



Release Notes for Cisco 7000 Family for Cisco IOS Release 12.3 YM

May 21, 2009

Cisco IOS Release 12.3(14)YM13

OL-7811-13

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.3(14)YM13. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(14)YM13, see the [“Caveats for Cisco IOS Release 12.3 YM” section on page 12](#) and *Caveats for Cisco IOS Release 12.3*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.3* located on Cisco.com and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 6](#)
- [MIBs, page 10](#)
- [Important Notes, page 11](#)
- [Caveats for Cisco IOS Release 12.3 YM, page 12](#)
- [Related Documentation, page 49](#)
- [Obtaining Documentation, page 56](#)
- [Documentation Feedback, page 56](#)
- [Obtaining Additional Publications and Information, page 58](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(14)YM13 and includes the following sections:

- [Memory Recommendations, page 2](#)
- [Supported Hardware, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 4](#)
- [Feature Support, page 4](#)

Memory Recommendations

Table 1 *Memory Recommendations for the Cisco IOS Release 12.3 YM*

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	IOS IP	c7200-is-mz	48 MB	128 MB	RAM
Cisco 7300 Series	IOS IP	c7301-is-mz	64 MB	128 MB	RAM
Cisco 7400 Series	IOS IP	c7400-is-mz	64 MB	128 MB	RAM

Multi-Processor Forwarding (MPF) System Memory Requirements

Since the second CPU, CPU1, uses shared system memory for various accelerated features, [Table 2](#) describes the minimum system memory requirements for all supported routers by type of deployment and whether the deployment is “basic” or features are turned on.



Note Only -i12s and -i12o3s images have MPF support.

The MPF for Broadband LAC, LNS, and PTA feature requires ROMmon version 2.0. If a ROMmon upgrade is needed, contact your Cisco support engineer (SE). The minimum required ROMmon version is:

- ROMmon version 12.3(4r)T2 for the Cisco 7301
- ROMmon version 12.3(4r)T3 for the Cisco 7200 VXR NPE-G1



Note MPF is only supported on the Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 routers. For more information, refer to [Multi-Processor Forwarding \(MPF\) for Broadband LAC, LNS, and PTA](#).

Table 2 *MPF Minimum System Memory Requirements*

Network Deployment	Supported Session Range	Minimum System Memory
LAC (basic, no features)	0-4000 sessions	<ul style="list-style-type: none"> • 256 MB
LAC (basic, no features)	4000-8000 sessions	<ul style="list-style-type: none"> • 512 MB • 1 Gigabyte is highly recommended.
LNS/PTA (basic, no features)	0-8000 sessions	<ul style="list-style-type: none"> • 512 MB • 1 Gigabyte is highly recommended.
LAC/LNS/PTA (with features)	0-8000 sessions	<ul style="list-style-type: none"> • 512 MB • 1 Gigabyte is highly recommended.
LAC/LNS/PTA (basic or with features)	8000-16000 sessions	<ul style="list-style-type: none"> • 1 Gigabyte is required.

Basic Deployment

In a basic deployment—there are no configured features and only minimal routes. Specifically there is no use of ACLs, QoS Policers, or VRFs. The maximum number of required routes fit into the available memory space.

Features Deployment

In a features deployment—any features and number of routes can be configured.

Supported Hardware

Cisco IOS Release 12.3(14)YM13 supports the following Cisco 7000 platforms:

- Cisco 7200 series routers
- Cisco 7301 series routers
- Cisco 7400 series routers

For detailed descriptions of the new hardware features, see the [“New and Changed Information”](#) section on page 6.

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 12.3(14)YM13:

```
Router> show version
Cisco IOS Software, 7301 Software (c7301-is-mz), Version 12.3(14)YM13, RELEASE SOFTWARE (fc1)
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to *Upgrading the Cisco IOS Software Release in Cisco Routers and Modems* located at:

<http://www.cisco.com/warp/public/732/>

Feature Support

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



Caution

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

The feature set tables have been removed from the Cisco IOS Release 12.3 release notes to improve the usability of the release notes documentation. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

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

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

<http://www.cisco.com/register>

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

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

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

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

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

To determine which software images (feature sets) in Cisco IOS Release 12.3 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

-
- Step 1** From the Cisco Feature Navigator home page, click **Feature**.
 - Step 2** To find a feature, use either “Search by full or partial feature name” or “Browse features in alphabetical order.” Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the text box on the left side of the web page.
 - Step 3** Select a feature from the left text box, and click the **Add** button to add a feature to the Selected Features text box on the right side of the web page.



Note To learn more about a feature in the list, click the **Description** button below the left box.

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

- Step 4** Click **Continue** when you are finished selecting features.
 - Step 5** From the Major Release drop-down menu, choose **12.3**.
 - Step 6** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 7** From the Platform Family drop-down menu, select the appropriate hardware platform. The “Your selections are supported by the following:” table will list all the software images (feature sets) that support the feature(s) that you selected.
-

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

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.3, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

-
- Step 1** From the Cisco Feature Navigator home page, click **Compare/Release**.
 - Step 2** In the “Find the features in a specific Cisco IOS release, using one of the following methods:” box, choose **12.3** from the Cisco IOS Major Release drop-down menu.
 - Step 3** Click **Continue**.
 - Step 4** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 5** From the Platform Family drop-down menu, choose the appropriate hardware platform.
 - Step 6** From the Feature Set drop-down menu, choose the appropriate feature set. The “Your selections are supported by the following:” table will list all the features that are supported by the feature set (software image) that you selected.
-

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family of routers for Cisco IOS Release 12.3 YM:

New Hardware Features in Cisco IOS Release 12.3(14)YM13

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM13.

New Software Features in Cisco IOS Release 12.3(14)YM13

There are no new software features supported in Cisco IOS Release 12.3(14)YM13.

New Hardware Features in Cisco IOS Release 12.3(14)YM12

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM12.

New Software Features in Cisco IOS Release 12.3(14)YM12

There are no new software features supported in Cisco IOS Release 12.3(14)YM12.

New Hardware Features in Cisco IOS Release 12.3(14)YM11

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM11.

New Software Features in Cisco IOS Release 12.3(14)YM11

There are no new software features supported in Cisco IOS Release 12.3(14)YM11.

New Hardware Features in Cisco IOS Release 12.3(14)YM10

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM10.

New Software Features in Cisco IOS Release 12.3(14)YM10

There are no new software features supported in Cisco IOS Release 12.3(14)YM10.

New Hardware Features in Cisco IOS Release 12.3(14)YM9

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM9.

New Software Features in Cisco IOS Release 12.3(14)YM9

There are no new software features supported in Cisco IOS Release 12.3(14)YM9.

New Hardware Features in Cisco IOS Release 12.3(14)YM8

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM8.

New Software Features in Cisco IOS Release 12.3(14)YM8

There are no new software features supported in Cisco IOS Release 12.3(14)YM8.

New Hardware Features in Cisco IOS Release 12.3(14)YM7

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM7.

New Software Features in Cisco IOS Release 12.3(14)YM7

There are no new software features supported in Cisco IOS Release 12.3(14)YM7.

New Hardware Features in Cisco IOS Release 12.3(14)YM6

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM6.

New Software Features in Cisco IOS Release 12.3(14)YM6

There are no new software features supported in Cisco IOS Release 12.3(14)YM6.

New Hardware Features in Cisco IOS Release 12.3(14)YM5

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM5.

New Software Features in Cisco IOS Release 12.3(14)YM5

There are no new software features supported in Cisco IOS Release 12.3(14)YM5.

New Hardware Features in Cisco IOS Release 12.3(14)YM4

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM4.

New Software Features in Cisco IOS Release 12.3(14)YM4

There are no new software features supported in Cisco IOS Release 12.3(14)YM4.

New Hardware Features in Cisco IOS Release 12.3(14)YM3

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM3.

New Software Features in Cisco IOS Release 12.3(14)YM3

There are no new software features supported in Cisco IOS Release 12.3(14)YM3.

New Hardware Features in Cisco IOS Release 12.3(14)YM2

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM2.

New Software Features in Cisco IOS Release 12.3(14)YM2

The following new software feature is supported by the Cisco IOS Release 12.3(14)YM2:

Multi-Processor Forwarding (MPF) for Broadband LAC, LNS, and PTA

Platforms: Cisco 7204VXR, Cisco 7206VXR routers, and Cisco 7301 router

Multi-Processor Forwarding (MPF) for Broadband LAC, LNS, and PTA is a method of accelerating a subset of broadband aggregation features on the Cisco 7301 and Cisco 7200 VXR routers by enabling fast forwarding software on the second CPU. MPF for Broadband LAC, LNS, and PTA significantly improves performance by up to two times that of a regular Cisco 7301 or Cisco 7206VXR router, without any hardware changes.

For more information, refer to the “Multi-Processor Forwarding (MPF) for Broadband LAC, LNS, and PTA” document at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123ym14/mpf123ym.htm>

New Hardware Features in Cisco IOS Release 12.3(14)YM1

There are no new hardware features supported in Cisco IOS Release 12.3(14)YM1.

New Software Features in Cisco IOS Release 12.3(14)YM1

The following new software feature is supported by the Cisco IOS Release 12.3(14)YM1:

Logical Line ID Blocking

Platforms: Cisco 7200 series routers, Cisco 7300 series routers, and Cisco 7400 series routers

Logical Line ID Blocking enables Service Providers to provide their customers with the capability of enabling Privacy option on their accounts.

This capability needs to be managed by the LAC Router, which will inform other devices in the network as to when this option is enabled.

For more information, refer to the “Logical Line ID Blocking” document at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/products_feature_guides_list.html.

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>

Important Notes

The following sections contain important notes about Cisco IOS Release 12.3(14)YM that can apply to the Cisco 7200 series routers, Cisco 7300 series routers, and Cisco 7400 series routers:

Deferrals

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

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

Field Notices and Bulletins

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

http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/1654_pp.htm

- **Field Notices**—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.
- **Product Bulletins**—If you have an account on Cisco.com, you can find product bulletins at <http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml>. If you do not have a Cisco.com login account, you can find product bulletins at <http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml>.
- *What's Hot in Software Center*—*What's Hot in Software Center* provides information about caveats that are related to deferred software images. If you have an account on Cisco.com, you can access *What's Hot for IOS Releases* at <http://www.cisco.com/kobayashi/sw-center> or by logging in and selecting **Technical Support: Software Center: Cisco IOS Software: What's Hot in Software Center**.
- *What's New for IOS* — *What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml> or by logging into Cisco.com and selecting **Technical Support: Software Center: Products and Downloads: Cisco IOS Software**.

Caveats for Cisco IOS Release 12.3 YM

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 only open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T are also in Cisco IOS Release 12.3(14)YM13.

For information on caveats in Cisco IOS Release 12.3, see *Caveats for Cisco IOS Release 12.3*.

For information on caveats in Cisco IOS Release 12.3 T, see *Caveats for Cisco IOS Release 12.3 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.



Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Service and Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/>.

Table 3 Caveats Reference for Cisco IOS Release 12.3 YM

DDTS Number	Open in Release	Resolved in Release
CSCdy80322		12.3(14)YM11
CSCec10149		12.3(14)YM13
CSCec12299		12.3(14)YM10
CSCec77703		12.3(14)YM13
CSCed94829		12.3(14)YM4
CSCee56309	12.3(14)YM2	
CSCee79019	12.3(14)YM2	
CSCef82993		12.3(14)YM13
CSCef93594		12.3(14)YM13
CSCeg38420		12.3(14)YM6
CSCeg51096		12.3(14)YM4
CSCeg70465		12.3(14)YM2
CSCeg77994	12.3(14)YM2	12.3(14)YM5
CSCeg87396		12.3(14)YM11
CSCeh02624		12.3(14)YM13
CSCeh04006	12.3(14)YM2	
CSCeh11994		12.3(14)YM11
CSCeh13489		12.3(14)YM4
CSCeh37211		12.3(14)YM6
CSCeh47169		12.3(14)YM4

Table 3 Caveats Reference for Cisco IOS Release 12.3 YM (continued)

CSCeh54163	12.3(14)YM2	
CSCeh73049		12.3(14)YM4
CSCeh84894		12.3(14)YM2
CSCeh88425		12.3(14)YM13
CSCeh94148		12.3(14)YM2
CSCei00766		12.3(14)YM12
CSCei13040		12.3(14)YM12
CSCei20231		12.3(14)YM10
CSCei20511	12.3(14)YM2	
CSCei25164		12.3(14)YM2
CSCei40008		12.3(14)YM9
CSCei43744	12.3(14)YM2	
CSCei49288	12.3(14)YM2	
CSCei49931	12.3(14)YM2	
CSCei61732		12.3(14)YM3
CSCei62952		12.3(14)YM12
CSCei73343	12.3(14)YM2	
CSCei74569	12.3(14)YM2	
CSCei74950	12.3(14)YM2	12.3(14)YM5
CSCej04091		12.3(14)YM5
CSCej15751		12.3(14)YM5
CSCej20505		12.3(14)YM10
CSCej64945		12.3(14)YM5
CSCek25330		12.3(14)YM6
CSCek25819		12.3(14)YM6
CSCek26492		12.3(14)YM8
CSCek33777	12.3(14)YM6	
CSCek42751		12.3(14)YM13
CSCek50177		12.3(14)YM11
CSCek58542		12.3(14)YM11
CSCek61276		12.3(14)YM11
CSCin75630	12.3(14)YM2	
CSCin78805		12.3(14)YM13
CSCin86070		12.3(14)YM13
CSCin92031	12.3(14)YM2	12.3(14)YM5
CSCin92814		12.3(14)YM12
CSCin95447		12.3(14)YM13

Table 3 Caveats Reference for Cisco IOS Release 12.3 YM (continued)

CSCsa49922		12.3(14)YM13
CSCsa75784	12.3(14)YM2	
CSCsa77439		12.3(14)YM10
CSCsa86252		12.3(14)YM12
CSCsa86572		12.3(14)YM12
CSCsa86958		12.3(14)YM10
CSCsa87733		12.3(14)YM2
CSCsb06658		12.3(14)YM8
CSCsb11124		12.3(14)YM4
CSCsb24007		12.3(14)YM3
CSCsb25337		12.3(14)YM8
CSCsb31777	12.3(14)YM2	
CSCsb33682	12.3(14)YM2	
CSCsb35565	12.3(14)YM2	
CSCsb39237		12.3(14)YM3
CSCsb62317		12.3(14)YM13
CSCsb63166	12.3(14)YM3	
CSCsb78345		12.3(14)YM12
CSCsb83459		12.3(14)YM13
CSCsc00891		12.3(14)YM5
CSCsc09874		12.3(14)YM5
CSCsc44237		12.3(14)YM6
CSCsc66612		12.3(14)YM11
CSCsc68085		12.3(14)YM6
CSCsc69967	12.3(14)YM6	
CSCsc73532		12.3(14)YM6
CSCsc77704		12.3(14)YM13
CSCsc86307		12.3(14)YM13
CSCsc95588		12.3(14)YM12
CSCsd04677	12.3(14)YM9	12.3(14)YM10
CSCsd08112		12.3(14)YM6
CSCsd08862		12.3(14)YM13
CSCsd20371		12.3(14)YM13
CSCsd28570	12.3(14)YM6	
CSCsd39972	12.3(14)YM6	
CSCsd40334		12.3(14)YM8
CSCsd58381		12.3(14)YM8

Table 3 Caveats Reference for Cisco IOS Release 12.3 YM (continued)

CSCsd75854		12.3(14)YM11
CSCsd81407		12.3(14)YM10
CSCsd95616		12.3(14)YM10
CSCsd98626		12.3(14)YM7
CSCse05642		12.3(14)YM9
CSCse47912		12.3(14)YM8
CSCse56501		12.3(14)YM10
CSCse68138		12.3(14)YM9
CSCse68355		12.3(14)YM10
CSCsf04754		12.3(14)YM9
CSCsf08998		12.3(14)YM10
CSCsg11029		12.3(14)YM10
CSCsg40482		12.3(14)YM10
CSCsg51538		12.3(14)YM10
CSCsg91306		12.3(14)YM12
CSCsh02315		12.3(14)YM11
CSCsh30863		12.3(14)YM11
CSCsh48919		12.3(14)YM13
CSCsh65517		12.3(14)YM11
CSCsh70906		12.3(14)YM10
CSCsh71247		12.3(14)YM11
CSCsh78054		12.3(14)YM10
CSCsi01470		12.3(14)YM10
CSCsi20225		12.3(14)YM10
CSCsi32334	12.3(14)YM11	
CSCsi90974		12.3(14)YM13
CSCsi99217		12.3(14)YM11
CSCsj81502		12.3(14)YM12
CSCsk00177		12.3(14)YM12
CSCsk26719		12.3(14)YM13
CSCsk32150		12.3(14)YM12
CSCsk70446		12.3(14)YM12
CSCsk73104		12.3(14)YM12
CSCsl34280		12.3(14)YM12
CSCsl59294		12.3(14)YM13
CSCsm61105		12.3(14)YM13
CSCsm77199		12.3(14)YM13

Table 3 Caveats Reference for Cisco IOS Release 12.3 YM (continued)

CSCso47627		12.3(14)YM13
CSCso81854		12.3(14)YM12
CSCsq62976		12.3(14)YM13
CSCsr08094		12.3(14)YM13
CSCsr74835		12.3(14)YM13
CSCsu00178		12.3(14)YM13
CSCsu47128		12.3(14)YM13
CSCsu97934		12.3(14)YM13
CSCsv04836		12.3(14)YM13
CSCuk55995		12.3(14)YM6

Open Caveats—Cisco IOS Release 12.3(14)YM13

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM13 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no specific open caveats for Cisco IOS Release 12.3(14)YM13.

Resolved Caveats—Cisco IOS Release 12.3(14)YM13

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM13. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec10149
The router crashes.
This condition is observed when **del recursive** command or **dir recursive** command is run on a directory containing large number of subdirectories and the inner most directory path exceeds 128.
Workaround: Run the **del** and **dir** commands on individual directories.
- CSCec77703
Disk corruption in the router.
This condition is observed when simultaneous disk operations are performed, for example:
 - Two vty sessions accessing disk using CLI commands
 - A router application and a SNMP application simultaneously accessing a disk
 - Two different router applications accessing a disk
 Workaround: There is no known workaround.
- CSCef82993
Authentication fails if the router is configured for CHAP authentication but the peer offers the PAP authentication.

This condition is observed when **aaa new-model** command is configured. In such a case, the PPP acknowledge PAP as an authentication protocol even if there is no **ppp pap sent-username** command configured. The call fails during the authentication phase since there are no credentials to send to the peer.

Workaround: Disable the **aaa new-model** command or configure the **ppp pap refuse** command.

- 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.

Workaround: There is no known workaround.

- CSCeh02624

The router crashed.

This condition is observed when multiple process attempt to lock the same disk for access.

Workaround: There is no known workaround.

- CSCeh88425

The switch fails to boot up properly.

This condition is observed when HTTP client password is configured before reloading the switch using the **ip http client password** command.

Workaround: Remove the **ip http client password** command.

- CSCek42751

The running configuration on the router becomes inaccessible after copying a new configuration file to running configuration.

This condition is observed after rebooting a Cisco router that has an ATA file system.

Workaround: Reboot the router.

- 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.

- CSCin86070

The router, with MFR protocol configured on subinterfaces, displays incorrect bandwidth. The ifSpeed for the subinterfaces returns the value of 100Mbps.

This condition is observed on a Cisco 12000 series router that is configured for MFR.

Workaround: Do not poll the ifSpeed of the subinterface. Instead, poll the ifSpeed of the main interface.

- CSCin95447

Authentication fails if the router is configured for CHAP authentication but the peer offers the PAP authentication.

This condition is observed when **aaa new-model** command is configured. In such a case, the PPP acknowledge PAP as an authentication protocol even if there is no **ppp pap sent-username** command configured. The call fails during the authentication phase since there are no credentials to send to the peer.

Workaround: Disable **aaa new-model** command or configure the **ppp pap refuse** command

- CSCsa49922

The EIGRP internal route remains in the routing table even if:

- The EIGRP internal route is down, and
- The EIGRP internal route is removed from the EIGRP topology table.

This condition is observed when a router has EIGRP internal route and external route as Successor and Feasible Successor respectively for the same network and then the internal route goes down.

Workaround: Do not use both the internal and external EIGRP route for the same network.

- CSCsb62317

The LNS sends acct-stop record with Acct-Terminate-Cause 0.

This condition is observed when ppp terminates by receiving LCP CONFACK at the OPENED status.

Workaround: There is no known workaround.

- CSCsb83459

The router reloads while initiating multiple PPPoE sessions due to insufficient memory or while multiple PPPoE sessions are simultaneously terminated.

This condition is observed on a Cisco router running one of the following software releases:

- Cisco IOS interim Release 12.3(12.5) or a later release
- Cisco IOS interim Release 12.3(12.4)T or a later release
- Cisco IOS Release 12.4 or Release 12.4T.

Workaround: There is no known workaround.

- CSCsc77704

The router hangs and is not accessible through console or telnet.

The reason for this condition is not known.

Workaround: There is no known workaround.

- CSCsc86307

The router crashed when **show interfaces Serial1/1:1 | include (adminlesrlt ratelkets inlkets outlclear)** command is run resulting in a TLB exception.

The condition for this exception not known.

Workaround: There is no known workaround.

- CSCsd08862

A router may crash because of a bus error when the **show interface** command or another command that displays the virtual-access information for a virtual-access interface or subinterface.

This condition is observed while clearing a session that is associated with the virtual-access interface or subinterface.

Workaround: There is no workaround.

- CSCsd20371

The router crashes when conditional debug option is removed from vty port while running the **show debug condition** command on the console pport.

This condition is observed when the above two operations are performed simultaneously.

Workaround: Avoid running these two operations simultaneously.
- CSCsh48919

With an ATA flash card, the **dir disk0:** command fails if any filename or directory name stored on disk0 contains embedded spaces. This applies to disk1 or disk2 as well. This situation can also occur with a compact flash (CF) card when the **dir flash:** command is used.

This condition is observed for removable flash card such as ATA flash card that are fomrmatted to use DOSFS.

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 adjacency 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.
- CSCsk26719

The router crashed on deleting an ACE(rule) when the **show ip access-list output** command is run using another session.

This condition is observed when next to next ACE(rule) that is about to be displayed using **show ip access-list** command is deleted via another vty/console.

Workaround: Avoid holding up the **show ip access-list output** command in prompt and delete the access control entry(rules) that are about to be displayed.
- CSCsl59294

A Cisco router may show 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 on a Cisco 2811 router running Cisco IOS Release 12.4(13d).

Workaround: Disable the following configuration on the router:

 - **voice hpi capture buffer size**
 - **voice hpi capture destination filename**
- CSCsm61105

The router crashed due to bus error when PPTP is configured after removing virtual-template interfaces under ATM.

This condition is observed when:

Number of PPPoE and PPPoEoA sessions exceed 3000.

You run **configure no interface virtual-template number** under ATM interfaces command.

Workaround: There is no workaround.

- CSCsm77199

The switch shows error message after initializing the supervisor.

This condition is observed when the HTTPS server capability is enabled.

Workaround: Remove the HTTPS server capability using **configure no ip http server** command.

- CSCso47627

Router crashes while performing the simultaneous operation in **pvc-in-range 0/32** and **vc-class atm word** command.

Workaround: There is no known workaround.

- CSCsq62976

The Router may crash when clearing vpdn l2tp tunnels.

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

Workaround: There is no known workaround.

- CSCsr08094

The vpdn process ignores udp checksum of l2tp control packet under the configuration command, **vpdn ip udp ignore checksum**.

This condition is observed when **vpdn ip udp ignore checksum** command is enabled.

Workaround: There is no workaround.

- CSCsr74835

Potential overflow of the destination buffer due to unspecified bounding length in the **sprintf** command.

Workaround: There is no known workaround.

- CSCsu00178

Range pvc is not created under point to point sub interface.

This condition is observed only on a point to point sub interface.

Workaround: There is no known workaround.

- CSCsu47128

The router crashes due to the storm of error log message on the console.

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

Workaround: There is no known workaround.

- CSCsu97934

NPE-G1 crashed after **pppoe_sss_holdq_enqueue** function.

Workaround: Run **deb pppoe error** command.

- 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>.

Open Caveats—Cisco IOS Release 12.3(14)YM12

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM12 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no specific open caveats for Cisco IOS Release 12.3(14)YM12.

Resolved Caveats—Cisco IOS Release 12.3(14)YM12

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM12. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei00766

A router crashes when the encapsulation is set to the Point-to-Point Protocol (PPP) and removed repeatedly.

This condition occurs on a Cisco router that runs Cisco IOS Release 12.3 or Release 12.4 and is configured for the PPP Link Control Protocol (LCP).

There are no known workarounds.

- CSCei13040

When an Open Shortest Path First (OSPF) neighbor comes back up after a very fast (sub-second) interface flap, OSPF routes that were learned through the interface that flapped may not be re-installed in the Routing Information Base (RIB).

This condition is observed when the following two events occur:

- The interface flaps very quickly.
- The neighbor comes back up before the Link-State Advertisement (LSA) generation timer expires.

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

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

- CSCei62952

A Cisco device running Cisco IOS may drop traffic because the routing table and the Cisco Express Forwarding (CEF) forwarding table are inconsistent.

This rare condition occurs when the routing table is reloaded by clearing the routing table or the forwarding complex (PXF) is reset on a box that supports hardware forwarding.

There are no known workarounds.

- CSCin92814

A router crashes when you enter the **no ip vrf vrf-name** global configuration command.

This condition occurs only when you remove the VRF configuration immediately after removing VRF forwarding from an interface.

Workaround: Wait 60 seconds between removing VRF forwarding from the interface and removing the VRF configuration.

- CSCsa86252

When **write memory** is entered from the console connection while **show startup-config** is entered from a Telnet connection, the configuration is deleted. The old configuration has the [D] flag, and the new configuration has a length of 0.

This condition occurs when the configuration is large or the boot configuration is in slot 0.

Workaround: Undelete the configuration file and save it in the NVRAM.

- CSCsa86572

A large configuration in NVRAM on a primary or secondary RSP may become corrupted and the router may generate relevant warning messages during the execution of a **copy system:running-config nvram: startup-config** command. When you erase NVRAM by entering the **erase nvram** command and then enter the **copy system:running-config nvram: startup-config** command, the router may crash.

Workaround: If the configuration file is significantly large, place a copy of the configuration file on a flash card or disk with ample space and enter the **boot config slot0:startup-config** command to force the startup configuration file to be read from the flash card. When you enter the **copy system:running-config nvram: startup-config** command, the current running configuration is saved to the flash card or disk and the configuration is auto-synchronized to the corresponding flash card on the secondary RSP.



Caution

Do not remove the flash card while the **boot config slot0:startup-config** command is being executed.

- 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 **show mls cef ipv6** command, or wait 60 seconds after making the cost change before entering the **show ipv6 cef** command.

- CSCsc95588

A Cisco router reloads when you enter the **show log**, **show interface**, or **show caller** command.

This condition can occur when Point-to-Point Protocol (PPP) sessions go down while the output of a **show** command is suspended.

There are no known workarounds.

- 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>.

- CSCsj81502

The output of the **show pagp neighbor** command may truncate the neighbor device name and port name fields by one character. This issue is just a display issue and has no functional impact on the Port Aggregation Protocol (PAgP).

This condition only affects PAgP EtherChannel member ports.

Workaround: There are no known workarounds at this time. To find out the partner's correct information, use the **show cdp neighbor** command.

- CSCsk00177

Generic Routing Encapsulation (GRE) traffic needs to be specifically allowed on the outside interface terminating Dynamic Multipoint VPN (DMVPN) IPsec protected traffic.

This condition occurs on a DMVPN tunnel interface with tunnel protection IPsec, Cisco Express Forwarding (CEF), or fastswitching.

Workaround: Use process switching or allow the GRE traffic.

- 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.

- CSCsk70446

A traceback occurs when long URLs are used to configure a device using the Cisco IOS HTTP web parser. The device does not crash.

This condition occurs when you try to configure commands that have a single keyword or parameter greater than N characters in length using the web-based Cisco IOS command parser. The value of N that causes a traceback is release-dependent as follows:

- 50 for Cisco IOS Release 12.0 and later releases
- 128 for Cisco IOS Release 12.2 and later releases
- 256 for Cisco IOS Release 12.2(25) and later releases

Workaround: Avoid using the web-based command line parser for CLI commands with long keywords or arguments.

- 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>

- CSCs134280

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). The GigabitEthernet Interface 0/0 used to terminate the Layer 2 Tunneling Protocol (L2TP) tunnels is not affected by the TX underruns.

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.

- CSCso81854

Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml>.

This security advisory is being published simultaneously with announcements from other affected organizations.

Open Caveats—Cisco IOS Release 12.3(14)YM11

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM11 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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.
```

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

There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(14)YM11

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM11. 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.

- CSCeh11994
The reply from an L2TP network server (LNS) to an L2TP access concentrator (LAC) may be delayed.
This condition occurs on a Cisco router that is configured as an LNS and that has several tunnels to different LACs.
There are no known workarounds.
- CSCek50177
A large blank space displays in the output of **show 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.
- CSCsc66612
A Cisco router configured for Virtual Private Dialup Network (VPDN) may unexpectedly reload with a bus error.
This condition occurs on a Cisco7200VXR series router equipped with an NPE-G1 processor card and is preceded by "SYS-2-INPUT_GETBUF: Bad getbuffer" error messages.
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 is used in the PADI packet.
- 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.
This message might only be seen in bootloader images that contain the diffs of CSCin64354.
```

- CSCsh65517

Applying an IPv6 access-list to a Cisco router does not work immediately.

This condition is the result of changes to the adjacency code introduced in the recent 12.0S code with CSCek61276.

Workaround: Perform a **shut/noshut** of the interface.

- 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.

- 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.

Open Caveats—Cisco IOS Release 12.3(14)YM10

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM10 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no specific open caveats for Cisco IOS Release 12.3(14)YM10.

Resolved Caveats—Cisco IOS Release 12.3(14)YM10

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM10. 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>.

- CSCei20231

An L2TP network server (LNS) configured with a small receive window size causes the L2TP access concentrator's (LAC's) `unsentQ` to fill. The LAC does not process the `unsentQ` enough to drain the queue rapidly or in a timely manor. Instead, it only drains when the `resendQ` is processed or when a valid control message is received from the peer. If the peer is not sending control messages, then the `unsentQ` is only processed when the `resendQ` is processed, which can be as frequent as 1 second intervals, or longer, if the `resendQ` processing is backing off due to congestion.

This condition occurs with a call rate of about 20 calls per second with `RWS = 4` set on the LNS. The LAC puts the majority of the packets within the `unsentQ` and there are no new calls established.

There are no known workarounds besides using a lower call rate or a higher receive window size (`RWS`) on the LNS.

- CSCej20505

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>

- CSCsa77439

A Cisco L2TP network server (LNS) running Cisco IOS release 12.3(4)T or later releases of Cisco IOS does not respond to a challenge in the L2TP Start Control Connection Request (SCCRQ) correctly when the **no l2tp tunnel authentication** command is configured under the vpdn-group.

Workaround: Re-enable tunnel authentication.

- CSCsa86958

Currently, the CISCO-IP-LOCAL-POOL-MIB offers one notification to indicate when the number of free addresses in an IP local pool are running low. To send the notification, the user has to set up two threshold values: cIpLocalPoolStatInUseAddrThldLo and cIpLocalPoolStatInUseAddrThldHi. When the number of used addresses exceeds the cIpLocalPoolStatInUseAddrThldHi value, a notification is sent out. However, the MIB will not send a notification again until the number of used addresses goes below the cIpLocalPoolStatInUseAddrThldLo value.

This behavior presents an inconvenience because the number of addresses can be increased or decreased as necessary, and therefore, the threshold values need to be change accordingly. The customer requests notification to be based on a percentage, instead of an absolute number, of used address in an IP local pool

Workaround: The network management application can compute the percentage values every time the total number of address changes in an IP local pool and adjust the values of cIpLocalPoolStatInUseAddrThldLo and cIpLocalPoolStatInUseAddrThldHi.

- CSCsd04677

A Cisco 7200 series router experiences a CPU memory crash after 8 weeks of continuous Context-Based Access Control (CBAC) session flaps.

Workaround: Increase CPU memory with the **sw-module heap cp xx** command, or reboot the router within the 8-week period.

- CSCsd81407

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsd95616

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

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

- CSCse56501

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>.

- CSCse68355

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>

- CSCsf08998

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>

- CSCsg40482

ISDN L2 may remain in the "TEI_ASSIGNED" state.

This condition occurs on a Cisco router after you perform a hard online insertion and removal (OIR) of a PA-MC-4T1 port adapter. After the condition occurs, you must reload the router.

Workaround: There are no known workarounds.

- CSCsg51538

A router acting as an L2TP access concentrator (LAC) with remote-end customer PCs crashes with a bus error.

There are no known workarounds.

- CSCsh11029

A CPU1 memory leak occurs after repeated Context-Based Access Control (CBAC) session flapping.

This condition occurred after 1000 CBAC sessions flapped. Memory was exhausted after a period of 2 days. The problem typically occurs after 8 weeks of continuous CBAC session flaps and has been seen on the YM9 and YM 8 images.

Workaround: Increase CPU memory with the **sw-module heap fp xx** command.

- CSCsh70906

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

This condition occurs when there are a lot of session establish requests for the Point-to-Point Protocol over Ethernet (PPPoE).

There are no known workarounds.

- CSCsh78054

IP Local Pool Trap messages for Hi and Low Notification do not include the length field for the specific Pool name in each object of that Trap; SNMP Get/Walk does include the length field for the specific pool and displays properly.

Workaround: Configure the "Ip local pool" with high and low threshold values. For example:

```
Router (conf t)# ip local pool pool-name ip-low ip-high threshold low high
```

- CSCsi01470

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>CSCsi20225

Continuous trace backs are seen on the L2TP network server (LNS) on a Cisco 7201 router. These trace backs occur continuously while bringing up PPP over X(PPPoX)/Layer 2 Tunnel Protocol (L2TP) sessions and can occur with just a few hundred sessions. There are no unusual CPU spikes, which you might expect with this behavior.

This condition occurs when you bring up PPPoX sessions continuously over multiple tunnels. There is no traffic flowing, and this condition does not seem to impact performance.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(14)YM9

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM9 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsd04677

An MPF-enabled L2TP network server (LNS) with 1GB memory crashed with the error code: %FF-2-NOMEMORY: No memory available on CPU 0.

This condition occurred while running Cisco IOS Release 12.3(14)YM5 on a c7200 with 1GB memory and the following configured features: RADIUS, simple Virtual access interface (VAI) policing via the Modular QoS CLI (MQC), and Layer 2 Tunnel Protocol (L2TP). The LNS crashed after an uptime of 2w0d with 4K subscribers pushing 120mbps and with roughly a 20% CPU load on both CPUs.

There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(14)YM9

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM9. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei40008

An incorrect NAS-Port value is showing at the L2TP network server (LNS).

This condition occurs when configuring the Layer 2 Tunnel Protocol (L2TP) and the L2TP access concentrator (LAC) (uut) and LNS are configured with "vpdn aaa attribute nas-port vpdn-nas" and "radius-server attribute nas-port format d".

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.

- 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-snmv3.shtml>

Open Caveats—Cisco IOS Release 12.3(14)YM8

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM8 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no specific open caveats for Cisco IOS Release 12.3(14)YM9.

Resolved Caveats—Cisco IOS Release 12.3(14)YM8

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM8. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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>

- CSCsb06658

A vulnerability exists in certain Cisco IOS software release trains running on the Cisco IAD2400 series, Cisco 1900 series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.

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

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060920-docsis.shtml>.

- 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>

- CSCsd40334

Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

Cisco has made free software available to address this vulnerability for affected customers.

There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml>

- 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>

- CSCse47912

An MPF-enabled Cisco 7200 or 7301 Series router running the Cisco IOS 12.3(14)YM image does not generate the Internet Control Message Protocol (ICMP) unreachable message with the "DF set fragmentation needed" code for incoming packets larger than the maximum transmission unit (MTU) of the outgoing interface.

Workaround: Use the Transmission Control Protocol (TCP) Maximum Segment Size (MSS) adjust feature to avoid fragmentation.

Open Caveats—Cisco IOS Release 12.3(14)YM7

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM7 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no specific open caveats for Cisco IOS Release 12.3(14)YM7.

Resolved Caveats—Cisco IOS Release 12.3(14)YM7

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM7. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsd98626

An MPF-enabled router drops packets whose source interface is the same as its destination.

This condition occurs when there is high traffic at less than the line rate.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(14)YM6

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM6 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek33777

The **test sw-module show mem** command displays both the CPU0 (MPF control plane) and CPU1 (MPF data plane) heap use by default.

CLI options include the following:

```
test sw show mem [detail]
test sw show mem cpu0 [detail]
test sw show mem cpu1 [detail]
```

There are no known workarounds.

- CSCsc69967

A router software-forced reload occurs in Breakpoint exception.

This condition occurs when testing PA-A6-OC3 OIR.

There are no known workarounds.

- CSCsd28570
When using the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Devices not using the AAA command authorization feature, or that do not support TCL functionality, are not affected by this vulnerability.

This vulnerability is present in all versions of Cisco IOS that support the **tcsh** command.

Workaround: This advisory with appropriate workarounds is posted at <http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>
- CSCsd39972
Negative counter values are seen in the **show mpf interface** command.

This condition occurs when large packet sizes (~1518) are sent in an IPv6 environment. The traffic rate must be above the rate Multi-Processor Forwarding (MPF) can handle.

Workaround: Use the **show interface Gig** to check the counter values.

Resolved Caveats—Cisco IOS Release 12.3(14)YM6

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM6. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg38420
No IPv6 adjacency is seen on a Frame Relay point-to-point interface.

This condition occurs when configuring an IPv6 address on a Frame Relay point-to-point interface running Cisco IOS release 12.3, 12.3T or 12.2SX.

Workaround: Use **shut, no shut** on the interface.
- CSCeh37211
Spurious access errors are generated when the **show interface port-channel 1** command is used. The errors occur only if the Gigabit Ethernet interface is part of port-channel.

There are no known workarounds.
- CSCek25330
Traffic does not flow in the setup on the L2TP access concentrator (LAC)---Client connection. The Tx locks up after 5 retries during the GigEth Tx underflow.

This condition occurs when bidirectional traffic is sent in a hair pinning setup.

There are no known workarounds.
- CSCek25819
The **show interface accounting** exec command for virtual-access is not working correctly. The “Pkts In” counter of Virtual-Access decreases step by step.

This condition occurs when using the virtual-access interface.

There are no known workarounds.

- CSCsc73532

The router may unexpectedly reload under high loads.

This condition occurs when the Embedded Syslog Manager (ESM) is used to modify syslog messages and a large number of messages are generated. The content of the script may have an influence on the probability of the unexpected reload.

There are no known workarounds.

- CSCsc44237

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

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

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

Condition 1: This condition occurs on a Cisco switch or router that runs a Cisco IOS software image and that contains the fixes for caveats CSCeh04646 and CSCeb30831. A list of the affected releases can be found at:

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh04646> and

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb30831>

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

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

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

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

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

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef50104>.

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

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

- CSCsc68085

There is an Input Queue drop when Cisco 7206 with NPE-G1 functions as L2TP network server (LNS).

This condition occurs when Multi-Processor Forwarding (MPF) is enabled.

Workaround: Disable MPF.

Alternative workaround: Ignore the incorrect input queue drop counts. The problem is due to the reporting any MPF drops as input queue drops. Use the **show mpf punt** or **show mpf int** command to confirm if detailed MPF drops are occurring.

- CSCsd08112

When clearing the vaccess interface of an active user with IOS firewall configured, the router unexpectedly reloads or hangs indefinitely.

This condition can occur even when only a small number of users with IOS firewall are configured and they are generating only a small amount of traffic.

There are no known workarounds.

- CSCuk55995

The CEFv6 interface configuration may be lost after a reload.

This condition occurs on a Cisco router running IPv6 CEF.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(14)YM5

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no specific open caveats for Cisco IOS Release 12.3(14)YM5.

Resolved Caveats—Cisco IOS Release 12.3(14)YM5

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg77994

A L2TP access concentrator (LAC) does not send an Accounting-Start RADIUS record to a RADIUS server for a user session.

This condition occurs on a Cisco platform that functions as a LAC and that runs Cisco IOS Release 12.3(14)T1 when a switchover occurs from one L2TP network server (LNS) to another LNS while the user session is brought up.

There are no known workarounds.

- CSCei74950

Traffic is dropped as glean drops, when sent across the next hop, with static routes. Traffic processes properly if routing protocols are configured.

The condition occurs only when static routes are involved.

Workaround: Ping the next hop before sending traffic across it.

- CSCej04091

CPU spikes are observed periodically on CPU1 at 40% CPU load or above, resulting in a few packets dropped.

This condition occurs when IPv4 and ACL are configured.

There are no known workarounds.

- CSCej15751

Certain Multi-Processor Forwarding (MPF) configurations may perform at less than 2x of Cisco IOS performance when compared to the current Cisco IOS performance under the same configurations. The reason is that MPF performance was originally designed to perform at 2x of Cisco IOS performance, and cannot take into account the fact that Cisco IOS performance has improved recently.

- CSCej64945

If the L2TP access concentrator (LAC) receives STOPCCN from L2TP network server (LNS) without receiving a Start Control Connection Reply (SCCRP) beforehand, the LAC responds with a Zero-Length Body Acknowledgement (ZLB ACK) containing no tunnel ID information.

There are no known workarounds.

- CSCin92031

A Cisco 7200 or Cisco 7301 router running the Multi-Processor Forwarding (MPF) code might show the following message when there are many fragmented packets:

```
%FF-3-BADADDBYTES: add_bytes_to_particle_pak length
```

There are no known workarounds.

- CSCsc00891

The IP Input process accumulates memory, even with an image that contains the repair for CSCec87860.

This condition occurs when a system is configured with Embedded Syslog Manager (ESM) to modify syslog messages using a Tool Command Language (TCL) script. The actual trigger that starts the memory leak is not yet known.

To identify this problem, look for the string “ESM 28-Byte” in the output of the **show mem sum** command. If a large number of entries like this exist and IP Input memory is increasing, you may have found the problem.

Workaround: If ESM is needed, there are no known workarounds.

- CSCsc09874

The “Input drop” counter in the **show interface** command is double-counting the “RX sbeth bad descriptors”.

This condition occurs under heavy traffic loads that cause RX drops and bad RX descriptor.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(14)YM4

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no specific open caveats for Cisco IOS Release 12.3(14)YM4.

Resolved Caveats—Cisco IOS Release 12.3(14)YM4

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed94829

Multiple Cisco products contain vulnerabilities in the processing of IPsec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) “PROTOS” Test Suite for IPsec and can be repeatedly exploited to produce a denial of service.

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

This advisory is posted at

<http://www.cisco.com/warp/customer/707/cisco-sa-20051114-ipsec.shtml>.

- CSCeg51096

Traceback is seen on the tandem gateway when Cisco CallManager (CCM) calls a Cisco Call Manager Express (CME) phone and the CME phone picks up.

This condition occurs in the following setup:

```
CCM -IP- tandem -IP- CME(2651)
```

There are no known workarounds.

- CSCeh13489

A Cisco router may reset its Border Gateway Protocol (BGP) session.

This condition occurs when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

Workaround: Configure the **bgp maxas limit** command in such a way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

- CSCeh47169

A Cisco router that contains the fix for CSCef84400 may experience a reload due to memory corruption in I/O memory when using telnet, reverse telnet, rsh or other vty based applications, such as accessing service-modules.

This condition occurs on a Cisco 2851, Cisco 3745, and Cisco 3845.

There are no known workarounds.

- CSCeh73049

A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Devices that are not running AAA command authorization feature, or do not support TCL functionality, are not affected by this vulnerability.

This vulnerability is present in all versions of Cisco IOS that support the **telsh** command.

Workaround: This advisory with appropriate workarounds is posted at

<http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>

- CSCsb11124

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

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

Cisco has published a Security Advisory on this issue; it is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>

Open Caveats—Cisco IOS Release 12.3(14)YM3

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsb63166

In Cisco IOS Release 12.3(15) or Cisco IOS Release 12.3(8)T6 and later, the **transport input all** command is not shown in the configuration and is not written to NVRAM. This will cause the router to default to **transport input none** when the router is rebooted.

This condition occurs in feature sets which do not contain the UDP Telnet (UDPTN) feature (non-enterprise images).

Workaround: Configure explicitly all the transports you want to allow. For example, **transport input telnet ssh**.

Resolved Caveats—Cisco IOS Release 12.3(14)YM3

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei61732

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

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

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

- CSCsb24007

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>

- CSCsb39237

When using a Cisco 3845 router with IOS 12.4 and the **show ip inspect statistics** command, the number for the half-open session will keep increasing and never decrease. If it reaches the maximum number limit for half-open sessions, then no one can establish any new Secure Socket Layer (SSL) session. It can also cause an unexpected reload of the router.

This condition occurs on a Cisco 3845 router with IOS 12.4 (1). This condition has also been seen when Internet Control Message Protocol (ICMP) inspection is enabled with the **ip inspect name name icmp** command.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(14)YM2

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCee56309

Two MPi Border Gateway Protocol (BGP) peers with next-hop-self configured will fall in different update-groups. This will cause some convergence slowdown in this corner case.

There are no known workarounds.

- CSCee79019

The **ip mtu adjust** command incorrectly sets the Point-to-Point Protocol (PPP) Maximum Received Unit (MRU).

This condition occurs when the **ip mtu adjust** command is configured under a vpdn-group.

Workaround: Explicitly set the maximum transmission unit (MTU) for the vpdn-group.

- CSCeg77994

An L2TP access concentrator (LAC) does not send an Accounting-Start RADIUS record to a RADIUS server for a user session.

This condition occurs on a Cisco platform that functions as a LAC and runs Cisco IOS Release 12.3(14)T1, when a switchover occurs from one L2TP network server (LNS) to another LNS while the user session is brought up.

There are no known workarounds.
- CSCeh04006

A Point-to-Point Protocol over Ethernet (PPPoE) session in an L2TP access concentrator (LAC) cannot be created on a Gigabit Ethernet interface.

In a LAC router configuration, if there is a VLAN configured under a Gigabit Ethernet interface, then it is not possible to create a PPPoE session on the main Gigabit Ethernet interface.

Workaround: Either remove the VLAN from the Gigabit Ethernet interface and create a PPPoE session, or create a PPPoEoVlan session instead as per required.
- CSCeh54163

Setting qos-group on input policy-map inhibits all output classifications.

When applying qos-group on the packets coming inside the box, the packets will not be classified on the output direction.

There are no known workarounds. Presently, this feature is disabled and ignored in the Multi-Processor Forwarding (MPF) Path. However, it works in Punt Path.
- CSCei20511

When using indirect routing (some routing protocol on the nonDR), the router does not fast switch or fast drop the multicast packets.

This condition occurs if Open Shortest Path First (OSPF), or some other routing protocol on a router, is configured between some multicast destination and a source. When this happens, the nonDR router might not fast switch / fast drops the packets correctly.

There are no known workarounds.
- CSCei43744

cpu-hog is seen on an atm sub interface in which 900 active sessions are deleted from the router config.

This condition occurs if the ATM subinterface config is removed after lots of active Point-to-Point Protocol (PPP) sessions.

Workaround: Shut down the ATM PA before deleting ATM subinterface from the router configuration.
- CSCei49288

The Layer 2 Tunnel Protocol (L2TP) ToS reflection feature does not work for L2TP multicast data traffic.

This condition occurs when an L2TP user is getting Multicast data traffic.

There are no known workarounds.

- CSCei49931

The **show policy-map session output** does not show any output.

This condition occurs when shaping policy is configured on the Home gateway, and the session is established. The traffic is sent but, when the **show policy-map session** command is sent, no output is reported.

There are no known workarounds.

- CSCei73343

Dynamic changes done to the policy-map or class-map can cause the router to unexpectedly reload or cause classification failures.

This condition occurs with any kind of dynamic changes such as, changing police values with traffic flowing, changes to the class-map match statements, or unconfiguring and configuring of policy map values, and can cause the router to unexpectedly reload or cause classification failures. These dynamic changes refer to when traffic is flowing or when sessions are up.

There are no known workarounds. It is advised to make changes by stopping the traffic (in case of the sessions bringing down the sessions) then making the changes. The best course of action would be to make the changes and reload the router with the saved changes.

- CSCei74569

The following Internet Control Message Protocol (ICMP) unreachable message is not sent by Multi-Processor Forwarding (MPF):

```
Frag needed DF bit set
```

This condition occurs when a packet that requires fragmentation has DF bit set in the IP header.

There are no known workarounds.

- CSCei74950

When traffic is sent across the next hop, traffic is dropped as glean drops with static routes. There is no problem if there is routing protocols.

This condition only occurs when static routes are involved.

Workaround: Ping the next hop before sending traffic across it.

- CSCin75630

A 7200VXR router with NPE-G1 unexpectedly reloads while booting. This only occurs with the Cisco7XI releases and the Cisco YM releases.

This condition only occurs when the IO memory size is configured as 128Mb

Workaround: Do not configure IO memory size as 128Mb.

- CSCin92031

A 7200/c7301 router running the Multi-Processor Forwarding (MPF) code may display the following message:

```
%FF-3-BADADDBYTES: add_bytes_to_particle_pak length
```

This message occurs when there are lots of packets for fragmentation.

There are no known workarounds.

- CSCsa75784
A 7200VXR router running the 12.3T images may show a spurious memory access messages. This condition occurs when configuring the Ip-prefix list command on the global configuration. There are no known workarounds.
- CSCsb31777
Classification fails if class-maps are modified to match the same traffic type. This condition occurs when you apply the policy map with two or more class-maps matching the same traffic pattern to an interface. As desired, the first class map will match the traffic. However, if you attempt to dynamically change the class-map match statements, the classification fails, as both class-maps start matching the traffic instead of just the first one.
Workaround: To make changes to the class-maps dynamically, remove the policy-map configuration and re-configure it after the changes for class-map are done.
- CSCsb33682
When the L2TP access concentrator (LAC) is configured to suppress sending the Logical Line ID (LLID) string to the L2TP network server (LNS), LLID is not getting suppressed. However, it is still being sent to the LNS.
This condition occurs only when LLID is enabled in the LAC and the **vpdn l2tp attribute clid mask-method remove** command is configured in the global configuration mode, or the **l2tp attribute clid mask-method remove** command is configured in vpdn configuration mode
Workaround: Use RADIUS to suppress the LLID by configuring the avpair for suppressing LLID in the RADIUS profiles.
- CSCsb35565
Action under the default class after dynamic policy config change does not work. This condition occurs if a service-policy is installed with a classmap with an action and a class-default without an action. The initial classmap works fine. When the classmap is deleted and an action is added onto the class-default, the new class-default action is not performed.
Workaround: Reboot the router to have a working policy-map classmap deletion change.

Resolved Caveats—Cisco IOS Release 12.3(14)YM2

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg70465
There is no Quality of Service (QoS) classification at a main interface when packets are switched from a Generic Routing Encapsulation (GRE) tunnel that also has a QoS policy enabled. This condition occurs on a Cisco platform running Cisco IOS Release 12.3T or Release 12.4, when a QoS policy is enabled on both the GRE tunnel and the main interface in the output direction. The condition may also occur in other releases.
Workaround: Move the complete QoS configuration to the QoS policy on the main interface (that is, use an hierarchical policy).

- CSCeh84894
L2TP Multihop traffic is not MPF-switched but is instead punted to IOS.
This condition occurs when the VPDN source ip is present in Multihop node configuration.
Workaround: Remove the **vpdn source ip** command from multihop node configuration.
- CSCeh94148
If uRPF configuration “ip verify unicast ...” is applied to an MPF-accelerated Gigabit Ethernet main interface and the router’s client ARP entry is removed from the routers ARP table, the client packets received by the router will be dropped.
Workaround: The router’s ARP table must have a valid client ARP entry to allow uRPF to work on a main interface. This can be accomplished by any of the following:
 - Router pings the client to force the router to perform an ARP resolution of the client’s IP address.
 - Client pings the router to force the router to perform an ARP resolution of the client’s IP address.
 - Enable a routing protocol to force the router to perform an ARP resolution of the client’s IP address.
- CSCei25164
A Cisco 7000 series router may unexpectedly reload because of a bus error exception and may report CPUHOG message when performing an Online Insertion and Removal (OIR) of an ATM PA-A3 or ATM PA-A6 port adapter.
This condition occurs on a Cisco 7000 series router running Cisco IOS Release 12.3 with PVC auto-provisioning enabled on the ATM PA-A3 or ATM PA-A6 port adapter, and when many Point-to-Point Protocol (PPP) sessions are in transition.
There are no known workarounds.
- CSCsa87733
Only the first syslog server defined on a system receives syslog messages.
This condition occurs when more than one syslog server is defined on a router and when the **logging source-interface xxx.xxx** command is in place.
Workaround: For those logging hosts impacted (i.e. if their message counts are not changing), then enter **no logging source-interface xxx.xxx** and then re-enter **logging 1.1.1.1** type command for each configured host.

Open Caveats—Cisco IOS Release 12.3(14)YM1

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YM1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no specific open caveats for Cisco IOS Release 12.3(14)YM1.

However, Cisco IOS Release 12.3(14)YM1 will inherit all open caveats from Cisco IOS Release 12.3(14)T

For additional information on Cisco IOS Release 12.3(14)T caveats, please refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123t/123tcavs.htm>

Resolved Caveats—Cisco IOS Release 12.3(14)YM1

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YM1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.3(14)YM1.

Related Documentation

The following sections describe the documentation available for the Cisco 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 49](#)
- [Platform-Specific Documents, page 50](#)
- [Feature Modules, page 51](#)
- [Cisco Feature Navigator, page 51](#)
- [Cisco IOS Software Documentation Set, page 51](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.3*

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

Technical Documents

- *Caveats for Cisco IOS Release 12.3*

As a supplement to the caveats listed in “[Caveats for Cisco IOS Release 12.3 YM](#)” in these release notes, see *Caveats for Cisco IOS Release 12.3* and *Caveats for Cisco IOS Release 12.3 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Caveats

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Caveats



Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/bugtool.shtml>.

Platform-Specific Documents

These documents are available for the Cisco 7000 family of routers on Cisco.com and the Documentation CD-ROM:

- *Cisco 7000 User Guide*
- *Cisco 7000 Hardware Installation and Maintenance*
- *Cisco 7010 User Guide*
- *Quick Start Guide Cisco 7100 Series VPN Router*
- *Cisco 7200 VXR Installation and Configuration Guide*
- *Cisco 7200 Routers Quick Start Guide*
- *Cisco 7206 Installation and Configuration Guide*
- *Cisco 7204 Installation and Configuration Guide*
- *Quick Reference for Cisco 7204 Installation*
- *Cisco 7202 Installation and Configuration Guide*
- *Cisco 7301 Installation and Configuration Guide*
- *Network Processing Engine and Network Services Engine Installation and Configuration*

On Cisco.com at:

Technical Documents: All Product Documentation: Core/High-End Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: All Product Documentation: Core/High-End Routers

Feature Modules

Feature modules describe new features supported in Cisco IOS Release 12.3(14)YM 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:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: New Feature Documentation

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 software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

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

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

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

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

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 Releases 12.3: Instructions and Guides

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

Cisco IOS Software: Cisco IOS Release 12.3: Configuration Guides and Command References

Cisco IOS Release 12.3 Documentation Set Contents

Table 4 lists the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form if ordered.



Note

You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at:

Products and Services: Cisco IOS Software: Cisco IOS Releases 12.3: Instructions and Guides

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

Cisco IOS Software: Cisco IOS Release 12.3

Table 4 Cisco IOS Release 12.3 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> • <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2: Bridging</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2: IBM Networking</i> 	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Technologies Configuration Guide</i> • <i>Cisco IOS Dial Technologies Command Reference</i> 	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface and Hardware Component Configuration Guide</i> • <i>Cisco IOS Interface and Hardware Component Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces

Table 4 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS IP Configuration Guide</i> • <i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> • <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> • <i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i> • <i>Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility</i> 	<ul style="list-style-type: none"> IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	<ul style="list-style-type: none"> AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	<ul style="list-style-type: none"> Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Voice Configuration Library</i> • <i>Cisco IOS Voice Command Reference</i> 	<ul style="list-style-type: none"> Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	<ul style="list-style-type: none"> Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	<ul style="list-style-type: none"> AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	<ul style="list-style-type: none"> Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation

Table 4 **Cisco IOS Release 12.3 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Mobile Wireless Configuration Guide</i> • <i>Cisco IOS Mobile Wireless Command Reference</i> 	General Packet Radio Service
<ul style="list-style-type: none"> • <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i> 	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Software System Messages</i> 	

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments regarding Cisco IOS software release notes and caveats documentation to relnote-feedback@cisco.com.

You can submit e-mail comments about technical 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

<http://www.cisco.com/tac>

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- 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 online at this URL:
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed 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 49.

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)

Copyright © 2008
Cisco Systems, Inc.
All rights reserved.

