



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

January 24, 2007

Cisco IOS Release 12.3(7)XI4

OL-6248-05

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.3(7)XI4. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(7)XI4, see the [“Caveats for Cisco IOS Release 12.3 XI” section on page 10](#) 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 7](#)
- [MIBs, page 9](#)
- [Caveats for Cisco IOS Release 12.3 XI, page 10](#)
- [Related Documentation, page 38](#)
- [Obtaining Documentation, page 43](#)
- [Obtaining Technical Assistance, page 44](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(7)XI4 and includes the following sections:

- [Memory Recommendations, page 2](#)
- [Supported Hardware, page 5](#)
- [Determining the Software Version, page 5](#)
- [Upgrading to a New Software Release, page 5](#)
- [Feature Support, page 5](#)

Memory Recommendations

Table 1 *Memory Recommendations for the Cisco IOS Release 12.3(7)XI4*

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	IP Standard Feature Set	IP	c7200-is-mz	48 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	48 MB	128 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7200-p-mz	48 MB	128 MB	RAM
Cisco 7301 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	256 MB	RAM
			c7301-i12s-mz	64 MB	512 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7301-p-mz	64 MB	256 MB	RAM

Table 2 *Memory Recommendations for the Cisco IOS Release 12.3(7)XI3*

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	IP Standard Feature Set	IP	c7200-is-mz	48 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	48 MB	128 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7200-p-mz	48 MB	128 MB	RAM
Cisco 7301 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	256 MB	RAM
			c7301-i12s-mz	64 MB	512 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7301-p-mz	64 MB	256 MB	RAM

Table 3 *Memory Recommendations for the Cisco IOS Release 12.3(7)XI2*

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	IP Standard Feature Set	IP	c7200-is-mz	48 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	48 MB	128 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7200-p-mz	48 MB	128 MB	RAM
Cisco 7301 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	256 MB	RAM
			c7301-i12s-mz	64 MB	512 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7301-p-mz	64 MB	256 MB	RAM

Table 4 *Memory Recommendations for the Cisco IOS Release 12.3(7)XI1*

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	IP Standard Feature Set	IP	c7200-is-mz	48 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	48 MB	128 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7200-p-mz	48 MB	128 MB	RAM
Cisco 7301 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	256 MB	RAM
			c7301-i12s-mz	64 MB	512 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7301-p-mz	64 MB	256 MB	RAM

Table 5 *Memory Recommendations for the Cisco IOS Release 12.3(7)XI*

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	IP Standard Feature Set	IP	c7200-is-mz	48 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	48 MB	128 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7200-p-mz	48 MB	128 MB	RAM
Cisco 7301 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	256 MB	RAM
			c7301-i12s-mz	64 MB	512 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7301-p-mz	64 MB	256 MB	RAM

Supported Hardware

Cisco IOS Release 12.3(7)XI4 supports the following Cisco 7000 platforms:

- Cisco 7200 series routers
- Cisco 7301 router

For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 7.

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(7)XI4:

```
Router> show version
Cisco IOS Software, 7301 Software (c7301-I12S-MZ), Version 12.3(7)XI4, 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 XI:

New Hardware Features in Cisco IOS Release 12.3(7)XI4

There are no new hardware features supported in Cisco IOS Release 12.3(7)XI4.

New Software Features in Cisco IOS Release 12.3(7)XI4

There are no new software features supported in Cisco IOS Release 12.3(7)XI4.

New Hardware Features in Cisco IOS Release 12.3(7)XI3

There are no new hardware features supported in Cisco IOS Release 12.3(7)XI3.

New Software Features in Cisco IOS Release 12.3(7)XI3

There are no new software features supported in Cisco IOS Release 12.3(7)XI3.

New Hardware Features in Cisco IOS Release 12.3(7)XI2

There are no new hardware features supported in Cisco IOS Release 12.3(7)XI2.

New Software Features in Cisco IOS Release 12.3(7)XI2

There are no new software features supported in Cisco IOS Release 12.3(7)XI2.

New Hardware Features in Cisco IOS Release 12.3(7)XI1

There are no new hardware features supported in Cisco IOS Release 12.3(7)XI1.

New Software Features in Cisco IOS Release 12.3(7)XI1

There are no new software features supported in Cisco IOS Release 12.3(7)XI1.

New Hardware Features in Cisco IOS Release 12.3(7)XI

There are no new hardware features supported in Cisco IOS Release 12.3(7)XI.

New Software Features in Cisco IOS Release 12.3(7)XI

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.3(7)XI:

Multi-Processor Forwarding (MPF) for Broadband LAC

Multi-Processor Forwarding (MPF) for Broadband LAC is a method of improving the performance of broadband features, specifically the Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC), by enabling forwarding on a second CPU on the Cisco 7301 router. The need to improve performance is important due to the rapid increase in broadband users. MPF for Broadband LAC significantly improves performance by three times that of a regular Cisco7301, without adding a new chassis.

MPF for Broadband LAC is accomplished by the second CPU running Fast Forwarding (FF) software to switch data packets. The FF software is bundled together with the Cisco IOS software image. When the Cisco IOS image is loaded, the second CPU is enabled by default. To disable fast forwarding on the second CPU, use the **no ip mpf** command. In addition, **show ip mpf** commands and a **debug ip mpf** command monitor forwarding on the second CPU and provide statistics.

The MPF for Broadband LAC feature requires the purchase of enabling software for the second CPU. You may purchase the enabling software when you purchase a new Cisco 7301 router, or you may purchase the enabling software as an upgrade. In both cases, the second CPU software is bundled in the Cisco IOS image and turned on by default. Contact your Cisco field representative or sales support team for more information.

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at

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

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in [Table 6](#).

Table 6 *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Caveats for Cisco IOS Release 12.3 XI

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(7)XI4.

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/>.

Because Cisco IOS Release 12.3(2)XB is the initial base release, there are no resolved caveats. For a list of the resolved caveats, refer to the next set of release notes for this release version.

Table 7 *Caveats Reference for Cisco IOS Release 12.3 XI*

DDTS Number	Open in Release	Resolved in Release
CSCea22552		12.3(7)XI
CSCea56883		12.3(7)XI1
CSCeb78526		12.3(7)XI4
CSCeb85255		12.3(7)XI
CSCec16481		12.3(7)XI
CSCec24263		12.3(7)XI
CSCec38308		12.3(7)XI2
CSCec43747		12.3(7)XI
CSCec58512		12.3(7)XI
CSCec71950		12.3(7)XI
CSCec90041		12.3(7)XI2
CSCed09146		12.3(7)XI2
CSCed15391		12.3(7)XI2
CSCed16493		12.3(7)XI1
CSCed18557		12.3(7)XI2
CSCed27086		12.3(7)XI2
CSCed32394		12.3(7)XI
CSCed43581		12.3(7)XI
CSCed51952		12.3(7)XI2
CSCed57586		12.3(7)XI
CSCed57653		12.3(7)XI
CSCed59172		12.3(7)XI2
CSCed63357		12.3(7)XI2
CSCed65333		12.3(7)XI
CSCed65778		12.3(7)XI3
CSCed67358		12.3(7)XI3
CSCed67628		12.3(7)XI, 12.3(7)XI3
CSCed78149		12.3(7)XI2, 12.3(7)XI3
CSCed81418		12.3(7)XI
CSCed84464		12.3(7)XI
CSCed84912		12.3(7)XI2
CSCed86647		12.3(7)XI
CSCed88805		12.3(7)XI2
CSCed93630		12.3(7)XI2
CSCed95499		12.3(7)XI3
CSCee03702		12.3(7)XI2

Table 7 Caveats Reference for Cisco IOS Release 12.3 XI (continued)

CSCee04235		12.3(7)XI3
CSCee11770		12.3(7)XI2
CSCee12235		12.3(7)XI2
CSCee16150		12.3(7)XI2
CSCee18018		12.3(7)XI2
CSCee24899		12.3(7)XI2
CSCee26662		12.3(7)XI1
CSCee27641		12.3(7)XI1
CSCee29574		12.3(7)XI2
CSCee33633		12.3(7)XI
CSCee36445	12.3(7)XI	
CSCee38105		12.3(7)XI
CSCee42617		12.3(7)XI2
CSCee42660		12.3(7)XI
CSCee45655		12.3(7)XI
CSCee47898		12.3(7)XI
CSCee52915		12.3(7)XI1
CSCee53132	12.3(7)XI	
CSCee57091		12.3(7)XI
CSCee57149		12.3(7)XI
CSCee58039		12.3(7)XI
CSCee58990		12.3(7)XI1
CSCee66417		12.3(7)XI
CSCee68382		12.3(7)XI1
CSCee68725		12.3(7)XI1
CSCee69772		12.3(7)XI
CSCee70018		12.3(7)XI2
CSCee72249		12.3(7)XI1
CSCee72318		12.3(7)XI
CSCee76540		12.3(7)XI2
CSCee77244		12.3(7)XI1
CSCee79812		12.3(7)XI1
CSCee81662		12.3(7)XI2
CSCee82378		12.3(7)XI1
CSCee83079		12.3(7)XI1
CSCee84496		12.3(7)XI3
CSCee86557		12.3(7)XI2

Table 7 Caveats Reference for Cisco IOS Release 12.3 XI (continued)

CSCef00114		12.3(7)XI1
CSCef09165		12.3(7)XI2
CSCef11074		12.3(7)XI2
CSCef31712		12.3(7)XI2
CSCef44225		12.3(7)XI3
CSCef46191		12.3(7)XI2
CSCef50650		12.3(7)XI2
CSCef60659		12.3(7)XI3
CSCef61610		12.3(7)XI3
CSCef63785		12.3(7)XI2
CSCef68324		12.3(7)XI3
CSCef67682		12.3(7)XI3
CSCef73237		12.3(7)XI2
CSCef75555		12.3(7)XI2
CSCef81634	12.3(7)XI3	
CSCef93984		12.3(7)XI2
CSCef96810		12.3(7)XI2
CSCeg58833	12.3(7)XI3	
CSCeg71194	12.3(7)XI3	
CSCeh62257	12.3(7)XI4	
CSCin24544		12.3(7)XI
CSCin66200		12.3(7)XI2
CSCin66969		12.3(7)XI
CSCin68371		12.3(7)XI1
CSCin72029		12.3(7)XI
CSCin74759		12.3(7)XI
CSCin74857		12.3(7)XI
CSCin75481		12.3(7)XI1
CSCin75571		12.3(7)XI
CSCin76005		12.3(7)XI1
CSCin76381		12.3(7)XI3
CSCin78156		12.3(7)XI1
CSCin78416		12.3(7)XI1
CSCin78631		12.3(7)XI1
CSCin78781		12.3(7)XI1
CSCin82407		12.3(7)XI3
CSCsa54608		12.3(7)XI4

Table 7 Caveats Reference for Cisco IOS Release 12.3 XI (continued)

CSCsa59600		12.3(7)XI3
CSCsa62475	12.3(7)XI3	

Open Caveats—Cisco IOS Release 12.3(7)XI4

This section documents possible unexpected behavior by Cisco IOS Release 12.3(7)XI4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeh62257
PPP is not establishing new sessions.
This issue may occur when a leak in ppp is handle in full virtual-access interfaces.
Workaround: Reload the box or use sub VAI's.

Resolved Caveats—Cisco IOS Release 12.3(7)XI4

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(7)XI4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeb78526
A Cisco 7500 series router that is running LAN Emulation (LANE) and switched virtual circuits (SVCs) may experience a reload caused by a bus error, and the following error message may appear:
`System returned to ROM by bus error at PC 0XXXXXXXXX`
This issue is observed on a Cisco 7500 series router with a PA-A3-OC3MM ATM port adapter that is running Cisco IOS Release 12.2(15)T5 or a later release.
There are no known workarounds.
- CSCsa54608
The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.
Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.
Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.
Only devices running certain versions of Cisco IOS are affected.
Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.
This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml.

Open Caveats—Cisco IOS Release 12.3(7)XI3

This section documents possible unexpected behavior by Cisco IOS Release 12.3(7)XI3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef81634

Using the external generating tool IXIA Explorer to bring up and tear down SSG sessions quickly, the PRE2 crashes with a Bus Error Exception. This problem occurs when the tool initializes the interface and quickly brings sessions back up while the old sessions are still cleared out.

There are no known workarounds.

- CSCeg58833

The router unexpectedly reloads when removing a v-template from a router with active multi-cast interfaces running.

This issue occurs on any Cisco IOS release running multicast on v-template interfaces.

Workaround: Either remove multicast config from the v-template prior to v-template removal, or disable interfaces prior to removing config.

- CSCeg71194

PRE2 is not able to bring up additional PPPoA sessions when CPU running under stress.

This issue occurs when the CPU running under stress.

There are no known workarounds.

- CSCsa62475

The following message is logged:

```
%GENERAL-3-EREVENT: C10KSSG: Null c10k_turbo_acl for old out ACL
-Traceback= 60DBB7AC 60DBCE44 60DB670C 60DB6480 60DBB20C 60DB159C 60E09C68 60E09D4C
60E58434 60E585CC 608496AC 6085CD5C 6085CDD0 6084FD04 608559C8 60846C18
```

This issue is observed when a SSG user with a SSG output access-list defined in its RADIUS profile disconnect the PPPoX session.

Workaround: Define the ACL on the router and refer to it in the user profile instead of defining the ACEs directly in the user profile.

Resolved Caveats—Cisco IOS Release 12.3(7)XI3

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(7)XI3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed67358

An IPv6 PIM neighbor may be down after changing the PIM configuration.

This issue is observed when the **no ipv6 pim** command is entered on some subinterfaces of a physical Ethernet interface and when PIM is enabled on several subinterfaces of the same physical Ethernet interface. The issue affects both IPv4 and IPv6, and configurations with multicast and OSPF Hello messages.

There are no known workarounds.

- CSCed67628

During an initial boot of a Cisco 7301 that has a PA-MC-8TE1+ or PA-MCX-8TE1-M in bay 0, an unexpected reload may occur.

This issue may occur irrespective of whether a regular Cisco IOS software image or a boot software image is present in the bootflash filesystem.

Workaround: Powercycle the Cisco 7301 and reboot platform. The problem only surfaces during the initial boot of the platform.

- CSCed78149

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP "hard" error messages
2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.cpni.gov.uk/docs/re-20050412-00303.pdf>.

- CSCed95499

A Cisco router may unexpectedly reload if a PA driver attempts to convert an uncached iomem address to a cached iomem address.

This issue is observed on a Cisco 7200 series that is configured with an NPE-G1.

There are no known workarounds.

- CSCee04235

A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

```
Last reset from watchdog reset
```

This issue is observed on a Cisco 7200vxr series that is configured with an NPE-G1 Network Processing Engine.

There are no known workarounds.

- CSCee84496

An NPE-G1 may display an erroneous parity error message.

This issue is observed on a Cisco 7200 series when the NPE-G1 receives an ECC/bus error.

There are no known workarounds.

- CSCef44225

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at <http://www.cpni.gov.uk/docs/re-20050412-00303.pdf>.

- CSCef60659

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at <http://www.cpni.gov.uk/docs/re-20050412-00303.pdf>.

- CSCef61610

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at <http://www.cpni.gov.uk/docs/re-20050412-00303.pdf>.

- CSCef67682

Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at <http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml> contain fixes for this issue.

- CSCef68324

Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

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

More details can be found in the security advisory that is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

- CSCin76381

A PXF exception may occur on a Cisco 7200 series that is configured with an NSE-1 or on a Cisco 7401 that has PXF enabled when either of these platforms function as an LNS.

This issue is observed when an L2TP session is established over a VLAN subinterface that has ISL encapsulation enabled and when traffic is processed on this subinterface.

Workaround: Disable PXF by entering the **no ip pxf** command.

- CSCin82407

Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to <http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

- CSCsa59600

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP "hard" error messages
2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at <http://www.cpni.gov.uk/docs/re-20050412-00303.pdf>.

Open Caveats—Cisco IOS Release 12.3(7)XI2

This section documents possible unexpected behavior by Cisco IOS Release 12.3(7)XI2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(7)XI2.

Resolved Caveats—Cisco IOS Release 12.3(7)XI2

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(7)XI2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec38308

SSG only supports one class attribute rather than several of them, although a RADIUS client is supposed to put all class attributes that it receives in Access-Accept messages into Accounting-Request messages that it sends for a session. (See RFC2865/2866.)

This issue is observed on a Cisco platform that is configured as an SSG.

There are no known workarounds.

- CSCec90041

BGP update generation may enter a deadlock.

This issue is observed when the RR configuration is changed.

Workaround: Remove the BGP process and add it back.

- CSCed09146

Extra network Accounting STOP record may be seen when an Async call fails on authentication. These are unwanted records and should not be generated.

This issue is seen for an Async call on 5300-T1 platform running 12.3(5.8). This could be service affecting.

There are no known workarounds.

- CSCed15391

There is spurious memory access at atm_vcmode_subcommands.

This issue occurs under the low memory conditions.

There are no known workarounds.

- CSCed18557

A memory leak may occur in the “dead process” on a Cisco router, and memory allocation failures (MALLOCFAIL) may be reported in the processor pool. The authentication, authorization, and accounting (AAA) User Identifier (UID) database may leak about 200,000 bytes for each failed EXEC call or vty session because of internal errors during the initiation process.

This issue is observed when EXEC Accounting and Network Accounting are enabled and when a failure occurs during an EXEC call or a vty session. The reasons for the EXEC call failure or vty session failure could be low processor memory on the Cisco router, an internal message processing error, or a timeout during the prompting for a username and password.

Workaround: If this is an option, disable EXEC Accounting and Network Accounting.



Note See similar caveat: CSCee35379

- CSCed27086

A Cisco router that functions as a PPPoX aggregator may crash because of a bus error.

This issue is observed in a highly scaled environment when many sessions are simultaneously established and torn down.

There are no known workarounds.

- CSCed51952

A Cisco router may crash when you perform an online insertion removal (OIR) of a line card.

This issue is observed when an interface on the line card is being configured through the CLI while the OIR of the line card removes the interface.

There are no known workarounds.

- CSCed59172

An SNMP trap configuration may be erased when you enter the **snmp-server enable traps snmp** global configuration command with any trap type followed by the **snmp-server enable traps [syslog | entity]** global configuration command.

This issue is observed on multiple Cisco platforms that run Cisco IOS Release 12.2 or Release 12.3.

For example, the symptom occurs when you enter the following configuration:

```
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
```

```
snmp-server enable traps syslog
```

```
snmp-server enable traps entity
```

Then you enter:

```
no snmp-server enable traps snmp authentication
```

```
no snmp-server enable traps syslog
```

or you enter:

```
no snmp-server enable traps snmp authentication
```

```
no snmp-server enable traps entity
```

At this point, the **snmp-server enable traps snmp linkdown linkup coldstart warmstart** command is no longer in the output of the **show running-config** command.

Workaround: Manually reconfigure the **snmp-server enable traps snmp linkdown linkup coldstart warmstart** command.

Alternate workaround: First enter the **no snmp-server enable traps syslog** command or the **no snmp-server enable traps entity** command before you enter the **no snmp-server enable traps snmp authentication** command.

- CSCed63357

This caveat consists, of six separate symptoms, conditions, and workaround, of which the first three apply to all Cisco IOS releases and the last three apply only to Cisco IOS Release 12.3 T:

Symptom 1:

There are three issues:

- There may be a inconsistent or duplicate display of files between the **show disk slot-number** and **dir disk slot-number** commands.
- When a file is deleted from the CLI, the file may be deleted but a “No such file” message may be printed.
- One cluster may leak. Entering the **fsck** command truncates the original file and creates an orphan file for the leaked cluster.

This symptom is observed when an application creates or opens a file without the “O_TRUNC:” mode, as in the following example:

```
show version | append disk#:
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#vtp file new
Setting device to store VLAN database at filename new.
Router(config)#^Z
```

There are no known workarounds.

Symptom 2:

The **show disk slot-number** and **dir disk slot-number** commands may show inconsistent information (such as inconsistent file sizes) when multiple images are copied.

This symptom is observed when you make two copies of the image file to the disk by using two vtys and by entering the **dir disk slot-number** command at the same time.

Workaround: Do not enter the **show disk slot-number** and **dir disk slot-number** commands when multiple images are being copied.

Symptom 3:

There are two issues:

- The **show disk slot-number** and **dir disk slot-number** commands may show inconsistent information.
- Entering the **fsck** command may delete or truncate the valid files or create an orphan file for an unused cluster.

This symptom is observed when you rename a directory that consists of many subdirectories or files.

Workaround: Reload the router.

Symptom 4:

There are two issues:

- There may be a duplicate entry for each file when you enter the **show disk slot-number** command.
- An snmpGet on a ciscoFlashFileSize object may enter a loop.

This symptom is observed on a router that runs Cisco IOS Release 12.3 T after the router boots up.

There are no known workarounds.

5) Symptoms: There are two symptoms:

- The **show disk slot-number** and **dir disk slot-number** commands may show inconsistent information.
- Entering the **fsck** command may delete or truncate the original file.

This symptom is observed on a router that runs Cisco IOS Release 12.3 T when an application or a CLI command overwrites a file on the disk.

Workaround: Reload the router.

Symptom 6:

A router that runs Cisco IOS Release 12.3 T unexpectedly reloads.

This symptom is observed when an application creates or opens a file without the "O_TRUNC" mode and attempts to delete the file, as in the following example:

```
show version | append disk0:redirect.out" and issuing
delete disk0:disk0:redirect.out
```

Workaround: Reload the router and delete the file.

- CSCed65778

Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml>

- CSCed68523

A LAC sends incorrect connection speed information in the L2TP setup message to the LNS, which in turn gets forwarded to the AR RADIUS server for authentication.

This issue is observed on a router that runs Cisco IOS Release 12.3(6.2)T2. The symptom may also occur in other releases.

There are no known workarounds.

- CSCed78149

TCP connections may be vulnerable to spoofed ICMP packets. A spoofed ICMP packet may cause the TCP connection to use a very low segment size for 10 minutes at a time.

This issue is observed when TCP connections are configured for PMTU discovery. Note that PMTU discovery is disabled by default on a router.

Workaround: Disable PMTU discovery.
- CSCed84912

A Cisco router may reload unexpectedly with a bus error when you enter the **show caller** command.

This issue is observed when PPP is configured on a router that runs Cisco IOS Release 12.3, 12.3(3)B1, or 12.3 T.

The issue is more likely to occur when the show caller output is lengthy, and particularly so if the output causes a ---More--- prompt.

The issue is also more likely to occur when there is a high rate of connection and disconnection of PPP sessions, for example, when an interface flaps.

There are no known workarounds.
- CSCed88805

A router may unexpectedly reload with a bus error with the same address:

```
System was restarted by bus error at PC 0x606B2BE4, address 0xB0D0C11
```

Decodes indicate that a PPP problem may be the cause of the symptom.

This issue is not platform dependent and may occur with any type of IP PPP connection. This problem is also most likely occur when there is a high volume of call connections and disconnections, for example, when an interface carrying multiple calls flaps.

There are no known workarounds.
- CSCed93630

A Cisco router may reload unexpectedly when a **bgp debug** command is enabled.

This issue is observed on a Cisco router that runs Cisco IOS Release 12.0S, 12.2S, or 12.3T.

There are no known workarounds.
- CSCee03702

A Cisco router that is configured for SSG may unexpectedly reloads with a bus error.

This issue is observed on a Cisco router that is configured for SSG and that has PPP SSG users when there are IPCP renegotiations on an active PPP session and a new IP address is assigned to the session.

Workaround: Enter the **ip address negotiated previous** command on the client to prevent a new address from being assigned during the IPCP renegotiations.
- CSCee11770

All SWIDBs may be used.

This issue is observed when PPPoA sessions flap continuously.

There are no known workarounds.

- CSCee12235

A Cisco platform reloads because of a watchdog timer expiration.

This issue is observed on a Cisco platform that runs Cisco IOS Release 12.2(20)S2 or Release 12.3 under the following conditions:

- A service policy (“A”) is attached to an ATM PVC.
- Policy-map “A” is renamed to “B”.
- Service policy “B” is attached to the ATM PVC.

Workaround: First detach the service policy from the PVC, then rename it and attach it again.

- CSCee16150

The router may not respond to valid PoD packets by disconnecting the user. Instead, the router will return a RADIUS-format packet with a Code of Disconnect-Request-NAKed (42 in decimal) and a Reply-Message attribute with a value set to the string “No Matching Session”.

This issue occurs when you are using PoD to disconnect users and have **aaa pod server ... auth-type all ...** configured, and are using a PoD server which includes an EXACT copy of RADIUS attribute 151 from an earlier accounting request in the PoD packet.

Workaround: Either use a program to generate the PoD packets which knows to convert from an ASCII string of hexadecimal characters to a 32-bit number or Configure the router to ignore the value of attribute 151 in the PoD request by configuring **aaa pod server ... auth-type all ignore session-key ...**

- CSCee18018

During the reloading of a Cisco router with dual RSP8 processors, the following error message may be displayed:

```
%Error opening nvram:/startup-config (Device or resource busy)
```

As a result, the configuration in NVRAM might not be applied. This issue is unlikely to occur outside a specific timing condition.

This issue is observed on a Cisco 7500 series router with dual RSP8 processors but is platform independent.

Workaround: Use boot config to redirect the config to slot/disk/bootflash.

- CSCee24899

A router that is configured for multicast routing may reload due to a bus error.

This issue is observed on a Cisco router that runs a Cisco IOS software release that contains the fix for CSCec80252. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec80252> .

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

There are no known workarounds.

- CSCee29574

A child policy bandwidth calculation is wrongly mixed with the specified rate of an old parent policy.

This issue is observed after you have changed the configuration of a policy map in a hierarchical policy.

Workaround: Detach and reattach the policy map.

- CSCee42617

Users are unable to authenticate using RADIUS, or accounting is not sent to the RADIUS server. In addition, when the **debug radius** command is entered, the following information is generated:

```
RADIUS(00000049): sending
%RADIUS-3-NOSERVERS: No Radius hosts configured.
RADIUS/DECODE: parse response no app start; FAIL
RADIUS/DECODE: parse response; FAIL
```

The output of the **show running-config** command indicates that there are in fact RADIUS servers in the server group.

These issues are observed after following these steps:

1. Remove and recreate a server group that is still referenced by one or more method lists, by entering the following commands:

```
no aaa group server radius XXXX
  aaa group sever radius XXXX
    server x.x.x.x
  ...
```

2. Allow one of these method lists to be used, causing a transaction to be sent to a RADIUS or TACACS+ server in the server group.

3. Remove and re-add the **radius-server host ...** command lines for all authentication-capable (or accounting-capable if this group is used for accounting) servers in this server group.

Workaround: Remove all RADIUS or TACACS+ server configurations, remove all RADIUS or TACACS+ server group configurations, and remove all method lists. Then, reconfigure all of them.

- CSCee70018

A router sends three access requests for one call session; the first request is the normal request, the second request has the right password but the wrong user name, and the third request comes just with the domain name as the user name.

This issue is observed with a call rate condition of above 20 calls per second and occurs randomly for a view call sessions only.

There are no known workarounds.

- CSCee76540

The radius-server attribute 4 NAS IP address attribute is not accepted.

This issue occurs when Radius attribute 4 is configure.

There are no known workarounds.

- CSCee81662

PPP sessions may get stuck in the TERMSENT state.

This issue is observed on a Cisco platform that has a high CPU utilization.

Workaround: Clear the underlying layer (VPDN, PPPoA, or PPPoE).

- CSCee86557

All SWIDBs may be used.

This issue is observed when PPPoE or VPDN sessions flap continuously.

There are no known workarounds.

- CSCef09165
SSG VPDN services and normal VPDN tunnels may not function together in some configurations. This issue is observed when SSG is configured and when VPDN parameters are locally provisioned but VPDN tunnels are not established between the LAC and the LNS.
Workaround: Enter the **aaa authorization network default group radius** command.
- CSCef11074
Auto-logout services for some PPP SSG users may not be active after the PPP session comes up. The issue is seen when there are a large number of PPP sessions and more SSG PPP sessions are coming at a high rate.
The following error messages are seen with “debug ssg ctrl-error” is turned on:
SSG-CTL-ERR: Unable to add HostRoute in CEF table x.x.x.x
SSG-CTL-ERR: host route addition failed
There are no known workarounds.
- CSCef31712
A CPU hog message is generated when you enter the **show pppoe summary** command. This issue is observed when there are high-scaling unambiguous QinQ sessions and interfaces configured.
There are no known workarounds.
- CSCef46191
A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.
All other device services will operate normally.
User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.
Workaround: The detail advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>
- CSCef50650
A router unexpectedly reloads when it attempts to access a TACACS+ server. This issue is observed when the TACACS+ server is not up or unreachable.
Workaround: Ensure that the router accesses a valid TACACS+ server that is up and running.
- CSCef63785
The Cisco router unexpectedly reloads on clearing the PPPoEoA session when mqc with fair queue is configured on the atm vc and pulled policy is rejected.
There are no known workarounds.
- CSCef73237
SSG authentication and accounting requests sent with nas-port-type = Ethernet. This issue occurs in Cisco IOS Release 12.3(7)XI1.
There are no known workarounds.

- CSCef75555
Cisco 7200 router with ATM PA-A3 might crash when ATM PA-A3 is OIR removed.
This issue happens when dynamic VC modification is enabled on the interface using the **dbns enable** command and the ATM PA-A3 is OIR removed.
Workaround: Without dbns enable, this problem does not happen.
- CSCef93984
A Fail to apply Service-Policy on a VC can be seen in case where qos configuration is dependent upon the DBS avpair, which is applied by AAA code after Policy avpair.
Workaround: AAA code apply DBS avpair before apply Policy avpair on the VC.
- CSCef96810
Spurious access messages may be seen after clear sss session command.
There are no known workarounds.
- CSCin66200
Show l2tun needs large contiguous memory (64MB/128MB) to display 16k/32k sessions.
There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(7)XI1

This section documents possible unexpected behavior by Cisco IOS Release 12.3(7)XI1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed16493
Gige port does not establish link.
This issue occurs when the gige default value for autonegotiation is changed from “negotiation auto” to “no negotiation auto”. This change in the default setting will cause gige ports that have established link with previous images to fail to do so.
Workaround: Add “negotiation auto” to the gige port configuration.
- CSCee79812
C10000 12.3-7.XI unexpected reloads.
This issue occurs when timing out all PPPoA sessions with DBS enable.
There are no known workarounds.
- CSCee83079
Broadband 128k queue config removes input policy from Virtual-Template cause CPUHOG traceback and reset output pxf queues.
This issue occurs when configuring 31.5k atm subint with output cbwfq policy and input police policy in Virtual-Template
There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(7)XI1

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(7)XI1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea56883

A Cisco 7204VXR that functions as an L2TP network server (LNS) may pause indefinitely because of a bus error when a user disconnects and then reconnects.

This issue is observed on a Cisco 7204VXR that is configured with a Network Processing Engine G1 (NPE-G1) under the following conditions:

- The router functions as an LNS that terminates Layer 2 Tunneling Protocol (L2TP) tunnels.
- Output route filters are applied via RADIUS attributes to the Routing Information Protocol (RIP) routing process.

There are no known workarounds.

- CSCed62371

A Cisco router may be reloaded if tacacs+ configuration is present in the startup config.

This issue occurs when TACACS+ configuration is present in the startup configuration.

There are no known workarounds.

- CSCee26662

A platform may reload when the **aaa dnis map dnis-number authentication ppp group server-group-name** command is entered.

This issue is observed when **aaa dnis map** commands are enabled.

There are no known workarounds.

- CSCee27641

The ESR 10000 could have its interface being reset if it experiences the CPUHOG. The CPUHOG could be the result of altering configurations with live sessions.

This issue occurs when there are PPP SSG hosts logging into a service, and the SSG port-map feature has not been enabled. There can be a CPU hog when a large number of PPP users connect to and disconnect from a service.

There are no known workarounds.

- CSCee52915

An Accounting Stop message is sent in case an Access Reject Message is not received from the radius Server, which is not applicable for all customer. The DDTS will fix this issue.

Workaround: If possible, configure Tunnel Link Acct with or without the possibility to disable “aaa accounting send stop-record authentication failure”.

- CSCee58990

Raceback is seen towards the end of ssg link redundancy test cases.

This issue may occur under the following conditions:

- When creating an open-garden service
- When Login a user to ssg.
- When issuing a “no ssg enable force-cleanup”, a Traceback is seen.

There are no known workarounds.

- CSCee68382
Spurious Access is occurs when changing RADIUS address or addresses with live sessions. There are around 32K RFC1483 and PPPOE sessions configured and around 1000 sessions are active.
This may occur when changing RADIUS address or addresses with live sessions.
There are no known workarounds.
- CSCee68725
In a redundant system, the ifIndex-table is not written to the standby nvram: when a **write** command is issued on the primary. As a result, if a switchover occurs, the interface indices can be renumbered.
This issue occurs when using “snmp-server ifindex persist” in a redundant system.
Workaround: Explicitly copy the nvram:ifIndex-table from the primary to the stby-nvram:
- CSCee72249
The **snmp-server host** command only supports 1 host. Adding another host will overwrite the existing host. Also, the **traps** subcommand for snmp-server host does not show in the running configuration. However, traps are sent to the host if **traps** was entered in the host configuration.
When using the **snmp-server host** command to configure more than one host or to configure the host to receive traps.
There are no known workarounds.
- CSCee77244
CPU hog syslog messages are popping up when oids mibs from the CISCO-CLASS-BASED-QOS-MIB mib are polled.
There are no known workarounds.
- CSCee82378
When the Create-on-demand feature is configured over a range pvc on a point-to-point subinterface, the following may occur:
 - Create several VCs in INAC status
 - Establish only one of the connections on receiving traffic by several of them
 - Running config show several subinterfaces on performing the reload of the device
 Workaround: Use Multipoint subinterfaces.
- CSCef00114
A Cisco router unexpectedly reloads when tunnel password is downloaded using the RADIUS.
This issue occurs under the following conditions:
 - Tunnel-Password should be configured in the RADIUS domain profile used for establishing the tunnel.
 - Tunnel-Password string should be more than 64 characters.
 Workaround: Configure password string to less than 64 bytes.
- CSCin68371
Autoprovisioning does not get enabled on the ATM interface.
This issue occurs when “create on-demand” is configured in a vc-class and the vc-class config is sourced to the ATM interface or PVCs.
Workaround: Configure “create on-demand” directly on the PVCs.

- CSCin75481

A MPF microcode module may have timing issues related to MPF <-> IOS packet handover when a VPDN session is flapped with traffic (the timing is not guaranteed to work when VPDN session is flapped with traffic).

There are no known workarounds.
- CSCin76005

The PVC becomes INACTIVE (MODIFYING) after the parameters for the PVC are changed.

If the QoS parameters associated with the PVC are changed, this defect is observed sometimes.

There are no known workarounds.
- CSCin78156

The following multiuser configuration error message is observed:

```
Unable to delete PVC 1/2660 on ATM5/0/0.110000. Possibly multiple users configuring
IOS simultaneously
```

When PVC configured as Auto VC is changed to normal PVC the above error message is observed.

There are no known workarounds.
- CSCin78416

After the router reloads, the un-configured p2p sub-interfaces appear in the running-configuration.

When range command is configured on p2p sub-interface and member PVCs associated with the range do not receive traffic after reload, their corresponding p2p sub-interfaces appear in the running configuration.

There are no known workarounds.
- CSCin78631

The “PVC creation failure” error message appears when the PVC that is part of range is changed from Auto VC to normal VC.

This issue occurs when the PVC range that is part of p2p sub-inteface is changed from Auto VC to normal VC. When this happens, the PVC creation failure message appears.

Workaround: The operator can delete the range and configure it again with normal VCs.
- CSCin78781

Auto VCs remain INACTIVE even when the traffic is received on them.

This issue occurs when VC-class is configured on Auto VC and the parameters of the VC-class are modified to trigger re-creation of the PVC then this problem is observed.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(7)XI

This section documents possible unexpected behavior by Cisco IOS Release 12.3(7)XI and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCee36445

The router becomes unstable after a failure and the user will not be able to bring up more sessions and or copy configs.

There are no known workarounds.

- CSCee53132
When having large amount of PPPoE sessions in PTA or LAC, doing “show pppoe summary” can generate multiple CPUHOG tracebacks in the log.
This issue occurs when large amount of PPPoE sessions (62000) in the system.
There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(7)XI

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(7)XI. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea22552
GRE implementation of Cisco IOS is compliant with RFC2784 and RFC2890 and backward compatible with RFC1701.
As an RFC compliancy this DDTS adds the check for bits 4-5 (0 being the most significant) of GRE header.
This issue does not cause any problem for router operation.
- CSCeb85255
A unexpected reload can occur on a Cisco 1000 series and Cisco 6400 series with an atm interface.
This issue occurs when executing the **show atm** command.
There are no known workarounds.
- CSCec16481
A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.
The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.
Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:
<http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml>.
- CSCec24263
Under specific circumstances the values reported by RADIUS attribute 46, acct-session-time are incorrect. It was reported by the customer in the following circumstances:
 - For sessions brought up short after restart. The reason might be that when the session started it was using the internal timer and when stopping the NTP timer was used which would cause wrong data.
 - For sessions brought up during changing timezone or daylight savings information (see below):

```
(config)#clock summer-time CEST recurring 1 Tue Sep 12:15 1 Tue Sep 13:30 60
new session established
Router#sh clock
12:14:59.218 MEZ Tue Sep 2 2003
Router#sh clock
13:15:05.175 CEST Tue Sep 2 2003
logout
```

```

RADIUS debug --
Acct-Terminate-Cause[49] 6 user-request
Acct-Session-Time [46] 6 4294963734
Acct-Input-Octets [42] 6 120
Acct-Output-Octets [43] 6 108

```

This issue was reported for the NRP2 only. It was tested with the following image: c6400r-g4p5-mz.122-4.BX.bin in a testbed when testing accounting functionality.

There are no known workarounds.

- CSCec43747

A Cisco router configured for MPLS/VPN hub&spoke using the Half Duplex VRF feature does not install the per-user static routes (learned from AAA server) in the downstream VRF.

There are no known workarounds.

- CSCec58512

In case of a long period of Radius server unavailability and a very high rate of incoming calls, a Cisco access server may experience a shortage of I/O memory.

This issue prevents the AAA authentication from queuing any Radius packets if the amount of free I/O memory is less than five.

There are no known workarounds.

- CSCec71950

Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

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

There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing. This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

- CSCed32394

Cisco 12.2BX crashes in pppoa_set_event with DBS.

There are no known workarounds.

- CSCed43581

On a Cisco router running one of the latest IOS images, the output of “show interface description” is truncated, only 9 characters are displayed for Interface field which is the Interface identifier.

There are no known workarounds.

- CSCed57586
 PPP sessions are no longer accepted by a NAS. A PPP debug shows:
 "IPCP: Peer address ... in use by ..."
 This issue occurs if all the following conditions are met:
 - The **ppp ipcp address unique** command is configured under a virtual-template interface.
 - The system runs Cisco IOS Release 12.2(16)BX2, 12.3(4)T1 or 12.3(5.7)T or later.
 - Thousands of calls are brought up and down continuously within a few days.
 Workaround: Unconfigure the **ppp ipcp address unique** command.
- CSCed57653
 The router may run out of I/O memory and "show ssg service <servicename>" shows a large ReferenceCount.
 This issue may occur on an SSG when the remote AAA server for a radius proxy service goes down for a long time and many users try to login to this service.
 Workaround: Configure an alternate AAA server for the proxy service that responds when the primary AAA server is down.
- CSCed65333
 Bringing up a BGP session with BGP MD5 authentication may be delayed considerably on a router.
 This issue is observed on a Cisco router that runs Cisco IOS Release 12.2(15)BZ2, 12.3, or 12.3 T when MD5 authentication is enabled. The issue occurs when the router sends a SYNC ACK message that has a wrong total IP length field after a BGP session is initiated from a peer router.
 The issue goes unnoticed without MD5 authentication and occurs because of a mishandling on TCP options such as MD5, WND-SCL, TS, and Selective-ACK.
 There are no known workarounds.
- CSCed67628
 During an initial boot of a Cisco 7301 that has a PA-MC-8TE1+ or PA-MCX-8TE1-M in bay 0, an unexpected reload may occur.
 The issue may occur irrespective of whether a regular Cisco IOS software image or a boot software image is present in the bootflash filesystem.
 Workaround: Powercycle the Cisco 7301 and reboot platform. The problem only surfaces during the initial boot of the platform.
- CSCed81418
 The "show pppoe session | include <pattern>" took at least 30 minutes before seeing the result. RP CPU is running at 99% all the time with "Exec" running.
 This is observed when large amount of sessions are active in the C10K PTA or LAC systems.
 There are no known workarounds.
- CSCed84464
 When the **l2tp hidden** command is configured on a Cisco 10000 series and when the call rate is above 40 calls/second, the Cisco 10000 series uses a wrong tunnel ID in communication with the LNS, which causes the L2TP tunnel to go down.

This issue is observed when there are about 1000 sessions and more than one outgoing L2TP tunnel on the Cisco 10000 series that functions as a LAC and that runs Cisco IOS Release 12.2(16)BX2. This issue may also occur in other releases.

There are no known workarounds.

- CSCed86647

The session duration time reported in accounting packets may be wrong.

This issue is observed when you enter the **show aaa user all** command; the session time recorded in the accounting stop record is incorrect. This issue is seen only when the **aaa accounting session-duration ntp-adjusted** command is enabled via the CLI.

Workaround: Avoid using the **aaa accounting session-duration ntp-adjusted** command.

There are no known workarounds.

- CSCee33633

Cisco router running IOS versions 12.3(7)T may display the configuration of individual virtual-access interfaces or sub-interfaces in the running-configuration if the EXEC command **show running-config interface virtual-access** is executed.

There are no known workarounds.

- CSCee38105

Router crashed due to watchdog timeout.

This issue occurs when a policy is applied to a large number of PPP sessions using the virtual-template, the removal of the service-policy from the configuration will cause the router to crash.

There are no known workarounds.

- CSCee42660

With a auto-vc configuration and range-pv, using a trace back may occur by changing a pvc to a different class-vc with a different UBR+ speed:

```
-Traceback= 60140330 6014048C 60C1DC28 601EB508 601EB600 601EE1A4 601EE200
60356CB0 603588B0 603D20B8 603D209C
```

Afterwards, the pvc could go in a block state and the router eventually crash.

There are no known workarounds.

- CSCee45655

Even with the **snmp ifindex persist** command configured the c10000 does not ensure that the same ifindex number is used after a reboot.

There are no known workarounds.

- CSCee47898

On a p2p subinterface where range pvc is created, if we do any “do <exec command>” we see it displayed or applied 1 + number of vc in the range.

There are no known workarounds.

- CSCee57091

SSG redirection configuration does not kick in. This problem is present in a EFT image that we are testing.

There are no known workarounds.

- CSCee57149
 PPP users unable to login into services or PPP SSG user unable to login from SESM.
 This issue occurs when the port-bundle host key feature is enabled on the SSG, if a PPP SSG user logs out and tries to re-login from SESM, the user logon or service logon will fail.
 Workaround: Restart the PPP session and use will be able to login into services. relogin form SESM will also work if the port-map host-key feature is disabled.
- CSCee58039
 IP address may be allocated from the incorrect VPN when DHCP proxy client requests an IP address from a DHCP server which supports the VPN information option.
 This issue occurs when a DHCP server, which supports VPN information option (such as IOS DHCP server, CNR), uses the VPN information option to determine the address space for an address request. In the case of DHCP proxy client requesting an IP address for an interface which is configured with “ip vrf forwarding”, no VPN information option is sent, causes the DHCP server to allocate an IP address from the global, default address space.
 Workaround: Send VPN information option with the DHCP proxy client request if the interface is configured with “ip vrf forwarding”.
- CSCee66417
 The “possibly multiple users configuring IOS simultaneously” error message is seen when the router is reloaded and any PVC configuration is attempted to be changed.
 The exact message is as follows:

```
Unable to create PVC 0/33 on ATM5/0/0.1.Possibly multiple users configuring IOS
simultaneously
Further info about other user:
Process id: 3, Process: OSPF Hello 8, TTY: 0, Location: Console
```

 This issue occurs when range pvc configuration is present in the startup-configuration file on the router and it is reloaded this message is seen when PVC configuration is attempted to change.
 There are no known workarounds.
- CSCee69772
 No SNMP linkup or linkdown trap is generated for a 1CHOC12/4CHSTM1 SONET layer when a controller goes up and down.
 This issue is observed when monitoring a SNMP linkup or linkdown trap for a 1CHOC12/4CHSTM1 SONET layer.
 Workaround: Monitor the controller status using the **show controller sonet** command.
- CSCee72318
 Memory leaks occur on PTA or LAC when conducting PPPoA sessions. The leak size is consistent with the amount of sessions cycled in the system.
 There are no known workarounds.
- CSCin24544
 A permanent virtual connection (PVC) configuration is removed if a PVC fails when it is recreated.
 This issue is observed on a Cisco 7500 series that has a Versatile Interface Processor (VIP). The PVC configuration may be removed if the VIP is carrying data traffic and the parameters of the virtual circuit (VC) class that is attached to the configured PVCs on the associated interface are modified.
 There are no known workarounds.

- CSCin66969
IPCP may not come up when per-user virtual profile attributes are cloned from a remote AAA server. This issue is observed after a number of sessions are brought up and torn down and when a cloning failure is observed on one or more sessions.
There are no known workarounds.
- CSCin72029
A nas-port attribute of an accounting record points to an SESM interface rather than to the interface of the host.
This issue occurs under rare race conditions where there are host route changes at the time of the host logon.
There are no known workarounds.
- CSCin74759
The **radius-server vsa send cisco-nas-port** command cannot be unconfigured.
This issue occurs when the **radius-server vsa send** command is configured.
There are no known workarounds.
- CSCin74857
When the VSA2 is omitted via the “no radius-server vsa send cisco-nas-port” Radius aaa packets are being sent malformed.
This issue occurs when **radius-server vsa send** is enabled and the **no radius-server vsa send cisco-nas-port** command is invoked.
The following lists the running configs that causes this issue to occur:
 - radius-server vsa send accounting
 - radius-server vsa send authentication
 - no radius-server vsa-send cisco-nas-portWorkaround: Configure the **radius-server vsa send cisco-nas-port** command.
- CSCin75571
If the PVC is tried to be remove, the “Unable to delete PVC vpi/vci on ATMx/y. Possibly multiple users configuring IOS simultaneously” message appears.
This issue occurs if Auto VC is configured and is in INACTIVE state, or if the **create on-demand** command configured on this VC is removed.
There are no known workarounds.

Related Documentation

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

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

- [Release-Specific Documents, page 38](#)
- [Platform-Specific Documents, page 39](#)
- [Feature Modules, page 39](#)
- [Cisco IOS Software Documentation Set, page 40](#)

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(7)XI4*

As a supplement to the caveats listed in “[Caveats for Cisco IOS Release 12.3 XI](#)” 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 7200 VXR Installation and Configuration Guide*
- *Cisco 7200 Routers Quick Start Guide*
- *Cisco 7301 Installation and Configuration Guide*
- *Cisco 7301 Router Quick Start Guide*

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 by Cisco IOS Release 12.3(7)XI4 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

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

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:

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

On the Documentation CD-ROM at:

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

Cisco IOS Release 12.3 Documentation Set Contents

[Table 8](#) 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:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3

On the Documentation CD-ROM at:

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

Table 8 Cisco IOS Release 12.3 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	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</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2</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: Dial Access</i> • <i>Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications</i> • <i>Cisco IOS Dial Technologies Command Reference, Volume 1 of 2</i> • <i>Cisco IOS Dial Technologies Command Reference, Volume 2 of 2</i> 	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP Configuration Guide</i> • <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> • <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> • <i>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</i> 	IP Addressing IP 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> 	AppleTalk Novell IPX

Table 8 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<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> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i> • <i>Cisco IOS Voice, Video, and Fax Command Reference</i> 	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> 	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> 	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> 	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<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 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

Table 8 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<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 Error Messages</i> • <i>New Features in 12.3-Based Limited Lifetime Releases</i> • New Features in Release 12.3 T • Release Notes (Release note and caveat documentation for 12.3-based releases and various platforms) 	

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at <http://www.cisco.com>.

Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco products documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

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

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section on page 38.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0502R)

Copyright © 2003-2005
 Cisco Systems, Inc.
 All rights reserved.