisco 7200 VXR Routers Quick Start*

On http://www.cisco.com/univercd/home/index.htm at:

Routers > Cisco 7200VXR

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.4(4)XD 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 module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Products and Services > Cisco IOS Software > Cisco IOS Release 12.4T > Configure> Feature Guides

On http://www.cisco.com/univercd/home/index.htm at:

Cisco IOS Software > Cisco IOS Release 12.4 > New Feature Documentation> 12.4(x) New Features

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 references, 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.

On Cisco.com at:

Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4T > Configure > Configuration Guides

Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4T > Reference Guides > Command References

On http://www.cisco.com/univercd/home/index.htm at:

Cisco IOS Software > Cisco IOS Release 12.4T Configuration Guides

Cisco IOS Software > Cisco IOS Release 12.4T Command References

Cisco IOS Release 12.4T Documentation Set Contents

Table 23 and Table 24 list the contents of the Cisco IOS Release 12.4T software documentation set.

On Cisco.com at:

Products and Services > Cisco IOS Software > Cisco IOS Releases 12.4T

On http://www.cisco.com/univercd/home/index.htm at:

Cisco IOS Software > Cisco IOS Release 12.4T

Cisco IOS Release 12.4T Documentation Set

Table 23 lists the Cisco IOS Release 12.4T configuration guides and command references.

Note Some of the configuration guides in the following table reference Cisco IOS Release12.4 versions of these documents. In these instances, no distinct Cisco IOS Release 12.4T version of the guide exists and the necessary configuration information is in the Cisco IOS Release12.4 version of the document. Keep in mind that Cisco IOS Release 12.4(4)XD is based on Cisco IOS Release **12.4(4)T.** All features in Cisco IOS Release **12.4(4)T** are in Cisco IOS Release 12.4(4)XD. The references to Cisco IOS Release 12.4 configuration guides in the following table do not indicate that all features in Cisco IOS Release 12.4 are in Cisco IOS Release 12.4(4)XD.

Table 23 Cisco IOS Release 12.4T Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Description
IP	
Cisco IOS BGP Configuration Guide, Release 12.4T	The configuration guide describes configuration tasks to configure various advanced Border Gateway Protocol (BGP) features, such as BGP next-hop address tracking, BGP Nonstop Forwarding (NSF) awareness, and route dampening. BGP is an interdomain routing protocol designed to provide loop-free routing between organizations.
Cisco IOS DHCP Configuration Guide, Release 12.4T	The configuration guide describes the concepts and the tasks needed to configure the Cisco IOS Dynamic Host Configuration Protocol (DHCP).
Cisco IOS IP Addressing Services Configuration Guide, Release 12.4 *Cisco IOS IP Addressing Services Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring IP addressing and services, including Network Address Translation (NAT), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Application Services Configuration Guide, Release 12.4T *Cisco IOS Application Services Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring IP application services, including IP access lists, Web Cache Communication Protocol (WCCP), Gateway Load Balancing Protocol (GLBP), Server Load Balancing (SLB), Hot Standby Router Protocol (HSRP), and Virtual Router Redundancy Protocol (VRRP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Mobility Configuration Guide, Release 12.4 *Cisco IOS IP Mobility Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring Mobile IP and Cisco Mobile Networks. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Multicast Configuration Guide, Release 12.4 *Cisco IOS IP Multicast Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring IP multicast, including Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Source Discovery Protocol (MSDP). The command reference provides detailed information about the commands used in the configuration guide.

Table 23 Cisco IOS Release 12.4T Configuration Guides and Command References (Continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4 *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring IP routing protocols, including Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Switching Configuration Guide, Release 12.4 *Cisco IOS IP Switching Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring IP switching features, including Cisco Express Forwarding (CEF), fast switching, and Multicast Distributed Switching (MDS). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IPv6 Configuration Guide, Release 12.4T *Cisco IOS IPv6 Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring IP version 6 (IPv6), including IPv6 broadband access, IPv6 data-link layer, IPv6 multicast routing, IPv6 quality of service (QoS), IPv6 routing, IPv6 services and management, and IPv6 tunnel services. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS NAT Configuration Guide, Release 12.4T	The configuration guide contains configuration documentation for s configuring NAT for IP address conservation and using application level gateways with NAT.
Cisco IOS Optimized Edge Routing Configuration Guide, Release 12.4T *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring Optimized Edge Routing (OER) features, including OER prefix learning, OER prefix monitoring, OER operational modes, and OER policy configuration. The command reference provides detailed information about the commands used in the configuration guide.
Security and VPN	
Cisco IOS Security Configuration Guide, Release 12.4T *Cisco IOS Security Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring various aspects of security, including terminal access security, network access security, accounting, traffic filters, router access, and network data encryption with router authentication. The command reference provides detailed information about the commands used in the configuration guide.
QoS	
Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4T *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring quality of service (QoS) features, including traffic classification and marking, traffic policing and shaping, congestion management, congestion avoidance, and signaling. The command reference provides detailed information about the commands used in the configuration guide.
LAN Switching	
Cisco IOS LAN Switching Configuration Guide, Release 12.4 *Cisco IOS LAN Switching Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to local-area network (LAN) switching features, including configuring routing between virtual LANs (VLANs) using Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, and IEEE 802.1Q encapsulation. The command reference provides detailed information about the commands used in the configuration guide.

Table 23 Cisco IOS Release 12.4T Configuration Guides and Command References (Continued)

Configuration Guide and Command Reference Titles	Description
Multiprotocol Label Switching (MPLS)	
Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.4 *Cisco IOS Multiprotocol Label Switching Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring Multiprotocol Label Switching (MPLS), including MPLS Label Distribution Protocol, MPLS traffic engineering, and MPLS Virtual Private Networks (VPNs). The command reference provides detailed information about the commands used in the configuration guide.
Network Management	
Cisco IOS IP SLAs Monitoring Technology Configuration Guide, Release 12.4 *Cisco IOS IP SLAs Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring the Cisco IOS IP Service Level Assurances (IP SLAs) feature. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS NetFlow Configuration Guide, Release 12.4T *Cisco IOS NetFlow Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to NetFlow features, including configuring NetFlow to analyze network traffic data, configuring NetFlow aggregation caches and export features, and configuring Simple Network Management Protocol (SNMP) and NetFlow MIB features. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Network Management Configuration Guide, Release 12.4 *Cisco IOS Network Management Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to network management features, including performing basic system management, performing troubleshooting and fault management, configuring Cisco Discovery Protocol (CDP), configuring Cisco Networking Services (CNS), configuring DistributedDirector, and configuring Simple Network Management Protocol (SNMP). The command reference provides detailed information about the commands used in the configuration guide.
Voice	
Cisco CallManager and Cisco IOS Interoperability Configuration Guide, Release 12.4T	The configuration guide provides configuration information about Cisco IOS voice features for Cisco Unified CallManager and Cisco IOS Interoperability.
Cisco IOS Voice Configuration Library *Cisco IOS Voice Command Reference*	The configuration library is a task-oriented collection of configuration guides, application guides, a troubleshooting guide, feature documents, a library preface, a voice glossary, and more. It also covers Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. In addition, the library includes documentation for IP telephony applications. The command reference provides detailed information about the commands used in the configuration library.
Wireless / Mobility	
Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to understanding and configuring a Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunication System (UMTS) network. The command reference provides detailed information about the commands used in the configuration guide.

Table 23 Cisco IOS Release 12.4T Configuration Guides and Command References (Continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS Mobile Wireless Home Agent Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Home Agent Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Mobile Wireless Home Agent, which is an anchor point for mobile terminals for which Mobile IP or Proxy Mobile IP services are provided. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Packet Data Serving Node (PDSN), a wireless gateway between the mobile infrastructure and standard IP networks that enables packet data services in a Code Division Multiple Access (CDMA) environment. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to understanding and configuring Cisco IOS Radio Access Network products. The command reference provides detailed information about the commands used in the configuration guide.
Cisco *IOS Wireless LAN Configuration Guide*, Release 12.4T	The configuration guide provides the conceptual information, configuration tasks, and examples to help you configure and monitor a "wireless-aware" router using the Cisco IOS CLI, which can be used through a console port or Telnet session.
Long Reach Ethernet (LRE) and Digital Subscriber Line (xDSL)	
Cisco IOS Broadband Access Aggregation and DSL Configuration Guide, Release 12.4 *Cisco IOS Broadband Access Aggregation and DSL Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring broadband access aggregation and digital subscriber line features. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Service Selection Gateway Configuration Guide, Release 12.4 *Cisco IOS Service Selection Gateway Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring Service Selection Gateway (SSG) features, including subscriber authentication, service access, and accounting. The command reference provides detailed information about the commands used in the configuration guide.
Dial—Access	
Cisco IOS Dial Technologies Configuration Guide, Release 12.4 *Cisco IOS Dial Technologies Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring lines, modems, and ISDN services. This guide also contains information about configuring dialup solutions, including solutions for remote sites dialing in to a central office, Internet service providers (ISPs), ISP customers at home offices, enterprise WAN system administrators implementing dial-on-demand routing, and other corporate environments. The command reference provides detailed information about the commands used in the configuration guide.

Table 23 Cisco IOS Release 12.4T Configuration Guides and Command References (Continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS VPDN Configuration Guide, Release 12.4T *Cisco IOS VPDN Command Reference*, Release 12.4T	This book contains the commands used to configure and maintain a Cisco IOS virtual private dialup network (VPDN). The commands are listed alphabetically.
Asynchronous Transfer Mode (ATM)	
Cisco IOS Asynchronous Transfer Mode Configuration Guide, Release 12.4 *Cisco IOS Asynchronous Transfer Mode Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring Asynchronous Transfer Mode (ATM), including WAN ATM, LAN ATM, and multiprotocol over ATM (MPOA). The command reference provides detailed information about the commands used in the configuration guide.
WAN	
Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 *Cisco IOS Wide-Area Networking Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring wide-area network (WAN) features, including: Layer 2 Tunneling Protocol Version 3 (L2TPv3); Frame Relay; Link Access Procedure, Balanced (LAPB); and X.25. The command reference provides detailed information about the commands used in the configuration guide.
System Management	
Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to using Cisco IOS software to configure and maintain Cisco routers and access servers, including information about using the Cisco IOS command-line interface (CLI), loading and maintaining system images, using the Cisco IOS file system, using the Cisco IOS Web browser user interface (UI), and configuring basic file transfer services. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Interface and Hardware Component Configuration Guide, Release 12.4 *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring and managing interfaces and hardware components, including dial shelves, LAN interfaces, logical interfaces, serial interfaces, and virtual interfaces. The command reference provides detailed information about the commands used in the configuration guide.

Table 23 Cisco IOS Release 12.4T Configuration Guides and Command References (Continued)

Configuration Guide and Command Reference Titles	Description
IBM Technologies	
Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4 *Cisco IOS Bridging Command Reference*, Release 12.4T *Cisco IOS IBM Networking Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring: • Bridging features, including: transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and Token Ring Route Switch Module (TRRSM). • IBM network features, including: data-link switching plus (DLSw+), serial tunnel (STUN), and block serial tunnel (BSTUN); Logical Link Control, type 2 (LLC2), and Synchronous Data Link Control (SDLC); IBM Network Media Translation, including SDLC Logical Link Control (SDLLC) and Qualified Logical Link Control (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA Frame Relay Access, Advanced Peer-to-Peer Networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach. The two command references provide detailed information about the commands used in the configuration guide.
Additional and Legacy Protocols	
Cisco IOS AppleTalk Configuration Guide, Release 12.4 *Cisco IOS AppleTalk Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring the AppleTalk protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS DECnet Configuration Guide, Release 12.4 *Cisco IOS DECnet Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring the DECnet protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS ISO CLNS Configuration Guide, Release 12.4 *Cisco IOS ISO CLNS Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring International Organization for Standardization (ISO) Connectionless Network Service (CLNS). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Novell IPX Configuration Guide, Release 12.4 *Cisco IOS Novell IPX Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring the Novell Internetwork Packet Exchange (IPX) protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Terminal Services Configuration Guide, Release 12.4 *Cisco IOS Terminal Services Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring terminal services, including DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD). The command reference provides detailed information about the commands used in the configuration guide.

Table 24 lists the documents and resources that support the Cisco IOS Release 12.4T software configuration guides and command references.

Table 24 Cisco IOS Release 12.4T Supporting Documents and Resources

Document Title	Description
Cisco IOS Master Commands List, Release 12.4T	An alphabetical listing of all the commands documented in the Cisco IOS Release 12.4T command references.
Cisco IOS New, Modified, Replaced, and Removed Commands, Release 12.4T	A listing of all the new, modified, replaced and removed commands for the Cisco IOS Release 12.4T release, grouped by maintenance release and ordered alphabetically within each group.
System Messages for Cisco IOS Release 12.4 T	These publications list and describe Cisco IOS system messages for Cisco IOS Release 12.4T. Not all system messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.
Cisco IOS Debug Command Reference, Release 12.4T	This publication contains an alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, and usage guidelines.
Cisco IOS Fax and Modem Services over IP Application Guide, Release 12.4T	The application guide includes descriptions and configuration instructions for fax and modem transmission capabilities on Cisco Voice over IP (VoIP) networks.
Cross-Platform Release Notes for Cisco IOS Release 12.4T	This documentation describes general release information, including information about supported platforms, feature sets, platform-specific notes, and Cisco IOS software defects.
Dictionary of Internetworking Terms and Acronyms	This publication compiles and defines the terms and acronyms used in the internetworking industry.
RFCs	RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/
MIBs	MIBs are used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Open Source License 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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 75.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. 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. (0805R)

© 2008 Cisco Systems, Inc.
All rights reserved.