



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

August 8, 2007

Cisco IOS Release 12.3(5a)B5

OL-4851-09

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.3(5a)B5. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(5a)B5, see the “[Caveats for Cisco IOS Release 12.3 B](#)” section on page 36 and *Caveats for Cisco IOS Release 12.3 T*. 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 T* located on Cisco.com and the Documentation CD-ROM.

Documentation Survey

Is Cisco documentation helpful? Click [here](#) to give us your feedback or go to the following URL to give us your feedback: <http://www.cisco.com/warp/public/732/docsurvey/rtg>.



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

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [Feature Support, page 12](#)
- [New and Changed Information, page 14](#)
- [MIBs, page 34](#)
- [Important Notes, page 35](#)
- [Caveats for Cisco IOS Release 12.3 B, page 36](#)
- [Related Documentation, page 96](#)
- [Obtaining Technical Assistance, page 103](#)

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3B and includes the following sections:

- [Memory Recommendations, page 2](#)
- [Supported Hardware, page 11](#)
- [Determining the Software Version, page 12](#)
- [Upgrading to a New Software Release, page 12](#)

Memory Recommendations

Table 1 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B5*

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
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	48 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	48 MB	128 MB	RAM

Table 1 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B5 (continued)*

Cisco 7300 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7301-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 56	c7301-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 3DES	c7301-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7301-g4js-mz	64 MB	128 MB	RAM	
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 56	c7400-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 3DES	c7400-jk9o3s-mz	64 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	64 MB	128 MB	RAM

Table 2 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B4*

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
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 56	c7200-jk8o3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 3DES	c7200-jk9o3s-mz	48 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	48 MB	128 MB	RAM

Table 2 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B4 (continued)*

Cisco 7300 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7301-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7301-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7301-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7301-g4js-mz	64 MB	128 MB	RAM	
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	64 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	64 MB	128 MB	RAM

Table 3 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B3*

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
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	48 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	48 MB	128 MB	RAM

Table 3 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B3 (continued)*

Cisco 7300 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7301-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7301-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7301-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7301-g4js-mz	64 MB	128 MB	RAM	
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	64 MB	128 MB	RAM	

Table 4 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B2*

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
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	48 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	48 MB	128 MB	RAM	

Table 4 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B2 (continued)*

Cisco 7300 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7301-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 56	c7301-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 3DES	c7301-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7301-g4js-mz	64 MB	128 MB	RAM	
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 56	c7400-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 3DES	c7400-jk9o3s-mz	64 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	64 MB	128 MB	RAM

Table 5 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B1*

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
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 56	c7200-jk8o3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPsec 3DES	c7200-jk9o3s-mz	48 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	48 MB	128 MB	RAM

Table 5 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B1 (continued)*

Cisco 7300 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7301-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7301-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7301-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7301-g4js-mz	64 MB	128 MB	RAM	
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	64 MB	128 MB	RAM	

Table 6 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B*

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
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	48 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	48 MB	128 MB	RAM	

Table 6 *Images and Memory Recommendations for Cisco IOS Release 12.3(5a)B (continued)*

Cisco 7300 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7301-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7301-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7301-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7301-g4js-mz	64 MB	128 MB	RAM	
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	64 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	64 MB	128 MB	RAM

Table 7 *Images and Memory Recommendations for Cisco IOS Release 12.3(3)B1*

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
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	48 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	48 MB	128 MB	RAM

Table 7 *Images and Memory Recommendations for Cisco IOS Release 12.3(3)B1 (continued)*

Cisco 7300 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7301-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7301-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7301-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7301-g4js-mz	64 MB	128 MB	RAM	
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	64 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	64 MB	128 MB	RAM

Table 8 *Images and Memory Recommendations for Cisco IOS Release 12.3(3)B*

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
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	48 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	48 MB	128 MB	RAM

Table 8 *Images and Memory Recommendations for Cisco IOS Release 12.3(3)B (continued)*

Cisco 7300 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7301-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7301-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7301-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7301-g4js-mz	64 MB	128 MB	RAM	
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	64 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	64 MB	128 MB	RAM

Table 9 *Images and Memory Recommendations for Cisco IOS Release 12.3(1a)B*

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
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	48 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	48 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	48 MB	128 MB	RAM

Table 9 *Images and Memory Recommendations for Cisco IOS Release 12.3(1a)B (continued)*

Cisco 7300 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7301-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7301-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7301-jk9o3s-mz	64 MB	128 MB	RAM
SSG Standard Feature Set	Enterprise SSG	c7301-g4js-mz	64 MB	128 MB	RAM	
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	64 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	64 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.3(5a)B5 supports the following Cisco 7000 family platforms:

- Cisco 7200 series routers (including the Cisco 7202, Cisco 7204, Cisco 7206, Cisco 7204VXR, and Cisco 7206VXR)
- Cisco 7301 routers
- Cisco 7304 routers
- Cisco 7401ASR routers

For detailed descriptions of the new hardware features, see the [“New and Changed Information”](#) section on page 14.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco family router, log in to the Cisco 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(5a)B5:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.3 B Software (c7200-is-mz), Version 12.3(5a)B5, RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

http://www.cisco.com/en/US/customer/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml

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 is a list of the new hardware and software features supported by the Cisco 7000 family for Cisco IOS Release 12.3 B.

New Hardware Features in Cisco IOS Release 12.3(5a)B5

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B5.

New Software Features in Cisco IOS Release 12.3(5a)B5

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B5.

New Hardware Features in Cisco IOS Release 12.3(5a)B4

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B4.

New Software Features in Cisco IOS Release 12.3(5a)B4

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B4.

New Hardware Features in Cisco IOS Release 12.3(5a)B3

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B3.

New Software Features in Cisco IOS Release 12.3(5a)B3

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B3.

New Hardware Features in Cisco IOS Release 12.3(5a)B2

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B2.

New Software Features in Cisco IOS Release 12.3(5a)B2

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B2.

New Hardware Features in Cisco IOS Release 12.3(5a)B1

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B1.

New Software Features in Cisco IOS Release 12.3(5a)B1

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B1.

New Hardware Features in Cisco IOS Release 12.3(5a)B

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B.

New Software Features in Cisco IOS Release 12.3(5a)B

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.3(5a)B.

New Hardware Features in Cisco IOS Release 12.3(3)B1

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.3(3)B1.

New Software Features in Cisco IOS Release 12.3(3)B1

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.3(3)B1.

New Hardware Features in Cisco IOS Release 12.3(3)B

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.3(3)B.

New Software Features in Cisco IOS Release 12.3(3)B

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.3(3)B:

Attribute Screening for Access Requests

Platforms: Cisco 7200 series routers, Cisco 7301 routers, Cisco 7304 routers, and Cisco 7401 ASR routers

Attribute Screening for Access Requests features allows you to configure your network access server (NAS) to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization.

RADIUS NAS-IP-Address Attribute Configurability

Platforms: Cisco 7200 series routers and Cisco 7401 ASR routers

The RADIUS NAS-IP-Address Attribute Configurability feature allows you to configure an arbitrary IP address to be used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets. This feature may be used for situations in which service providers are using a cluster of small network access servers (NASs) to simulate a large NAS to improve scalability. This feature allows the NASs to behave as a single RADIUS client from the perspective of the RADIUS server.

SSG Default DNS Redirection

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

The SSG Default DNS Redirection feature allows a default Domain Name System (DNS) domain to be configured in a service profile. When a default DNS domain is configured, all DNS queries that do not match a service with a specific domain name will be redirected to the DNS server for a default service.

SSG Enhancements

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG Enhancements describes Layer 2 Tunneling Protocol (L2TP) enhancements for authentication, service logon, and the interface between the Service Selection Gateway (SSG) and the Subscriber Edge Services Manager (SESM). For Release 12.3(3)B, SSG enhancements include a new Account-Info vendor specific attribute (VSA), Account-Accept VSA, and Service-Accept VSA.

The SSG interacts with the SESM, through a Remote Authentication Dial-in User Service (RADIUS) interface. SSG Enhancements describe the enhancements to the RADIUS interface to allow a separate Mobile Station ISDN Number (MSISDN) and Challenge Handshake Authentication Protocol (CHAP) for service logon. The SSG Enhancements documentation also describes error codes in the SSG response to the SESM.

For more information, see the SSG Enhancements feature at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/1231abw/ssgenh.htm>

SSG Permanent TCP Redirection

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

The SSG Permanent TCP Redirection feature enables Service Selection Gateway (SSG), in conjunction with Cisco Subscriber Edge Services Manager (SESM), to provide service selection support to users whose web browsers are configured with HTTP proxy servers. This feature supports plug-and-play functionality in Public Wireless LANs.

SSG TCP Redirect Enhancements

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

The TCP Redirect feature is enhanced to allow access lists to be associated with server groups. This enhancement can be used to limit the kind of traffic that is redirected based on the source or destination IP address and/or TCP ports. It can also be used to redirect different sets of users to different dashboards for unauthenticated user and unauthorized service redirection.

For more information, see the SSG TCP Redirect Enhancements feature at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/1231abw/tcpdrct.htm>

SSG Transparent Auto-Logon

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

The SSG Transparent Auto-Logon (TAL) feature enables the Service Selection Gateway (SSG) to authenticate/authorize users based on IP packets received from the user. SSG authorizes users by using information from the Authentication, Authorization, and Accounting (AAA) server when a first IP packet is received from the user.

Users can be activated on SSG through Web-based login procedures using Service Edge Subscriber Management (SESM), RADIUS Proxy, and PPP session termination. The Transparent Auto-Logon feature provides an additional activation method. Transparent Auto-Logon provides SSG services to a user who is authorized based on the source IP address of packets received on a downlink interface of SSG, without any previous authentication phase.

For more information on the Transparent Auto-Logon feature, see the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/1231abw/autologn.htm>

New Hardware Features in Cisco IOS Release 12.3(1a)B

The following new hardware feature is supported by the Cisco 7000 for Cisco IOS Release 12.3(1a)B:

Cisco 7301 Router Platform

Platforms: Cisco 7301 routers

The Cisco 7301 router provides application-specific features for broadband subscriber aggregation and network application services with high processing performance.

Each Cisco 7301 router consists of the following features:

- Small form-factor—One rack-unit (RU) high with stacking capability: 1.72 in. x 17.3 in. x 13.87 in. (4.27 cm x 43.9 cm x 30 cm). The weight is approximately 10.5 lbs (4.76 kg).
- Three native Gigabit Ethernet interfaces—six ports:
 - Three optical fiber Gigabit Ethernet (1000 Mbps) ports that use a small form factor pluggable (SFP) Gigabit Interface Converters (GBICs) with LC connectors
 - Three Gigabit Ethernet (10/100/1000 Mbps) ports with RJ-45 connectors (Any three ports are available at any one time)
- Both 25-MHz and 50-MHz port adapter operation
- A 64- or 128-MB CompactFlash Disk
- Two SFP GBIC modules: SX and LH options
- Power supplies:
 - Single or dual AC power supplies
 - Single 24V DC power supply
 - Dual 48V DC power supply

- BCM 1250 microprocessor that operates at an internal clock speed of 700 MHz
- 512-KB Boot ROM
- 32-MB Boot Flash
- Three SDRAM memory options: 256 MB, 512 MB, and 1 GB
- Auxiliary port
- Console port
- Online insertion and removal (OIR)—Allows you to add, replace, or remove port adapters with minimal interruption of the system
- Environmental monitoring and reporting functions—Allow you to maintain normal system operation by resolving adverse environmental conditions prior to loss of operation
- Downloadable software—Allows you to load new images into Flash memory remotely, without having to physically access the router, for fast, reliable upgrades

Front-to-back airflow—Allows you to mount the router from either front or back into 19-inch two-post racks and 21-23 inch four-post racks

New Software Features in Cisco IOS Release 12.3(1a)B

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.3(1a)B:

EAP SIM Enhancements

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

EAP SIM Enhancements

Two EAP-SIM enhancements for Pebble Beach 1.1 solution 1. AZR issue: SSG to cleanup the active hosts (EAP-SIM and SESM) users on receiving an Accounting On/Off from AZR due to a reboot. This is needed to close a security hole where an illegal user can hijack the session of a valid user by using the IP address of the valid user after the AZR reboot.

2. SESM reconnect for EAP-SIM users: This requires that EAP-SIM users access the SESM and perform an Account Logoff. Subsequent to the logoff they can access the SESM and do an account logon again.

IP Pool Backup

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

The IP Pool Backup feature introduces two new interface configuration commands, **peer pool backup** and **peer pool static**, which allow you to define alternate sources for IP address pools in the event the original address pool is not present or is exhausted.

The **peer pool backup** command is useful in large-scale dial-out environments with large numbers of independently controlled authentication, authorization, and accounting (AAA) servers that can make it difficult for the network access server (NAS) to provide proper IP address pool resolution in the following cases:

- A new pool name is introduced by one of the AAA servers before that pool is set up on the NAS.
- An existing local pool becomes exhausted, but the owner of that AAA server has other pools that would be acceptable as an IP address source.

The **peer pool backup** command uses the local pool names configured with the **peer default ip address pool** interface configuration command to supplement the pool names supplied by AAA. The problems of pool name resolution and specific local pool exhaustion can be solved by configuring backup pool names on a per-interface basis using the **peer default ip address pool** and **peer pool backup** interface configuration commands.

The **peer pool static** command controls attempts by the pool software to load dynamic pools in response to a pool request from a specific interface. These dynamic pools are loaded at system startup and refreshed whenever a pool name not configured on the NAS is specified for IP address allocation. Because the behavior of the NAS in response to a missing pool name can be changed using the **peer pool backup** interface configuration command, you can use the **peer pool static** command to control attempts to load all dynamic pools when the AAA-supplied pool name is not an existing local pool name.

MQC Hierarchical Shaping in PXF

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

MQC Hierarchical Shaping in PXF implements Modular Quality Of Service Command-Line Interface (MQC) hierarchical shaping in the Parallel Express Forwarding (PXF) path.

PXF

The Parallel Express Forwarding (PXF) processor enables parallel IP multipacket processing functions, working with the Route Processor (RP) to provide accelerated packet switching, as well as accelerated IP Layer 3 feature processing.

For more information about PXF, including troubleshooting information, refer to the [Cisco 7401ASR Installation and Configuration Guide](#).

MQC

Modular Quality of Service Command Line Interface (MQC) is designed to simplify the configuration of Quality of Service (QoS) on Cisco routers and switches by defining a common command syntax and resulting set of Quality of Service (QoS) behaviors across platforms. This model replaces the previous model of defining unique syntaxes for each QoS feature and for each platform.

The MQC contains the following three steps:

- Define a traffic class by issuing the **class-map** command.
- Create a traffic policy by associating the traffic class with one or more QoS features by issuing the **policy-map** command.
- Attach the traffic policy to the interface, subinterface, or virtual circuit (VC) by issuing the **service-policy** command.

For more information about MQC, refer to the [Modular Quality of Service Command-Line Interface](#) document.

Hierarchical Shaping

Using hierarchical shaping, it is possible to configure a group of classes to which class-based weighted fair queueing (CBWFQ) is applied within that group of classes. These separate classes can then be treated as an aggregate class for the purpose of shaping amongst other classes.

For more information about other QoS features supported by PXF, see the “Quality of Service Features for Parallel Express Forwarding” section of the [Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 B](#) for Cisco IOS Release 12.2(4)B.

Multilink PPP Minimum Links Mandatory

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

Multilink PPP allows multiple PPP links to be established in parallel to the same destination. Multilink PPP is often used with dialup lines or ISDN connections to easily increase the amount of bandwidth between points.

With the introduction of the Multilink PPP Minimum Links Mandatory feature, you can configure the minimum number of links in a Multilink PPP (MLP) bundle required to keep that bundle active by entering the **ppp multilink min-links links mandatory** command. When you configure this command, all Network Control Protocols (NCPs) for an MLP bundle are disabled until the MLP bundle has the required minimum number of links. When a new link is added to the MLP bundle that brings the number of links up to the required minimum number of links, the NCPs are activated for the MLP bundle. When a link is removed from an MLP bundle, and the number of links falls below the required minimum number of links for that MLP bundle, the NCPs are disabled for that MLP bundle.

PPPoE Session Limit Per NAS Port

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

Using the PPPoE Session Limit Per NAS Port feature, you can limit the number of sessions on a specific virtual circuit (VC) or VLAN configured on an L2TP access concentrator (LAC). The NAS port is either an ATM VC or a configured VLAN ID.

The PPPoE session limit per NAS port is maintained in a RADIUS server customer profile database. This customer profile database is connected to a LAC and is separate from the RADIUS server that the LAC and L2TP Network Server (LNS) use for the authentication and authorization of incoming users. When the customer profile database receives a pre-authorization request from the LAC, it sends the PPPoE per NAS port session limit to the LAC.

The LAC sends a pre-authorization request to the customer profile database when the LAC is configured for Subscriber Service Switch (SSS) pre-authorization. Configure the LAC for SSS pre-authorization using the `sss-subscriber access pppoe pre-authorize` command. When the LAC receives the PPPoE per NAS port session limit from the customer profile database, the LAC compares the PPPoE per NAS port session limit to the number of sessions currently on the NAS port. The LAC then decides whether to accept or reject the current call based upon the configured PPOE per NAS port session limit and the number of calls currently on the NAS port.

You can configure other types of session limits on the LAC including session limit per VC, per VLAN, per MAC, or a global session limit for the LAC. When PPPoE Session Limit Per NAS Port is enabled (that is, when you have enabled SSS pre-authorization on the LAC), local configurations for session limit per VC and per VLAN are overwritten by the PPPoE per NAS port session limit downloaded from the customer profile database. Configured session limits per VC and per VLAN serve as backups in case of a PPPoE per NAS port session limit download failure.

The customer profile database consists of user profiles for each user connected to the LAC. Each user profile contains the NAS-IP-Address (Attribute #4) and the NAS-Port-ID (Attribute #5.) When the LAC is configured for SSS pre-authorization, it queries the customer profile database using the username. When a match is found in the customer profile database, the customer profile database sends the PPPoE per NAS port session limit in the user profile. The PPPoE per NAS port session limit is defined in the username as a Cisco AVpair.

RFC-2867 RADIUS Tunnel Accounting

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

The RFC-2867 RADIUS Tunnel Accounting feature introduces six new RADIUS accounting types that are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop). These new accounting types are designed to support the provision of compulsory tunneling in dialup networks; that is, these attribute types allow you to better track tunnel status changes.

This feature also introduces two new commands—`vpdn session accounting network (tunnel-link-type records)` and `vpdn tunnel accounting network (tunnel-type records)`—that help identify the following events:

- A virtual private dialup network (VPDN) tunnel is brought up or destroyed
- A request to create a VPDN tunnel is rejected
- A user session within a VPDN tunnel is brought up or brought down
- A user session create request is rejected



Note

The first two events are tunnel-type accounting records: authentication, authorization, and accounting (AAA) sends Tunnel-Start, Tunnel-Stop, or Tunnel-Reject accounting records to the RADIUS server. The next two events are tunnel-link-type accounting records: AAA sends Tunnel-Link-Start, Tunnel-Link-Stop, or Tunnel-Link-Reject accounting records to the RADIUS server.



Note

The accounting types are divided into two separate tunnel types so users can decide if they want tunnel type, tunnel-link type, or both types of accounting.

Service Selection Gateway

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Autologoff Enhancement

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

The SSG Autologoff Enhancement feature configures Service Selection Gateway (SSG) to check the MAC address of a host each time that SSG performs an Address Resolution Protocol (ARP) ping. If SSG finds that the MAC address of the host has changed, SSG automatically initiates the logoff of that host. This prevents unauthorized reuse of IP addresses (spoofing). SSG MAC address checking also detects the assignment of a host IP address to a different host before the original hosts initiates a logoff and clears its host object. This prevents session reuse by a second host.

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

ARP Ping

The ARP is an Internet protocol used to map IP addresses to MAC addresses in directly connected devices. A router that uses ARP will broadcast ARP requests for IP address information. When an IP address is successfully associated with a MAC address, the router stores the information in the ARP cache.

When SSG Autologoff is configured to use ARP ping, SSG periodically checks the ARP cache tables. If a table entry for a host is found, SSG forces ARP to refresh the entry and checks the entry again after a configured interval. If a table entry is not found, SSG initiates autologoff for the host. However, if any data traffic to or from the host occurred during the interval, SSG does not ping the host because the reachability of the host during that interval was established by the data traffic.

When SSG MAC address checking is configured, SSG checks the MAC address of a host when an ARP ping is performed. If SSG detects a different host MAC address, it initiates an automatic logoff of that host.



Note

ARP ping should be used only in deployment scenarios in which all hosts are directly connected to SSG through a broadcast interface such as an Ethernet interface or a bridged interface such as a routed bridge encapsulation (RBE) or integrated routing and bridging (IRB) interface.

ARP request packets are smaller than Internet Control Message Protocol (ICMP) ping packets, so it is recommended that you configure SSG Autologoff to use ARP ping in scenarios where hosts are directly connected.

SSG Complete ID

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Complete ID

SSG Complete ID provides enhancements to the current interaction mechanism that is used between SSG and SESM, allowing SSG to pass along the following additional information:

- Client IP Address
- Client MAC Address
- Subinterface
- VPI/VCI
- MSISDN

This allows SESM to offer greater customization of Web portals, specifically by locations. Each hotspot can now have its own branded portal.

SSG EAP Transparency

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG EAP Transparency

The SSG EAP Transparency feature allows SSG to transparently pass EAP-SIM, EAP-TLS and Cisco LEAP authentication.

SSG Open Garden Configuration Enhancements

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Open Garden Configuration Enhancements

The Service Selection Gateway (SSG) is an IOS feature and implements layer 3 service selection through selective routing of IP packets to destination networks on a per subscriber basis. Out of the many features SSG has, Open Garden is one of the features, which is very useful for service providers to provide trial-based services to the customers.

An open garden is a collection of web sites that a user can access as long as the user has physical access to the network. The user doesn't need to provide any authentication information before accessing the Web sites in the open garden.

Currently, SSG open garden services can be configured/managed on the router itself, even though they are similar to normal SSG (subscribed) services. The modifications being proposed will allow open garden services to be defined and managed on the RADIUS server as well.

SSG L2TP Dialout

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG L2TP Dialout

The SSG L2TP Dialout feature enhances SSG tunnel services and provides a dialout facility to users. Many Small Office Home Offices (SOHOs) use the Public Switched Telephone Network (PSTN) to access their intranet. SSG L2TP provides mobile users with a way to securely connect to their SOHO through the PSTN.

To provide SSG L2TP Dialout, SSG requires a digital number identification service (DNIS) number for the SOHO to which the user wants to connect, the address of the L2TP Access Concentrator (LAC) closest to the SOHO, and configured tunnel parameters to establish a tunnel to the LAC.

Users can access SSG L2TP Dialout by selecting the dialout service using Cisco Subscriber Edge Services Manager (SESM) from the list of subscribed services or by using a structured username. The user must provide the DNIS number when using either method of connecting to the dialout service.

SSG Prepaid Enhancements

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Prepaid

The SSG Prepaid feature allows SSG to check a subscriber's available credit to determine whether to connect the subscriber to a service and how long the connection can last. The subscriber's credit is administered by the billing server as a series of quotas representing either a duration of use (in seconds) or an allowable data volume (in bytes). A quota is an allotment of available credit.

To obtain the first quota for a connection, SSG submits an authorization request to the authentication, authorization, and accounting (AAA) server. The AAA server contacts the prepaid billing server, which forwards the quota values to SSG. SSG then monitors the connection to track the quota usage. When the quota runs out, SSG performs reauthorization. During reauthorization, the billing server may provide SSG with an additional quota if there is available credit. If no further quota is provided, SSG logs off the user.

For more information refer to the [SSG Prepaid](#) document.

SSG Prepaid Enhancements

SSG Prepaid Enhancements introduces prepaid tariff switching, simultaneous volume and time based prepaid billing, and postpaid tariff Switching.

SSG Prepaid Idle Timeout

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Prepaid

The SSG Prepaid feature allows SSG to check a subscriber's available credit to determine whether to connect the subscriber to a service and how long the connection can last. The subscriber's credit is administered by the billing server as a series of quotas representing either a duration of use (in seconds) or an allowable data volume (in bytes). A quota is an allotment of available credit.

To obtain the first quota for a connection, SSG submits an authorization request to the authentication, authorization, and accounting (AAA) server. The AAA server contacts the prepaid billing server, which forwards the quota values to SSG. SSG then monitors the connection to track the quota usage. When the

quota runs out, SSG performs reauthorization. During reauthorization, the billing server may provide SSG with an additional quota if there is available credit. If no further quota is provided, SSG logs off the user.

For more information refer to the *SSG Prepaid* document.

SSG Prepaid Idle Timeout

The SSG Prepaid Idle Timeout feature enhances the SSG Prepaid feature by enabling SSG to return residual quota to the billing server from services that a user is logged into but not actively using. The quota that is returned to the billing center can be applied to the quota for the services the user is actively using.

When SSG is configured for SSG Prepaid Idle Timeout, a user's connection to services can be open even when the billing server returns a zero quota, but the connection's status is dependent on the combination of the quota and the idle timeout value returned. Depending on the connection service, SSG requests the quota for a connection from the billing server once the user starts using a particular service, when the user runs out of quota, or after the configured idle timeout value has expired.

The SSG Prepaid Idle Timeout feature enhances handling of a returned zero quota from the billing server. If a billing server returns a zero quota, and non-zero idle timeout, this indicates that a user has run out of credit for a service. When a user runs out of credit for a service, the user is redirected to the billing server to replenish the quota. When the user is redirected to the billing server, the user's connection to the original service or services is retained. Although the connection remains up, any traffic passing through the connection is dropped. This enables a user to replenish quota on the billing server without losing connections to services or having to perform additional service logons.

Using the SSG Prepaid Idle Timeout feature, you can configure SSG to reauthorize a user before the user completely consumes the allocated quota. You can also configure SSG to not pass traffic during reauthorization. This prevents revenue leaks in the event that the billing server returns a zero quota for the user. Without the SSG Prepaid Idle Timeout feature, traffic passed during reauthorization represents a revenue leak if the billing server returns a zero quota for the user. You can prevent this type of revenue leak by configuring a threshold value, causing SSG to reauthorize a user's connection before the user completely consumes the allocated quota for a service.

SSG Prepaid Idle Timeout enhances SSG to inform the billing server upon any connection failure. This enables the billing server to free quota that was reserved for the connection that failed and to apply this quota immediately to some other active connection.

SSG Proxy for CDMA2000

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

The SSG Proxy for CDMA2000 extends the functionality of the existing SSG RADIUS Proxy so that it may be used in CDMA2000 networks.

When used in a CDMA2000 network, SSG provides RADIUS proxy services to the Packet Data Serving Node (PDSN) and the Home Agent (HA) for both Simple IP and Mobile IP authentication. SSG also provides service selection management and policy-based traffic direction for subscribers.

SSG Proxy for CDMA2000, used with Cisco Subscriber Edge Services Manager (SESM), provides users with on-demand services and service providers with service management and subscriber management.

SSG Proxy for CDMA2000 supports time- and volume-based usage accounting for Simple IP and Mobile IP sessions. Prepaid and postpaid services are supported. Host accounting records can be sent to multiple network elements including Content Service Gateways (CSGs), Content Optimization Engines (COEs), and Wireless Application Protocol (WAP) gateways.

CDMA

Code Division Multiple Access (CDMA) is a digital spread-spectrum modulation technique used mainly with personal communications devices such as mobile phones. CDMA digitizes the conversation and tags it with a special frequency code. The data is then scattered across the frequency band in a pseudorandom pattern. The receiving device is instructed to decipher only the data corresponding to a particular code to reconstruct the signal.

CDMA2000

CDMA2000 Radius Transmission Technology (RTT) is a wideband, spread-spectrum radio interface that uses CDMA technology to satisfy the needs of Third generation (3G) wireless communication systems. CDMA2000 is backward compatible with CDMA.

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Proxy for CDMA2000 for Simple IP

When used in a CDMA2000 environment, SSG acts as a RADIUS proxy to the Packet Data Serving Node (PDSN) and to the Home Agent for Simple IP authentication. SSG sets up a host object for the following three different access modes:

- PAP/CHAP authentication. In this mode, Password Authentication Protocol/ Challenge Handshake Authentication Protocol (PAP/CHAP) is performed during PPP setup and the NAI is received from a mobile node (MN).
- MSID-Based Access. In this mode, the MN does not negotiate CHAP or PAP and no Network Access Identifier (NAI) is received by the PDSN. The PDSN does not perform additional authentication. PDSN constructs an NAI based on the MSID and generates accounting records. Because a user password is not available from the MN, a globally configured password is used as the service password.
- MSID-Based Access-Cisco Variant. In this mode, a Cisco PDSN supports MSID-based access by using a realm retrieved from the RADIUS server. This realm is retrieved during an extra authentication phase with the RADIUS server.

SSG operating in a CDMA2000 network correlates Accounting-Start and Accounting-Stop requests. A PDSN may send out many Accounting-Start and Accounting-Stop requests during a session. These Accounting-Start and Accounting-Stop requests can be generated by PDSN hand-off, Packet Control Function (PCF) hand-off, interim accounting, and time-of-date accounting. SSG terminates a session only when it receives an Accounting-Stop request with the 3GPP2-Session-Continue VSA set to "FALSE" or if a subsequent Accounting-Start request is not received within a configured timeout. PPP renegotiation during a PDSN hand-off is treated as a new session.

In SSG Proxy for CDMA2000 for Simple IP, the end-user IP address may be assigned statically by the PDSN, RADIUS server, or SSG. The end-user IP address can also be assigned directly from the automain service.

Network Address Translation (NAT) is automatically performed when necessary. NAT is generally necessary when IP address assignment is performed by any mechanism other than directly from the automain service (which may be a VPN). You can also configure SSG to always use NAT.

If the user profile contains Cisco Attribute-Value (AV)-pairs of Virtual Private Dialup Network (VPDN) attributes, SSG initiates Layer 2 Tunneling Protocol (L2TP) VPN.

SSG Proxy for CDMA2000 for Mobile IP

For Mobile IP, SSG functions as the RADIUS proxy for both PDSN and the HA. SSG proxies PPP PAP or CHAP and Mobile Node (MN)/Foreign Agent (FA) CHAP authentication. SSG Proxy for CDMA2000 for Mobile IP can assign IP addresses statically by the PDSN, RADIUS server, or SSG. The end user IP address can also be assigned directly from the autodomains service.

Home Agent-Mobile Node (HA-MN) authentication and reverse tunneling must be enabled so that SSG can create host objects for Mobile IP sessions based on proxied RADIUS packets received from the HA.

The Home Agent must generate RADIUS accounting packets so that SSG can discover the user IP address and detect the termination of the session. Multiple Mobile IP sessions with the same NAI are supported. RADIUS packets must contain the Accounting-Session-ID attribute to be associated with the correct user session. SSG correlates RADIUS packets from the PDSN in order to obtain MSID information for a host object of a Mobile IP session.

SSG can set up a host object either with or without PAP/CHAP performed during the original PPP session.

SSG initiates L2TP VPN according to the SSG tunnel service VSAs in the user's profile. If the user profile contains Cisco AV-pairs of VPDN, SSG sets up the L2TP tunnel per these VPDN attributes. SSG removes these AV-pairs when sending the Access-Accept packet back to the PDSN.

Either the HA or the RADIUS server can assign the user's IP address.

Dynamic Home Agent Assignment

Dynamic HA assignment based on a mobile user's location is supported.

SSG Proxy for CDMA2000 provides three options for dynamic HA assignment:

- The RADIUS server selects the local HA or any HA that is configured for session requests. For foreign-user call requests, the AAA server assigns the HA.
- SSG modifies the fixed HA address received from the RADIUS server to a local HA address. This method can be implemented without making any changes to the RADIUS server configuration. SSG does not modify the HA address for a foreign user. The foreign-user call request is registered with the HA address assigned by the AAA server.
- The PDSN implements dynamic HA assignment based on detection of the PDSN hand-off.

Multiple RADIUS Server Support

SSG Proxy for CDMA2000 provides geographical redundancy by copying host object accounting packets and sending them to multiple RADIUS servers.

SSG PTA-MD Exclusion Lists

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

Beginning in Cisco IOS Release 12.2(8)B, the option of passing the entire structured username in the form 'user@service' to PPP for authenticating an SSG request became available. The entire structured username can be passed to PPP through the use of a PTA-MD exclusion list; if an entire structured username should be passed to PPP, the domain (the '@service' portion of the structured username) should be added to a PTA-MD exclusion list. The PTA-MD exclusion list can be configured on the AAA server directly or via the router CLI. Structured usernames are parsed for authentication unless a PTA-MD exclusion list is configured for the particular domain requesting a service.

For additional information on SSG PTA-MD Exclusion Lists, see to the [Service Selection Gateway](#) feature module.

SSG Range Command for Bind Statements

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Range Command for Bind Statements

SSG Range Command for Bind Statements creates a A "range" command for SSG BIND statements. This is useful when provisioning RBE subscribers en masse, as it allows for streamlined provisioning and configuration with a decreased CPU load.

SSG Service Profile Caching

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

The SSG Service Profile Caching feature enhances the authentication process for SSG services by allowing users to authenticate a service using the service profile cached in SSG.

When SSG Service Profile Caching is not enabled, an authentication, authorization, and accounting (AAA) transaction is required to download a service profile each time an SSG subscriber logs onto the service. The other SSG subscribers already logged onto the service also have their service parameters automatically refreshed as a result of this AAA transaction. In many cases, this automatic refresh causes unnecessary traffic in SSG and on the AAA server.

The SSG Service Profile Caching feature creates a cache of service profiles in SSG. A service profile is downloaded from the AAA server and then stored in the SSG service profile cache as a service-info object. Subsequent SSG subscribers hoping to use that service are authorized by the SSG service profile cache provided that service profile remains in the cache. To ensure that the service profiles in the SSG service profile cache remain updated, the SSG service profile cache automatically refreshes the service profiles by downloading the service profiles from the AAA server at user-configured intervals (the default is every 120 minutes). SSG service profile caches can also be refreshed manually at any time. Service profiles that are not being used by any SSG subscriber are removed from the SSG service profile cache.

SSG Support of NAS Port ID

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Support of NAS Port ID

This feature will carry the NAS-Port attribute in the authentication packet. This will allow the authentication server to use consistent policies while authenticating PPPoX users and RFC1483 users. Currently, NAS-Port attribute is sent only for PPPoX users.

With this feature, SSG will send nas-port information for certain IP users in the authentication-request and accounting-request packets.

SSG Suppression of Unused Accounting Records

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Suppression of Unused Accounting Records

The SSG Suppression of Unused Accounting Records feature provides the ability to turn off those accounting records that are not needed on the router.

SSG Unconfig

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Unconfig

The SSG Unconfig feature enhances your ability to disable SSG at any time and releases the data structures and system resources created by SSG when SSG is unconfigured.

The SSG Unconfig feature enhances several IOS commands to delete all host objects, delete a range of host objects. You can also delete all service objects or connection objects. The **show ssg host** command has been enhanced to display information about an interface and its IP address when Host-Key mode is enabled on that interface.

System Resource Cleanup When SSG Is Unconfigured

When you enable SSG, the SSG subsystem in IOS acquires system resources that are never released, even after you disable SSG. The SSG Unconfig feature enables you to release and clean up system resources when SSG is not in use by entering the **no ssg enable force-cleanup** command.

SSG Unique Session ID

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

SSG Unique Session ID

SSG does not currently support a totally unique accounting session ID in the RADIUS accounting records. The SSG Unique Session ID feature provides a unique format in the RADIUS accounting records in order to be compatible with a customer's existing backend billing systems.

VRF in PXF

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR routers

VRF in PXF implements Virtual Route Forwarding (VRF) in the Parallel Express Forwarding (PEF) path.

PEF

The Parallel Express Forwarding (PEF) processor enables parallel IP multipacket processing functions, working with the Route Processor (RP) to provide accelerated packet switching, as well as accelerated IP Layer 3 feature processing.

For more information about PEF, including troubleshooting information, refer to the [Cisco 7401ASR Installation and Configuration Guide](#).

MQC

Modular Quality of Service Command Line Interface (MQC) is designed to simplify the configuration of Quality of Service (QoS) on Cisco routers and switches by defining a common command syntax and resulting set of Quality of Service (QoS) behaviors across platforms. This model replaces the previous model of defining unique syntaxes for each QoS feature and for each platform.

The MQC contains the following three steps:

- Define a traffic class by issuing the **class-map** command.
- Create a traffic policy by associating the traffic class with one or more QoS features by issuing the **policy-map** command.
- Attach the traffic policy to the interface, subinterface, or virtual circuit (VC) by issuing the **service-policy** command.

For more information about MQC, refer to the [Modular Quality of Service Command-Line Interface](#) document.

Hierarchical Shaping

Using hierarchical shaping, it is possible to configure a group of classes to which class-based weighted fair queueing (CBWFQ) is applied within that group of classes. These separate classes can then be treated as an aggregate class for the purpose of shaping amongst other classes.

For more information about other QoS features supported by PXF, see the “[Quality of Service Features for Parallel Express Forwarding](#)” section of the *Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 B* for Cisco IOS Release 12.2(4)B.

VRF

A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table (which includes forwarding information base [FIB] and Adjacency tables), and a set of interfaces that use this forwarding table. A VRF consists of the following:

- IP routing table
- Cisco Express Forwarding (CEF) table
- Set of interfaces that use the CEF forwarding table
- Set of rules and routing protocol parameters to control the information in the routing tables

VRF PXF offloads any VRF-related routing from the Route Processor (RP) to the PXF.

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 10](#).

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

Deprecated MIB	Replacement
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

Important Notes

CSCin49938 SSG: not accepting service real-ip

Effective with Cisco IOS Release 12.3(3)B1, Service Selection Gateway (SSG) supports the use of the IP address pool name vendor-specific attribute (VSA) in Access Accept packets from the authentication, authorization, and accounting (AAA) server for proxy services. When the AAA server provides the IP address pool name, SSG chooses one IP address from the pool to be used as the service IP address. The **show ssg connection** command with the *host-ip service-name* arguments can be used to display the IP pool name received from the AAA server.

The format of the IP address pool name VSA is as follows: `cisco-av-pair=ip:addr-pool=<pool-name>`.

SSG also allows the IP address pool name VSA to be configured in the local service profile for pass-through and proxy services. With this configuration, SSG chooses one IP address from the pool as the service IP address and performs Network Address Translation (NAT) between the user's actual IP address and the IP address of the service. Note that for proxy services, the IP address or IP address pool name that comes from the remote AAA server takes precedence over the pool name configured in the service profile. The **show ssg service service-name** command can be used to display the pool name configured in the service profile.

Caveats for Cisco IOS Release 12.3 B

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.

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

All caveats in Cisco IOS Release 12.3 are also in Cisco IOS Release 12.3 T.

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

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(3)B.

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

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



Note

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

Table 10 Caveats Reference for Cisco IOS Release 12.3 B

DDTS Number	Open in Release	Resolved in Release
CSCdv51281		12.3(5a)B1
CSCdw85843		12.3(1a)B
CSCdx55178		12.3(1a)B
CSCdx95455		12.3(1a)B
CSCdz33874		12.3(1a)B
CSCdz54555	12.3(1a)B	
CSCdz74721		12.3(1a)B
CSCea12794		12.3(1a)B
CSCea22552		12.3(3)B
CSCea25622		12.3(1a)B
CSCea26993		12.3(1a)B
CSCea31186		12.3(1a)B

Table 10 **Caveats Reference for Cisco IOS Release 12.3 B**

CSCea40426		12.3(1a)B
CSCea42223		12.3(1a)B
CSCea44460		12.3(5a)B1
CSCea51540		12.3(1a)B
CSCea53821		12.3(1a)B
CSCea55600		12.3(1a)B
CSCea56667		12.3(1a)B
CSCea56700		12.3(1a)B
CSCea56883		12.3(5a)B3
CSCea57826		12.3(3)B
CSCea61004		12.3(1a)B
CSCea63499		12.3(5a)B1
CSCea64506		12.3(1a)B
CSCea65313		12.3(1a)B
CSCea66194		12.3(1a)B
CSCea66267		12.3(3)B
CSCea66336		12.3(1a)B
CSCea67382		12.3(1a)B
CSCea67751		12.3(1a)B
CSCea70033		12.3(1a)B
CSCea70473		12.3(1a)B
CSCea70885		12.3(1a)B
CSCea71776		12.3(1a)B
CSCea72908		12.3(1a)B
CSCea73696		12.3(1a)B
CSCea77302		12.3(1a)B
CSCea78932		12.3(1a)B
CSCea79610		12.3(1a)B
CSCea84092		12.3(5a)B
CSCea86300		12.3(1a)B
CSCea88409		12.3(1a)B
CSCea90941		12.3(1a)B
CSCea91695		12.3(1a)B
CSCea91920		12.3(1a)B
CSCea93108		12.3(1a)B
CSCea93882		12.3(1a)B
CSCeb00104		12.3(1a)B

Table 10 Caveats Reference for Cisco IOS Release 12.3 B

CSCeb00875		12.3(1a)B
CSCeb01583		12.3(1a)B
CSCeb01888		12.3(1a)B
CSCeb06567		12.3(1a)B
CSCeb09370		12.3(1a)B
CSCeb60929		12.3(5a)B1
CSCeb61701		12.3(1a)B
CSCeb18293		12.3(1a)B
CSCeb21064		12.3(3)B
CSCeb24206		12.3(5a)B
CSCeb26162		12.3(1a)B
CSCeb35210		12.3(3)B
CSCeb43378		12.3(3)B
CSCeb47098		12.3(3)B
CSCeb49148		12.3(1a)B
CSCeb53162		12.3(1a)B
CSCeb60723		12.3(3)B
CSCeb64180		12.3(3)B
CSCeb66825		12.3(3)B
CSCeb69355		12.3(3)B
CSCeb71081		12.3(3)B
CSCeb72942		12.3(3)B
CSCeb84507		12.3(5a)B
CSCeb84839		12.3(5a)B
CSCeb87286		12.3(3)B
CSCec04016		12.3(3)B
CSCec06337		12.3(3)B
CSCec06617		12.3(3)B
CSCec08434		12.3(3)B
CSCec12911		12.3(3)B
CSCec14039	12.3(3)B1	
CSCec15964		12.3(3)B
CSCec22244		12.3(5a)B
CSCec22829		12.3(5a)B
CSCec22929		12.3(5a)B1
CSCec23167		12.3(5a)B
CSCec24098		12.3(3)B

Table 10 **Caveats Reference for Cisco IOS Release 12.3 B**

CSCec24878		12.3(5a)B1
CSCec27942		12.3(3)B
CSCec30789		12.3(3)B
CSCec31355		12.3(3)B
CSCec32135		12.3(3)B
CSCec32933		12.3(3)B1
CSCec37042		12.3(3)B
CSCec40202		12.3(5a)B1
CSCec44985		12.3(3)B
CSCec45012		12.3(3)B
CSCec46195		12.3(5a)B1
CSCec46351		12.3(3)B
CSCec47146		12.3(3)B
CSCec48087		12.3(3)B
CSCec49097		12.3(5a)B
CSCec51206		12.3(5a)B
CSCec59206		12.3(5a)B1
CSCec63438		12.3(3)B
CSCec64802		12.3(3)B
CSCec67336		12.3(3)B
CSCec67873		12.3(3)B, 12.3(3)B1
CSCec67879		12.3(5a)B
CSCed68575		12.3(5a)B1
CSCec69756		12.3(5a)B
CSCec74346		12.3(3)B1
CSCec77881		12.3(5a)B
CSCec77966		12.3(3)B1
CSCec83463		12.3(5a)B
CSCec86327		12.3(5a)B1
CSCec86420		12.3(5a)B4
CSCec89163		12.3(5a)B2
CSCed10161		12.3(5a)B
CSCed11793		12.3(5a)B1
CSCed13018		12.3(5a)B1
CSCed15714		12.3(5a)B1
CSCed17032		12.3(5a)B
CSCed18557		12.3(5a)B5

Table 10 Caveats Reference for Cisco IOS Release 12.3 B

CSCed19748		12.3(5a)B
CSCed21027		12.3(5a)B1
CSCed21813		12.3(5a)B1
CSCed27956		12.3(3)B1, 12.3(5a)B
CSCed29514		12.3(5a)B
CSCed29736		12.3(3)B1
CSCed33719		12.3(5a)B1
CSCed35253		12.3(5a)B1
CSCed38527		12.3(5a)B
CSCed39910		12.3(5a)B1
CSCed40933		12.3(5a)B2
CSCed42319		12.3(5a)B3
CSCed43332		12.3(5a)B1
CSCed46459		12.3(5a)B
CSCed47560		12.3(5a)B1
CSCed52163		12.3(5a)B1
CSCed54232		12.3(5a)B
CSCed56358		12.3(5a)B1
CSCed56379		12.3(5a)B1
CSCed60072		12.3(5a)B1
CSCed60133		12.3(5a)B1
CSCed64664		12.3(5a)B1
CSCed65778		12.3(5a)B3
CSCed67628		12.3(5a)B1
CSCed72657		12.3(5a)B1
CSCed77615		12.3(5a)B1
CSCed78149		12.3(5a)B2
CSCed89735		12.3(5a)B1
CSCed91215		12.3(5a)B1
CSCed93836		12.3(5a)B1
CSCed95499		12.3(5a)B3
CSCee02457		12.3(5a)B1
CSCee04235		12.3(5a)B1
CSCee21989		12.3(5a)B1
CSCee22618		12.3(5a)B1
CSCee25125		12.3(5a)B1
CSCee30904		12.3(5a)B1

Table 10 **Caveats Reference for Cisco IOS Release 12.3 B**

CSCee37933		12.3(5a)B1
CSCee46212		12.3(5a)B1
CSCee67450		12.3(5a)B3
CSCef03083		12.3(5a)B2
CSCef07948		12.3(5a)B2
CSCef42160		12.3(5a)B3
CSCef44225		12.3(5a)B4
CSCef46191		12.3(5a)B2
CSCef49858		12.3(5a)B2
CSCef67682		12.3(5a)B4
CSCef68324		12.3(5a)B4
CSCef74038		12.3(5a)B3
CSCef78169		12.3(5a)B3
CSCin13384		12.3(5a)B1
CSCin16800		12.3(3)B
CSCin24965		12.3(3)B
CSCin29325		12.3(5a)B
CSCin31767		12.3(1a)B
CSCin33325		12.3(5a)B3
CSCin38040		12.3(3)B
CSCin39896	12.3(1a)B	
CSCin40163		12.3(1a)B
CSCin40354	12.3(1a)B	
CSCin40575		12.3(1a)B
CSCin40647		12.3(1a)B
CSCin40652		12.3(1a)B
CSCin40713		12.3(1a)B
CSCin41018		12.3(1a)B
CSCin41280		12.3(1a)B
CSCin41414		12.3(1a)B
CSCin41510		12.3(1a)B
CSCin41525		12.3(1a)B
CSCin41855		12.3(1a)B
CSCin42216		12.3(1a)B
CSCin42253		12.3(1a)B
CSCin42549		12.3(1a)B
CSCin42662		12.3(1a)B

Table 10 Caveats Reference for Cisco IOS Release 12.3 B

CSCin42824		12.3(1a)B
CSCin43411		12.3(1a)B
CSCin43415		12.3(1a)B
CSCin43828		12.3(1a)B
CSCin44460		12.3(1a)B
CSCin45728		12.3(1a)B
CSCin45820		12.3(1a)B
CSCin45858		12.3(3)B
CSCin47430		12.3(1a)B
CSCin47493		12.3(1a)B
CSCin47884		12.3(1a)B
CSCin50030		12.3(3)B
CSCin50873		12.3(1a)B
CSCin51366		12.3(1a)B
CSCin53297		12.3(1a)B
CSCin54101		12.3(3)B
CSCin54739		12.3(3)B
CSCin54802		12.3(3)B
CSCin55905		12.3(5a)B1
CSCin55922		12.3(3)B
CSCin56055		12.3(3)B
CSCin56557		12.3(3)B
CSCin56817		12.3(3)B
CSCin57018		12.3(3)B
CSCin57036		12.3(3)B
CSCin57701		12.3(5a)B1
CSCin57718		12.3(3)B
CSCin57846		12.3(3)B
CSCin57902		12.3(3)B
CSCin58372		12.3(3)B
CSCin60510		12.3(3)B
CSCin60611		12.3(5a)B1
CSCin61004		12.3(5a)B
CSCin61028	12.3(3)B	
CSCin61156	12.3(3)B, 12.3(3)B1	
CSCin61296	12.3(3)B	

Table 10 **Caveats Reference for Cisco IOS Release 12.3 B**

CSCin61674		12.3(5a)B1
CSCin61757	12.3(3)B, 12.3(3)B1	
CSCin61934	12.3(3)B, 12.3(3)B1	
CSCin62450	12.3(3)B1	
CSCin62948	12.3(3)B1	12.3(5a)B
CSCin63604	12.3(3)B1	
CSCin64164		12.3(5a)B
CSCin64712		12.3(5a)B
CSCin65533		12.3(5a)B1
CSCin67236		12.3(5a)B1
CSCin67591		12.3(5a)B
CSCin67619		12.3(5a)B1
CSCin67783		12.3(5a)B1
CSCin68122		12.3(5a)B1
CSCin68728		12.3(5a)B
CSCin69417		12.3(5a)B1
CSCin70629		12.3(5a)B1
CSCin70884		12.3(5a)B1
CSCin72146		12.3(5a)B1
CSCin72429		12.3(5a)B1
CSCin75131		12.3(5a)B1
CSCin75829		12.3(5a)B1
CSCin76059		12.3(5a)B1
CSCin81667		12.3(5a)B3
CSCin82407		12.3(5a)B3
CSCsa49728		12.3(5a)B4
CSCsa65656		12.3(5a)B5
CSCsa68004		12.3(5a)B5
CSCuk47243		12.3(5a)B

Open Caveats—Cisco IOS Release 12.3(5a)B5

This section documents possible unexpected behavior by Cisco IOS Release 12.3(5a)B5 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(5a)B5.

Resolved Caveats—Cisco IOS Release 12.3(5a)B5

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(5a)B5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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: Disable EXEC Accounting and Network Accounting.

This issue is similar to CSCee35379.

- CSCsa65656

SSG uses a duplicate Acct-session-id (attribute 44) in a RADIUS accounting packet.

This issue is observed for post-paid users.

There are no known workarounds.

- CSCsa68004

SSG does not update tariff switch information to the users when the user logs-in exactly at tariff switching time.

This is observed for post-paid Users only.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(5a)B4

This section documents possible unexpected behavior by Cisco IOS Release 12.3(5a)B4 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(5a)B4.

Resolved Caveats—Cisco IOS Release 12.3(5a)B4

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(5a)B4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec86420

Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

This bug is a complementary fix to CSCeb56909 which addresses this vulnerability.

More details can be found in the security advisory which is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>

- 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>.

- 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>.

- CSCsa49728

Timer wheel may encounter an unwanted delay of (wheel size) * granularity.

This issue occurs when the timer attached to timer-wheel have tick value multiple of wheel size.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(5a)B3

This section documents possible unexpected behavior by Cisco IOS Release 12.3(5a)B3 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(5a)B3.

Resolved Caveats—Cisco IOS Release 12.3(5a)B3

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(5a)B3. 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.

- CSCed42319

A Cisco AS5x00 may ignore a service-login attribute and start a PPP session. The Cisco AS5x00 may also start a PPP session when the RADIUS Access-Accept reply contains unknown (that is, unsupported) Framed-Protocol attributes.

This issue is observed when a client uses PAP for authentication.

There are no known workarounds.

- 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>

- 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.

- CSCee67450

A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command ‘bgp log-neighbor-changes’ configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

If a malformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command ‘show ip bgp neighbors’ or running the command ‘debug ip bgp <neighbor> updates’ for a configured bgp neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

- CSCef42160

The **force-local-chap** VPDN configuration command does not work.

This issue occurs when the **force-local-chap** and **terminate-from hostname** commands are configured in the same vpdn-group.

Only Cisco IOS software version 12.3T is affected with this issue.

Workaround: Use the default L2TP VPDN group by deleting **terminate-from hostname** or use Cisco IOS software version 12.3 Main train.

- CSCef74038

PXF chunk memory is not freed after routes are removed.

The following message may occur and cause more PXF memory leaking:

```
%PXF-2-TALLOCFAIL
```

This issue is observed on a Cisco 7200 with NSE-1 processor board or Cisco 7401 platform. When PXF is enabled, adding/removing routes may not free PXF memory.

There are no known workarounds.

- CSCef78169

Radius Nas-Port attribute is not sent in accounting records and access-requests when the **vpdn aaa attribute nas-port vpdn- nas** global configuration command is configured, and when the LAC is NON-CISCO LAC.

This issue only occurs with NON-CISCO L2TP access concentrator (LAC).

Workaround: Remove the **vpdn aaa attribute nas-port vpdn- nas** command.

- CSCin33325

Object identifiers (OIDs) for the CISCO-ATM-PVCTRAP-EXTN-MIB MIB cannot be accessed.

This issue is observed with the CISCO-ATM-PVCTRAP-EXTN-MIB MIB. The MIB number of the CISCO-ATM-PVCTRAP-EXTN-MIB MIB has to be updated with the MIB number of the approved MIB.

There are no known workarounds.

- CSCin81667

The “On Accounting Off from AZR Host” is not cleared off.

This issue is found with a SSG acting as Radius Proxy with EAPSIM setup.

Workaround: Use “On Accounting Stop from AZR Host”, which will be cleared off.

- 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>

Open Caveats—Cisco IOS Release 12.3(5a)B2

This section documents possible unexpected behavior by Cisco IOS Release 12.3(5a)B2 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(5a)B2.

Resolved Caveats—Cisco IOS Release 12.3(5a)B2

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(5a)B2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec89163

A per-user IP route is not installed.

This issue may occur under the following conditions:

1. A Cisco IOS router is configured for VPDN LNS and PPP authentication and authorization via RADIUS.
2. The RADIUS user profile contains the Framed-Route attribute in order to install a per-user IP route on LNS.
3. IPCP renegotiation occurs during the PPP session terminated on LNS.

Workaround: Clear the Virtual-Access interface (on which the PPP user is terminated) after IPCP renegotiation with the **clear interface virtual-access x** command.

- CSCed40933

Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

More details can be found in the security advisory, which is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.

- 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>.

- CSCef03083

Downstream packets from open garden service may not be properly process switched. DNS packets are process switched in SSG, so the DNS replies may not reach the client.

This issue occurs when an Internet service is bound to the same interface as the open garden service, and an unauthenticated user accesses open garden service.

Workaround: Use pass-through filters for downstream packets.

- CSCef07948

A Cisco platform may run out of IDBs, preventing users from connecting to new SSG L2TP tunnel services.

This issue is observed when multiple users simultaneously log on to and log off from SSG L2TP tunnel services.

Workaround: Clear the unused virtual-access interfaces with the **clear interface Virtual-Access EXEC** command.

- CSCef46191

A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

Cisco will make free software available to address this vulnerability.

Workarounds, identified below, are available that protect against this vulnerability.

The Advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>

- CSCef49858

The reauthorization request sent by the router (SSG) does not contain the VSA 26,9,253=QB<bytes>;<timestamp>.

This issue occurs during the following two conditions:

- 1) QT>0, QX=TA>0;PRE>0;POST=0, Idle Timeout>0
- 2) QT>0, QX=TA>0;PRE>0;POST=0, Idle Timeout=0

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(5a)B1

This section documents possible unexpected behavior by Cisco IOS Release 12.3(5a)B1 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(5a)B1.

Resolved Caveats—Cisco IOS Release 12.3(5a)B1

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(5a)B1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv51281

A Cisco router that is configured for ISDN may reload unexpectedly and generate a “low stack for ISDN” error message.

This issue is observed when a high rate of bidirectional traffic occurs on the ISDN B channels. This issue occurred during a stress test.

There are no known workarounds.

- CSCea44460

It was identified in CSCdz88480 that the JMIX performance was lower when ATM-PA was placed in the even slot. This could be due to the extra PCI Bridge latency.

The purpose of this DDTS is to investigate into ways of improving perf when ATM in even slot.

There are no known workarounds.

- CSCea63499

A Cisco 7200 may reload unexpectedly when it attempts to translate virtual address 0x3C0C00C0 to a physical address.

This issue is observed under rare conditions on a Cisco 7200 that is configured with a C7200-I/O-FE I/O controller in slot 0. The issue is related to an error in the Fast Ethernet controller on the I/O controller.

There are no known workarounds.

- CSCeb60929

Previous to 12.2(15)T, **aaa accounting delay-start** in global config used to work as expected. From 12.2(15)T onwards, in VRF configuration, router does not send accounting records for VRFs.

This happens whenever VRF configs are used.

Workaround: Configure **aaa accounting delay-start vrf <vrf_name>** for each VRF begin used. Alternatively, in 12.2(16.4)T and 12.3, a new command **aaa accounting delay-start all** is provided.
- CSCec22929

A software-forced reload may occur on a Cisco 7200 series after an OIR of a PA-2T3+ port adaptor. This issue is observed when traffic enters through the interface of the port adapter.

Workaround: Shut down the interface of the port adapter before you perform an OIR.
- CSCec24878

A Cisco Media Gateway Control Protocol (MGCP) gateway may be unregistered by a Cisco CallManager.

This issue is observed on a Cisco router that functions as a gateway and that runs Cisco IOS Release 12.2 T, Release 12.3, or Release 12.3 T when the T1 channel-associated signaling (CAS) and PRI backhaul is configured.

The Following is an example of the sequence of events that cause this issue to occur:

 1. The Cisco CallManager tears down an active call on the gateway by sending an MGCP delete connection (DLCX) request.
 2. The gateway sends a “200 OK” response to the MGCP DLCX request.
 3. The Cisco CallManager sends an MGCP Request Notify (RQNT) response to the gateway with “DT/sup” and “D/[0-9ABCD*#]” as the requested events to be notified.
 4. The gateway receives the MGCP RQNT request but does not immediately send a “200 OK” response to the MGCP RQNT request.
 5. The Cisco CallManager retransmits the MGCP RQNT request four more times at a frequency of one request per 3 seconds.
 6. The Cisco CallManager unregisters the gateway because it does not receive any response to its MGCP RQNT request.
 7. After 20 seconds, the gateway sends an MGCP notify (NTFY) message with “DT/rlc” as the notified event.
 8. Subsequently, the gateway sends a “200 OK” response to the MGCP RQNT request.
 9. The gateway does not receive any response to its MGCP requests because the Cisco CallManager has unregistered the gateway.

Workaround: Do not use MGCP. Rather, use H.323.
- CSCec40202

The CLI unconfig has NO bearing whatsoever on server being marked as DEAD. The default behavior is not noticed.

This issue occurs when “no radius-server dead-criteria tries 20” is configured. The server gets marked as “DEAD” only after 20 tries (similar to when the CLI had been configured).

There are no known workarounds.

- CSCec46195

Dialer call may get authorized with the non-existent named radius method.

This is observed in as5850 router loaded with 123-3.9.T2 image

There are no known workarounds.

- CSCec59206

A router may reload unexpectedly because of a bus error when it accesses a low address during the translation of TCP port 514.

This issue is observed on a Cisco router that runs Cisco IOS Release 12.3(5) and that is configured for Network Address Translation (NAT).

Workaround: Prevent the translation of TCP port 514.

- CSCec86327

Slot 0 cannot be seen in show version (12.3(2)T1) and CompactFlash Disk (A 64- or 128-MB) should be indicated in show version. This phenomenon exists in both c7301-boot-mz.123-2.T1 and c7301-is-mz.123-2.T1. It appears that this issue is only cosmetic and not harmful.

The following is the instance of the output and is not indicated in show version:

```
-----
62976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
-----
```

But the information regarding slot 0 in dir disk0: and sh disk0 can be seen:

```
-----
Router(boot)#dir disk0:
Directory of disk0:/
 1  -rw-   17728924  Oct 10 2003 11:17:46 +00:00  c7301-is-mz.123-2.T1.bin
256376832 bytes total (238616576 bytes free)
-----

Router(boot)#sh disk0
-#- --length-- -----date/time----- path
1   17728924 Mar 8 2000 03:13:14 +00:00 c7301-is-mz.123-2.T1
46465024 bytes available (17760256 bytes used)
-----
```

This issue occurs in the following:

H/W : cisco 7301

S/W : 12.3(2)T1
 c7301-boot-mz.123-2.T1
 @@@c7301-is-mz.123-2.T1

There are no known workarounds.

- CSCed11793

The output queue of a Gigabit Ethernet port may become stuck, preventing traffic from leaving the interface.

This issue is observed on the Gigabit Ethernet port 0/1 (gig0/1) of a Network Processing Engine NPE-G1 (NPE-G1) that is installed in a Cisco 7200 series.

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

Alternate Workaround: Reload the router.

- CSCed13018
Native GE interface throttling is always bypassed.
The throttling is also bypassed with newer versions of the BCM chips, whereas the throttling is needed for older versions of the BCM chips.
There are no known workarounds.
- CSCed15714
A Cisco 7400 series may not recognize its Gigabit Ethernet interface.
This issue is observed on a Cisco 7400 series that runs a Cisco IOS software release that is listed in the “First Fixed-in Version” field at the following location:
<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec86327>.
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.
- CSCed21027
Software interface description blocks (IDBs) may become exhausted after an interface flaps repeatedly.
This issue is observed under the following conditions:
 - PPP sessions go down.
 - The same PPP sessions come back up and make use of a new IDB rather than the previously used IDB.
 - A virtual-access interface is used rather than a virtual-access subinterface.
 There are no known workarounds.
- CSCed21813
A Cisco 7204VXR in which an enhanced 1-port ATM OC-3c/STM-1 port adapter (PA-A3-OC3) is installed may reload unexpectedly because of a bus error. However, the cause of the issue may be a segmentation and reassembly (SAR) chip failure that occurs because of an “Address Error (store) exception”.
This issue is observed on a Cisco 7204VXR that is configured for Dynamic Bandwidth Selection (DBS) support when you attempt to modify the VC QoS parameters under high traffic conditions.
Workaround: Shut down the ATM interface before attempting to modify the VC QoS parameters.
- CSCed33719
A System Error Interrupt error message came up on c7301 during boot process. It uses 12.2(16)B2 and PA-2FE-TX, but there are no message using PA-FE-TX.

```
System Bootstrap, Version 12.2(8r)B3, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 2002 by cisco Systems, Inc.
C7301 platform with 262144 Kbytes of main memory
Self decompressing the image :
#####
[OK]
*** System Error Interrupt (IBIT6) ***                <<-----
int_stat register = 0x0
BCM-1250 Error Interrupt, Cause(s):
mask=0xf47effc3ffc0ecc3, cause=0x0080000000000000,
real_cause=0x0080000000000000
M_INT_PCI_ERROR
```

```

PC = 0xbfc00e9c, SP = 0x80005558, RA = 0xbfc02a24
Cause Reg = 0x00004000, Status Reg = 0x3040d003
monitor: command "boot" aborted due to exception

```

This issue occurs upon booting the router with the help of a boot-helper image.

Workaround: The Error Message is displayed only with a boot-helper image. The loading of IOS is fine and the router functions properly. As a workaround, Load the full IOS image from disk without the help of boot-helper this message will not be seen.

- CSCed35253

A router may reload unexpectedly after it attempts to access a low memory address.

This issue is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.

Workaround: Disable IP Inspect and IDS.

- CSCed39910

An LNS bringing up a maximum number of PPOeOA calls at the maximum rate may crash.

This issue is observed in Cisco IOS Release 12.3 T but may also occur in other releases.

There are no known workarounds.

- CSCed43332

The following commands appear in the vpdn-template configuration mode even though they are not supported in that mode:

```

force-local-chap Force a CHAP challenge to be instigated locally
  lcp             LCP specific commands
  terminate-from Terminate tunnel from remote peer

```

This issue is observed while configuring a vpdn-template for vpdn sessions on any Cisco router acting as a LNS in IOS versions 12.3B, 12.3 and 12.3T.

Workaround: As the above commands, if enabled in vpdn-template mode, may not work, the workaround is to enable them from the vpdn-group mode where they are supported.

- CSCed47560

The native Gigabit Ethernet ports of a Cisco 7200 series NPE-G1 or a Cisco 7301 may stop forwarding traffic.

This issue is observed in a stress situation when bursty traffic is received.

There are no known workarounds.

- CSCed52163

When the HSRP MIB is polled and there are HSRP groups configured on subinterfaces, an error such as "OID not increasing" may occur on the device that is polling the router. In some cases, a CPUHOG traceback may occur on a router when the HSRP MIB is polled, especially when a lot of interfaces are configured.

This issue is observed under either one of the following two conditions:

- An SNMP HSRP query triggers a loop in the getnexts. Some MIB browsers catch this, and exit with a message stating “OID not increasing”.
- A scaling problem may occur with HSRP when there are a high number of tracked interfaces. For every standby track statement, every interface is tested to see if it is an HSRP tracked interface. No defined thresholds have been identified and tested that qualify when this scaling problem may occur. The more interfaces there are configured, the greater is the possibility that the problem occurs.

Workaround: Do not initiate an SNMP query for HSRP.

Alternate Workaround: Enter the **snmp-server** global configuration command to specify which MIBs are available, as in the following example:

```
snmp-server view HSRP internet included
snmp-server view HSRP ciscoHsrpMIB excluded
snmp-server view HSRP ciscoHsrpExtMIB excluded
snmp-server community public view HSRP RW 20
snmp-server community private view HSRP RW 20
```

- CSCed56358

This problem is displayed “%SCHED-3-STUCKMTMR” error message at the process of “VPDN call manager”.

This issue is seen using NPE-300 with 12.3(4)T1 and NPE-G1 with 12.2(16)B1.

There are no known workarounds.

- CSCed56379

A “Spurious memory access” error message may be displayed and tracebacks may occur on a Cisco router.

This issue is observed on a Cisco router that functions as a LAC and that runs PPPoE.

There are no known workarounds.

- CSCed60072

Traffic coming from the tunnel internet service is being forwarded to the user, even if it is received on a non-tunnel interface.

This issue is seen when there are two pass-through & one tunnel (with NAT) service active in SSG.

There are no known workarounds.

- CSCed60133

This issue has been observed on the customer side on release 12.2(16)B2, but it still appears on latter releases. It is not possible to reestablish connections over SVC once this SVC has expired and the adjacencies shows as incomplete. LANE networks are also affected, because they run over SVCs.

This issue appears when pxf is enabled. On disabling pxf, SVC is establish on request.

Workaround: Disabling pxf fixes the issue. Sending traffic to the incomplete adjacency directly from the 7400 with pxf enabled recovers the SVC connection.

- CSCed64664

A “%SYS-2-LINKED: Bad enqueue” error message may be seen in the syslog of an LNS right after traffic is send through a PPP multilink bundle that is establish via an L2TP session on the LNS. This message is also seen when multilink PPP fragments are switched or when multicast packets are replicated.

Certain packet buffers (particle clones) are eventually depleted, and multilink fragmentation stops working when all particle clones are exhausted. You can monitor the availability of particle clones by entering the **show buffers | begin Particle Clones: EXEC** command; the command does not produce any output if no more particle clones are available.

This issue is observed when multilink is configured on a virtual template that is handling the VPDN sessions or when multicast packets are switched.

Workaround: When L2TP multilink calls are terminated, disable multilink fragmentation by entering the **ppp multilink fragment disable** interface configuration command on the virtual template.

- 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 issue only surfaces during the initial boot of the platform.

- CSCed68575

Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml>

- CSCed72657

The customer wants IOS to disable the logging of messages with prefix “VPDN-6-CLOSED”. They also want the history table not to add the entries with message “The remote server closed the session”.

New commands were added by this fix. By Default “vpdn logging cause normal” and “vpdn history failure cause normal” is enabled. “no vpdn logging cause normal” should not prevent the logging of “The remote server closed the session” in the table. And Configuring “no vpdn history failure cause normal” should not prevent the syslog message “VPDN-6-CLOSED” from appearing on console.

These issues uses IOS 12.3(3)B release.

There are no known workarounds.

- CSCed77615

SSG with permanent tcp-redirect (plug-and-play) enabled may reboot when the user connects into the service which has the following attribute:

```
    ssg-service-info "KW0"
[which means "no permanent http redirect for this service".]
```

Work-Around: Enable CEF on all uplink interfaces: interfaces reachable to service and interfaces to tcp-redirect servers.

- CSCed89735
An uncorrectable ECC parity error may occur on a Cisco 7200 series that is configured with an NPE-G1.
This issue is observed rarely when you enter the **show sysctlr** or the **show tech** command on the NPE-G1.
Workaround: Do not enter the **show sysctlr** or the **show tech** command.
- CSCed91215
Attributes 42 and 43 may be of value “zero” in Connection STOP records.
This issue is observed on a Cisco AS5400 and Cisco AS5850 that run Cisco IOS Release 12.3 or Release 12.3(4)T4 when a TCP-clear call is disconnected by the caller. For call disconnects by the NAS, the values are proper.
There are no known workarounds.
- CSCed93836
A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.
All Cisco products which contain TCP stack are susceptible to this vulnerability.
This advisory is available at
<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.
A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at
<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.
- CSCee02457
The authen-before-forward option is not available under vpdn-group CLI.
This issue is seen on a cisco 7200 router running 12.3(7.6) IOS version.
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 7200vrx series that is configured with an NPE-G1 Network Processing Engine.
There are no known workarounds.

- CSCee21989

A Cisco router may reload unexpectedly with a bus error.

This issue is observed on a Cisco router that has PPP configured.

There are no known workarounds.
- CSCee22618

Spurious memory access may occur on C7400 with 12.3(3)B1.

```
*Mar 26 01:02:01 jst: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x6128C3E4
reading 0x8
*Mar 26 01:02:01 jst: %ALIGN-3-TRACE: -Traceback= 6128C3E4 61278C9C 6127A4E4 6127A720
607128A0 60724104 607A0AD4 607A0AB8
```

This issue occurs when C7400 is used as a LAC router.

There are no known workarounds.
- CSCee25125

When SSG forwards accounting requests from the NAS to the AAA server and one packet gets lost between SSG and AAA, SSG behaves incorrectly. In order to do this the SSG should update its internal Translation Table when it receives a retry packet from NAS to the new Radius id, while the response from AAA is still outstanding. Furthermore it should keep the state of the session for some grace period to be able to respond to retry packets of the NAS, when response packets get lost between SSG and NAS.

This happens the AAA server response is slow, or if there is packet loss between the AAA-server and SSG.

Workaround: Avoid that the AAA-server has a performance issue, even in peak moments.

Alternative Workaround One: Avoid too much packet loss between AAA-server and SSG.

Alternative Workaround Two: Use some form of priority queueing for the Radius packets in the network between SSG and Radius-server.
- CSCee30904

Despite configuring PZIO in SSG service profile, Interim Accounting Records are regularly sent to prepaid server which is configured locally on SSG router. **debug ssg ctrl-events** and **debug radius** clearly show sent interim updates while **show ssg service** shows that prepaid accounting is disabled.

There are no known workarounds.
- CSCee37933

DNS requests will always be forwarded by SSG without any host objects created.

A new CLI option is being added to SSG to drop such DNS packets. Please see the decription attachment for details.

There are no known workarounds.
- CSCee46212

With Cisco IOS release 12.3(XI), When turning on PXF module, the VPDN mib counters will not increase till the module is turned off.

Workaround: Issue a **sh vpdn session packet exec** command before polling for tunnel counters via snmp.

- CSCin13384

The “ppp timeout idle <seconds>” configured under Virtual-Template does not work on LAC for VPDN sessions forwarded to LNS.

This issue occurs only for VPDN sessions forwarded by LAC.

Workaround: Configure “[no] ppp timeout aaa” first and then configure “ppp timeout idle <seconds>” under virtual-template.
- CSCin55905

An “ALIGN-3-SPURIOUS” spurious memory access and traceback may occur on a Cisco 7500 series.

This issue is observed in one of the following conditions:

 - When distributed Multilink PPP (MLP) is configured and when you enter the **microcode reload** global configuration command on the Route Switch Processor (RSP).
 - When a PPP timer expires after a PPP session has been cleaned up.

There are no known workarounds.
- CSCin57701

A router may reload when Serial Line Internet Protocol (SLIP) is configured on a virtual interface, and then PPP is configured on the same interface.

This issue is observed on the virtual interface of a Layer 2 Tunneling Protocol (L2TP) network server (LNS).

There are no known workarounds.
- CSCin60611

A router may reload when you enter the **show queue atm** command.

This issue is observed on a Cisco 7200 series with an NSE-1 processor board and a Cisco 7401 when PXF is enabled. The issue occurs when the **show queue atm** command is entered while traffic is flowing through an ATM PVC.

Workaround: Disable PXF globally by entering the **no ip pxf** command.
- CSCin61674

Configuring “pppoe limit per-vc 1” on the LAC’s virtual template configuration for PPPoE does not have any effect, since it is still possible to bring up more than 1 session on the same VC.

This issue occurs when NAS-Port Pre-authorization is enabled on LAC and global vpdn authen-before-forward also configured.

This issue is observed on pppoe server running 12.3(03)B.

Workaround: Remove the NAS-Port Pre-authorization.
- CSCin65533

A PPPoEoA session may fail to come up on a router on a user side. PPPoE profiles are used for establishing the PPPoE session. When the router receives a “CONFREQ” message from the LNS, the session goes down and cannot be reestablished.

This issue is observed on any Cisco platform that runs Cisco IOS Release 12.3 or Release 12.3(4)T2. The issue does not occur in Release 12.3(4)T1.

Workaround: Although the following is not a good workaround, it can be used. Use VPDN groups instead of BBA profiles. Normal PPPoE sessions using VPDN group can be established, but with some overhead. When a PPPoE session is initiated, it does not come up at the first attempt, but the PPPoE client somehow reinitiates the session.

Alternate Workaround: Remove the “lcp renegotiation always” configuration from the LNS and use BBA groups.

- CSCin67236

The “L” Attribute is not applied in the accounting records.

This issue occurs with the 12.3(5.12)PI4 image.

Workaround: Configure “L” attribute as a last attribute in the service profile.

- CSCin67619

Acct-Input-Gigawords/Acct-Output-Gigawords (Attributes 52 and 53) are not being sent in the periodic accounting records and accounting stop record after the Acct-Input-Octets or Acct-Output-Octets counter has wrapped around 2^{32} .

There are no known workarounds.

- CSCin67783

When the CIR is configured with some value for both Upstream & Downstream and the Normal Burst size and the Excess Burst size are not configured in the service profile, then ssg shows the wrong value of Excess burst rate in the connection object.

This issue occurs when CIR for both Upstream and Downstream only configured.

Workaround: Configure the Excess burst rate explicitly in profile.

- CSCin68122

The RADIUS server is still considered dead after re-configuring it. However, the **show aaa servers EXEC-mode** command will show the server to be UP.

This issue occurs when re-configuring a RADIUS server, that has already been configured previously (e.g. at startup), with a different configuration, for example change in timeout value. This refers to the **radius-server host** configuration mode command.

Workaround: There are no known workarounds to bring up a specific RADIUS server via CLI. However, re-issuing the **radius-server deadtime** config-mode command will bring all affected servers to UP state.

- CSCin69417

SSG crashes when permanent redirection is configured after Captive Portal has already sent a message to SSG that a user has web proxy settings.

Users with web proxy settings have been redirected to captive portal before permanent redirection has been configured on SSG, and SSG TCP redirect config is being disabled during that time.

Workaround: Do not unconfigure SSG TCP redirection on the box when there are active users.

- CSCin70629

Attribute 45 is not sent in accounting records.

This issue is observed on a Service Selection Gateway (SSG).

There are no known workarounds.

- CSCin70884
A Cisco 7200 (NSE-1) router with bidirectional PPPoA/l2tp traffic unexpectedly reloads.
This issue is observed on a Cisco 7200 (NSE-1) router with bidirectional PPPoA/l2tp traffic when the user tries to remove an ATM interface. This defect happens only with NSE-1.
There are no known workarounds.
- CSCin72146
Accounting start before prepaid service authorization with prepaid service defined with PZW attribute.
This issue will be seen in 12.3(8)T images.
This issue will be seen only for the services with PZW.
There are no known workarounds.
- CSCin72429
A platform may pause indefinitely when the **radius-server deadtime** command is configured.
This issue is observed on a Cisco platform under the following conditions:
 - System accounting is configured.
 - The platform device is starting up and tries to send the system accounting record.
 - The RADIUS server that is being contacted is not accessible.
 Workaround: There are three different workarounds:
 - Do not configure the **radius-server deadtime** command.
 - Ensure that the RADIUS server is accessible.
 - Disable system accounting and reload the platform.
- CSCin75131
The memory in use might increase over time.
A router with active SSG tunnel services and user logging into and logging off tunnel services may see an increase in the memory in use.
There are no known workarounds.
- CSCin75829
Connection interim accounting records won't be send at the intervals configured.
This issue first appeared with the commit to CSCin72146. All SSG images with CSCin72146 will have this issue.
There are no known workarounds.
- CSCin76059
SSG direction command is removed from the multilink interface config.
This issue is observed when a multilink interface configured as an SSG downlink interface, the “ssg direction downlink” is removed from the interface config when the multilink interface flaps.
Workaround: Re-configure the interface as downlink.

Open Caveats—Cisco IOS Release 12.3(5a)B

This section documents possible unexpected behavior by Cisco IOS Release 12.3(5a)B 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(5a)B.

Resolved Caveats—Cisco IOS Release 12.3(5a)B

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(5a)B. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea84092

There is a drift of time in the interim accounting records generation over a period when compared to the configured interval.

There are no known workarounds.

- CSCeb24206

Drops may occur when writing to nvram.

This issue occurs during high traffic, saving config or causing a nvram write can cause packets to be dropped.

Workaround: Lower traffic rate when performing maintenance such as configuration file saves.

- CSCeb84507

C7401ASR with 12.2(16)B cannot save envm stats by **show env all** command.

Therefore **show env last** command does not work correctly.

```
Router#sh env all
Power Supplies:
    Power Supply is Internal AC Power Supply. Unit is on.
Temperature readings:
    Thermal Sensor 1 measured at 43C/109F
    Thermal Sensor 2 measured at 33C/91F
Voltage readings:
    +1.8 V (PXF) measured at +1.78 V
    +1.8 V (CPU) measured at +1.77 V
    +2.50 V      measured at +2.49 V
    +3.30 V      measured at +3.27 V
    +5.00 V      measured at +4.96 V
    +5.20 V      measured at +5.22 V
    +12.25 V     measured at +12.17 V
    -12.00 V     measured at -12.05 V
Fans:
    Fan 1 is believed to be working
    Fan 2 is believed to be working
    Fan 3 is believed to be working
    Fan 4 is believed to be working
    Fan 5 is believed to be working
Envm stats saved 0 time(s) since reload <<<-----
Router#sh env last
    Data not available <<<-----
```

There are no known workarounds.

- CSCeb84839

An unexpected reload may occur with the following:

```
%ALIGN-1-FATAL: Corrupted program counter
pc=0x0, ra=0XXXXXXXX, sp=0XXXXXXXX
%ALIGN-1-FATAL: Corrupted program counter
pc=0x0, ra=0XXXXXXXX, sp=0XXXXXXXX
Unexpected exception, CPU signal 10, PC = 0x0
```

There are no known workarounds.

- CSCec22244

On a Cisco LNS running 12.2(13)T or later code, the EXEC command **show caller ip** will not display the CLID/DNIS information sent by the LAC if users are terminated on full virtual-access interfaces (as opposed to virtual-access sub-interfaces).

There are no known workarounds.

- CSCec22829

A timer wheel may fail when the same timer is started from both the process level and the interrupt level.

This issue is observed on a Cisco router that runs Network Address Translation (NAT).

There are no known workarounds.

- CSCec23167

During BGP scalability testing, error messages and tracebacks similar to the following ones may be logged, indicating a difficulty with TCP and buffer usage:

```
%SYS-2-MALLOCFAIL: Memory allocation of 4692 bytes failed from 0x6076F714,
align
Pool: I/O Free: 11143248 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
-Process= "Pool Manager", ipl= 0, pid= 6
-Traceback= 607FE10C 607FF1EC 6076F71C 6080C1D0 6080C400
%TCP-6-NOBUFF: TTY0, no buffer available
-Process= "BGP I/O", ipl= 0, pid= 139
-Traceback= 6098B4EC 609938C8 60993C1C 60D55CE4 60D0BEB0
%TCP-6-NOBUFF: TTY0, no buffer available
-Process= "BGP Router", ipl= 0, pid= 138
-Traceback= 6098B4EC 609938C8 60993C1C 60D55CE4 60D29858 60D2AF88 60D1B4BC
```

This issue is observed on a Cisco router that is in the processing of building BGP sessions for about 80,000 prefixes and about 1200 BGP peers.

There are no known workarounds.

- CSCec49097

A Cisco 7200 series pauses indefinitely in the middle of a link control protocol (LCP) negotiation. The PPP over ATM (PPPoATM) session receives a "Sending Acct Event [Reneg]" message and terminates the LCP phase. The remote peer renegotiates another PPP session and uses the same PPP ID. This causes a continuous LCP state for that user.

This issue is observed on a Cisco 7200 series that is configured for PPPoATM and that runs Cisco IOS Release 12.2(15)T9. The symptom may also occur in other releases.

There are no known workarounds.

- CSCec51206
A memory allocation failure (MALLOCFAIL) from the I/O memory pool may occur.
This issue is observed on a Cisco router that receives excessive multicast control traffic.
Workaround: Apply a quality of service (QoS) policy map to limit the rate of the multicast control traffic that can be received by the router.
- CSCec67879
Some PPP sessions may not come up and become stuck in the link control protocol (LCP) negotiation state.
This issue is observed on a Cisco 6400 series Node Route Processor (NRP). A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec49097>.
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.
- CSCec69756
You may not be able to configure the maximum transmission unit (MTU) on a virtual template.
This issue is platform independent.
There are no known workarounds.
- CSCec77881
The default number of missed keepalives required to bring down a ppp link has changed from 5 to 3 in releases that have integrated CSCdt94888. The original default behavior can be restored by configuring “keepalive 10 5” on the interface.
There are no known workarounds.
- CSCec83463
The service selection gateway (SSG) sends duplicate Acct-Session-Id in the SSG connection accounting record. Same session id is used in the user accounting record.
This issue occurs on Cisco IOS software version 12.2(16)B2 and 12.3(4)T.
There are no known workarounds.
- CSCed10161
When VPDN session is disconnected by authentication failure, no VPDN syslog message (%VPDN-6-AUTHENFAIL) and history failure table are logged. A record is overwritten by normal causes (%VPDN-6-CLOSED, Result 1, Error 0)
Cisco IOS software version 12.3(3)B, 12.3(4)T VPDN logging is enable
There are no known workarounds.
- CSCed17032
When the **ip radius source-interface** global configuration command is configured on a PPP over Ethernet (PPPoE) server, the interface address may not be set in the RADIUS NAS-IP-Address [4] attribute.
This issue is observed on a Cisco platform that runs Cisco IOS Release 12.3(2), 12.3(2)T, 12.3(3)B, or 12.3(4)T, that functions as a PPPoE server, and that has the **radius-server attribute nas-port format format** global configuration command enabled with the value **d** for the *format* argument.

Workaround: Do not use value **d** for the *format* argument. Rather, use another value to configure the network access server (NAS) port.

Alternate Workaround: Enter the **radius-server attribute 4 nrp** global configuration command.

- CSCed19748

The individual AAA periodic accounting update messages (Radius accounting messages with Acct-Status-Type=Watchdog) generated by an IOS gateway for each call leg (TDM and IP) of the same voice call may be sent to the Radius server more than 5 minutes apart due to the randomized timer algorithm used by the AAA message transmit function.

The command **aaa accounting update newinfo periodic** is configured.

There are no workaround.

- CSCed27956

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed29514

The C7200 NPE-G1 builtin GE (SBeth) MAC Filter accepts NULL DAs 00-00-00-00-00-00. This unintentional behavior may pose a denial of service security risk in customer environments if their networks are flooded with NULL DAs. This appears to be a Broadcomm silicon or documentation errata. The Broadcomm docs state that NULL DAs may be used for unused MAC Filter entries, implying that they are not accepted.

When NULL DAs are presented to the NPE-G1 SBeth I/F.

There are no known workarounds.

- CSCed38527

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed46459

When **ip address negotiate** is configured on an interface and our address is not successfully negotiated with the peer, no address is assigned to our interface which can cause problems with IP/CEF forwarding.

There are no known workarounds.

- CSCed54232

The memory held by SSGCmdQueue process increases continuously when SESM users log on and log off.

This issue occurs in SSG deployments when SESM users logon and logoff.

There are no known workarounds.

- CSCin29325

Without any global radius servers configured, an access-request is sent to the server defined in the AAA test server group. This happens even with no “radius-server key” defined. This behavior does not occur in 12.2(13.7)T, the error message “No radius servers defined” is displayed.

This is not a serious issue and is a configuration problem. The user is warned when a server that has not been defined is added to the server group.

```
Router(config)#aaa group server radius bogus
Router(config-sg-radius)#server 10.1.1.1 ?
  acct-port  UDP port for RADIUS accounting server (default is 1646)
  auth-port  UDP port for RADIUS authentication server (default is 1645)
  <cr>
Router(config-sg-radius)#server 10.1.1.1
00:55:48: %RADIUS-4-NOSERV: Warning: Server 10.1.1.1:1645,1646 is not defined.
```

It is expected that the behavior will be undefined if the user does not correct the misconfiguration.

- CSCin61004

You may not be able to configure an ATM permanent virtual circuit (PVC) range on a second ATM subinterface. The ATM PVC range can only be configured on one ATM subinterface.

This issue is observed on a Cisco router that runs Cisco IOS Release 12.3 or Release 12.3 B when you enter the **pvc range** subinterface configuration command to configure a second ATM subinterface.

There are no known workarounds.
- CSCin62948

SSG may not send a calling station ID in connection accounting records to a local and a remote AAA server.

This issue is observed when a client log on by using a proxy service with MSISDN.

There are no known workarounds.
- CSCin64164

Time Drift in Interim Accounting update was seen for SSG connection accounting packets.

This issue occurs with 10 Host Objects and Connection Accounting interval 300. After 4 days of testing time drift was seen in Interim accounting update packets.

There are no known workarounds.
- CSCin64712

PPPOA sessions may not come up.

This issue is observed on a Cisco router when CEF or PXF is enabled and when the encapsulation is changed while no VC is defined.

Workaround: Create a VC and then change the encapsulation.
- CSCin67591

%PXF-2-EXCEPTION: messages are observed on the console when L2TP downstream traffic is passing through.

This issue is observed on a Cisco 7200 with a NSE-1 processor board or Cisco 7401 platform (when these platforms functions as LNS) and when PXF is enabled. Rate-limit is configured on L2TP tunnel egress physical interface.

Workaround: Disable PXF with the **no ip pxf**.
- CSCin68728

Unauthorized service users do not get redirected.

This issue occurs under the following conditions:

 - Service redirection is configured.
 - PBHK is enabled.
 - CEF is enabled on downlink interface

Work around: Either disable CEF or port-map.

- CSCuk47243
High CPU utilization may occur on a Cisco 7200 series that is configured with a Network Processing Engine G1 (NPE-G1), and some unicast packets may be dropped when there is a lot of multicast replication.
This issue is observed when more than 300 packets are replicated for one packet.
There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(3)B1

This section documents possible unexpected behavior by Cisco IOS Release 12.3(3)B1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec14039
A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:
`Last reset from watchdog reset`
This problem is observed on a Cisco 7200 series that is configured with an NPE-G1 and that is running Cisco IOS Release 12.2(14)S3. The problem may also occur in other releases.
There are no known workarounds.
- CSCin61156
SSG Service re-authorization failure with after Quota Time expiry.
This problem occurs when SSG does not send re-authorization request after Quoa Time expiry for connection with QT60, QV0 and Idle 0.
There are no known workarounds.
- CSCin61757
SSG unexpectedly reloads when logging in HO with chap authentication.
Workaround: Use only PAP authentication.
- CSCin61934
SSG unexpectedly reloads for proxy service authorization.
This problem occurs when SSG tries to allocate memory for proxy service authorization packet.
There are no known workarounds.
- CSCin62450
SSG send Interim accounting update to local and prepaid server alternatively.
With PZI60 and L60 in service profile, SSG sends Interim accounting update alternatively to local and prepaid server.
There are no known workarounds.
- CSCin62948
Calling-Station-Id not sent in connection accounting records.
For proxy service logon with MSISDN, SSG does not send calling-statin-id in connection accounting records sent to local and remote aaa server.
There are no known workarounds.

- CSCin63604
Wrong Calling-station-id sent in tunnel service creation to LNS.
When a different calling-station-id is received for tunnel service logon from sesm ssg should use this calling-id for tunnel service creation with LNS. SSG is sending host logon calling-id to LNS for tunnel creation which is wrong.
There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(3)B1

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(3)B1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec32933
Cisco router with SSG application may reload.
This is noticed with Cisco MSID access request and when the access accept from a AAA is delayed and/or the access response doesn't contain CDMA Realm.
There are no known workarounds.
- CSCec67873
SSG system shows tracebacks and reloads with unexpected exception, CPU signal 10, PC = 0x613F1C10.
This problem occurs when a user is cleared by CLI or disconnects by switching CPE off. Exact cause not yet known.
There are no known workarounds.
- CSCec74346
With an AZR Power Off / Power On (i.e. AZR Accounting ON Only) Accounting ON are not acknowledged by SSG.
Workaround: To create a new Radius group called CAR and configure SSG to forward all accounting messages to CAR.
- CSCec77966
A Cisco router that terminates both PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA) sessions may fail for a period of up to 3 minutes to switch traffic downstream toward the subscriber via Cisco Express Forwarding (CEF).
This problem is observed when the PPPoE and PPPoA sessions use different virtual templates and when subinterfaces are enabled. The problem may affect only some subscribers.
Workaround: Configure one virtual template for both PPPoE and PPPoA sessions.
Alternate workaround one: Disable subinterfaces.
Alternate workaround two: Disable CEF.
- CSCed27956
A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond

terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed29736

SSG upstream counter stats for connection object is wrong.

SSG TCP redirect feature is enabled.

Workaround: Disable IP CEF on the downlink interface. However this will bring down the packet throughput of the box greatly.

Open Caveats—Cisco IOS Release 12.3(3)B

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

- CSCec67873

SSG system shows tracebacks and reloads with unexpected exception, CPU signal 10, PC = 0x613F1C10.

This problem occurs when a user is cleared by CLI or disconnects by switching CPE off. Exact cause not yet known.

There are no known workarounds.

- CSCin61028

Unable to login to Service on SSG.

This problem occurs when SSG Service logon has failed form service profile having an AC Attribute.

There are no known workarounds.

- CSCin61156

SSG Service re-authorization failure with after Quota Time expiry.

This problem occurs when SSG does not send re-authorization request after Quoaat Time expiry for connection with QT60, QV0 and Idle 0.

There are no known workarounds.

- CSCin61296
Unable to logon to tunnel and proxy service.
This problem occurs with Chap Host logon and Pap service logon are unable to activate the service on SSG.
There are no known workarounds.
- CSCin61757
SSG unexpectedly reloads when logging in HO with chap authentication.
Workaround: Use only PAP authentication.
- CSCin61934
SSG unexpectedly reloads for proxy service authorization.
This problem occurs when SSG tries to allocate memory for proxy service authorization packet.
There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(3)B

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(3)B. 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.
- CSCea57826
Incoming packets may become stuck indefinitely on the native Gigabit Ethernet interfaces of a Network Processing Engine G1 (NPE-G1) that is installed in a Cisco 7200 series router.
This problem is observed under a full traffic load and only on a Cisco 7200 series router that is configured with an NPE-G1.
Workaround: Issue the **shutdown** command followed by the **no shutdown** command on the affected NPE-G1 Gigabit Ethernet interface.
- CSCea66267
SSG makes authorization requests towards a prepaid server even though the connection cannot be activated.
SSG makes a service authorization request towards OCS for a prepaid service, before it checks whether this service can be activated or not. The service authorization request causes the OCS (prepaid server) to deliver a quota, but if the quota cannot be used by the SSG, this unused quota will not be returned to OCS for other active services. One reason why a service cannot be activated could be that the service is pointing to the same network as another service.
Workaround: Mark services with overlapping service networks as sequential or part of a mutually exclusive service group so that user cannot log into both of them simultaneously.

- CSCeb21064

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

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

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

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

This advisory is posted at

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

- CSCeb35210

A Cisco router that has a Quality of Service (QoS) service policy attached to an interface may generate memory alignment errors or reload unexpectedly because of a bus error during normal mode of operation.

This problem is observed when the policy map of the service policy has a set action configuration and when traffic is being processed.

Workaround: Remove the set action configuration from the policy map.

- CSCeb43378

A Cisco router may have a software-forced reload when the **show interfaces virtual-access *number* [configuration]** EXEC command is entered.

This problem is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(17).

Workaround: Do not use the **show interfaces virtual-access *number* [configuration]** EXEC command.

- CSCeb47098

When VPDN session is terminated by PPP authentication failure, no VPDN syslog message (%VPDN-6-AUTHENFAIL) and history failure table are logged.

Cisco IOS software version 12.2(16)B, 12.3(1) VPDN logging is enable

There are no known workarounds.

- CSCeb60723

SSG forwards accounting retransmits from radius-clients to the AAA server and also does additional retransmits for each forwarded request.

When SSG is configured to forward accounting requests from radius-clients, if the AAA server responds slowly, radius clients will retransmit the accounting requests. SSG forwards the accounting requests even though it is waiting for a response from the AAA server. However, for access-requests from radius-clients, SSG does not forward retransmitted access-requests while waiting for a response from AAA server.

Workaround is to make the radius-client (Radius timeout*Retry) time greater than SSG (Radius timeout*Retry) time.
- CSCeb64180

The bug was reported on Cat6k. Other platforms also may have this issue. In hybrid mode, when a reset [15/16] is issued from SP (CatOS, hybrid mode), the reload time displayed is very large.

The reload time displayed is right when a reload is issued from RP console.

There are no known workarounds.
- CSCeb66825

A Cisco 7200 series may reload unexpectedly during a service-policy configuration.

This problem is observed when you attach a level 2 policy map as a child of a level 1 policy map and when the level 1 policy map is already attached to an interface.

Workaround: Create a level 3 policy map and attach it to the interface.
- CSCeb69355

In case you have an image with the fix for CSCin24965 (which no customer has), you might see a SYS-2-BADSHARE message.

There are no known workarounds.
- CSCeb71081

The queueing of LCP configuration requests on the LAC when the down stream switching path (LNS to client) has been established but the upstream path has not, was implemented by CSCin24965, and then disabled by CSCeb69355. None of this was ever seen by a customer, since there were no versions shipped with this code.

This DDTS restores the queueing that was disabled by CSCeb69355.

With the queueing disabled, the call connection latency will be increased during periods of high CPU utilization on the LAC, since the client may have to retry sending configuration requests.

Nobody will notice this, since no customer is running code with the CSCin24965 fix.

There are no known workarounds.
- CSCeb72942

c7301 may unexpectedly reload during POS-OC3MM port adapter OIR with traffic running through on-board GigE interfaces

Workaround: Stop the traffic and initiate OIR.

- CSCeb87286
Enhanced Interior Gateway Routing Protocol (EIGRP) hello messages may be sent from a virtual-access interface when they should not be sent.
This problem is observed on a Cisco router that has the **passive-interface default** or **passive-interface virtual-template** *interface-number* router configuration command enabled.
There are no known workarounds.
- CSCec04016
Auto-domain radius-proxy user logon can crash the box.
This problem occurs if the primary service logon fails because of authentication any wrong tunnel parameters in the tunnel profile can crash the box.
Workaround: Configure correct tunnel parameters.
- CSCec06337
A router may reload with a bus error when a high volume of new PPP connections occurs on the router.
This problem is observed on a Cisco router that is running Cisco IOS Release 12.2(15)T5 or Release 12.3.
There are no known workarounds.
- CSCec06617
Configure the router to send accounting start and stop records for a exec connection and configure the following command **aaa accounting send stop-record authen fail**.
Do a telnet to the router from any other router. Do not enter anything when it prompts to enter a username. After some time it timesout and will say “[Connection to <IP Addr> closed by foreign host]”
When the telnet connection timesout, two accounting stop records are generated
There are no known workarounds.
- CSCec08434
The Cisco 7200 series boothelper image for Cisco IOS Release 12.2(14)S2 may reload unexpectedly, and the router may return to the ROM monitor (ROMmon) mode.
This problem is observed when you install a 2-port Token Ring Inter-Switch Link 100BASE-TX port adapter (PA-2FEISL-TX) or a 1-port ATM Enhanced OC-3 Packet-over-SONET (POS) port adapter in a Cisco 7200 series Network Processing Engine G-1 (NPE-G1) and you reload, reset, or power up the router with the boothelper image.
Workaround: Remove the PA-2FEISL-TX or 1-port ATM Enhanced OC-3 POS port adapter when you reload, reset, or power up the router with the boothelper image. Once the router has booted up, you can reinstall the port adapters.
- CSCec12911
If the Connection to the LNS fails (due to LNS Reboot or redundant LNS-Failover) the SSG needs a long time to send L2TP HELLO packets to tear down control connection and re-establish tunnel to redundant LNS.
During this period quite a few L2TP-HELLOs are sent to LNS.
There are no known workarounds.

- CSCec15964
 Radius server is marked dead and does not show as “UP” after the deadtime interval has expired.
 Two radius servers are configured on LNS, one of them is marked as Dead during the bootup process because it was not able to respond to system accounting request.
 When PPP sessions come up LNS is still trying to send radius request to dead radius server but now it can access that AAA server because LNS builds up the routing information. LNS is getting responses back from the radius server.
 LNS is not changing the status of that radius server to UP. Even after the elapse of configured dead time.
 There are no known workarounds.
- CSCec24098
 When SSG control error debugs are enabled, “Stale network routes” error message is displayed.
 This will happen if there are exclude networks (“E”) configured in the service profile and if the user logs on to this service and does an account logoff.
 There are no known workarounds.
- CSCec27942
 Virtual-access interface not freed when client session torn down.
 Client session was momentarily disconnected and then re-connected.
 There are no known workarounds.
- CSCec30789
 The router unexpectedly reloads at sb_timer_intr_handler.
 There are no known workarounds.
- CSCec31355
 In Cisco IOS 12.3 B releases with CSCeb30098 integrated, LCP renegotiation at the L2TP Network Server after authentication has already completed will cause the session to enter the wt-sss state (as seen in “show vpdn”). Unless the LAC tears down the session, the session may get stuck in the wt-sss state.
 Workaround: Clear the L2TP tunnel that the stuck sessions are part of.
- CSCec32135
set commands that are used with a service policy can cause a router to reload in some circumstances. The **set cos** policy-map class configuration command can cause reloads in addition to other set commands.
 This problem may be observed with configurations that have a service policy with the set command on the interface in combination with one or all of the following three configurations: access-list filtering
 There are no known workarounds.

- CSCec37042

If the boot image is 12.2(16)B2, the router will experience boot failure. The router will boot in boot image, not main IOS image.

This problem occurs under the following conditions:

```
H/W : cisco 7301 (NPE-G1) processor
      cisco 7401ASR (NSE) processor
```

```
S/W : 12.2(16)B2 ( boot image )
      c7301-boot-mz.122-16.B2.bin"
      c7400-kboot-mz.122-16.B2.bin
```

Workaround: Set the router to boot the image from the disk using the **boot system** global configuration command.

- CSCec44985

User does not get connection to service, for a PPPoE user when logs in second time.

This problem is seen with the PBHK enabled and the PPP session is created as a non SSG PPP user session.

This problem is seen only in 12.3(3)B.

There are no known workarounds.

- CSCec45012

SSG hosts are not cleared when the PPP session for that user went down.

Also the **show ssg host** command shows an error message that prints that memory is low. The **show ssg host count** shows that host count is -ve.

This happens under the following circumstances:

1. SSG binds the PPPoX interface dynamically as downlink (because "ssg direction downlink" has been configured under virtual-template interface mode)
2. user behind the PPPoX interface logs in through the web dashboard (SESM)

SSG host is not deleted when the PPP session goes down. Also when the host is deleted using "clear ssg host all", the host count becomes -ve.

Workaround: Make sure that the condition#1 does not occur. This can be done by inserting a dummy ssg-account-info attribute in the access-accept of the PPPoX user. This dummy attribute can be: ssg-account-info "Nabracadabra".

- CSCec46351

c7200 with NSE-1 processor board or c7401 platform, shows %PXF-2-TALLOCFAIL messages repeatedly.

Turning on any routing protocol.

There are no known workarounds.

- CSCec47146

A Cisco router terminating both PPPoE and PPPoA sessions may fail to CEF switch traffic downstream toward the user when different vtemplates are used for the two types of sessions and sub-interfaces are enabled. This problem may affect only a portion of the subscribers.

Workaround: Use one vtemplate for both types of sessions, disable sub-interfaces or disable CEF.

- CSCec48087
The input queue of the Gi0/0 interface on MWAM module, used by a sbyte processor running the SSG application, becomes full if a AAA server failure occurs. From that point on, no traffic is forwarded between the MSFC and the subinterfaces configured on Gi0/0 from within the SSG application on the sbyte (pings between MSFC and subinterfaces on Gi0/0 fail, etc.).
Workaround: Reset the MWAM module.
- CSCec63438
The set command will not work if used in a hierarchical policy at any level
The failure is observed in 12.3(4.4a) on c7200 platform.
There are no known workarounds.
- CSCec64802
c7200 with NSE-1 processor board or c7401 platform, system acts as PPPoA termination point, may crash due to a bus error while establishing session.
PXF unsupported ATM PA is used, and runs PPPoA on it.
Workaround: Replace PXF unsupported ATM PA or disable PPPoA.
- CSCec67336
The router produces the error message:
%AAA-3-BADMETHODERROR: Cannot process authorization method SERVER_GROUP
or the error message:
%AAA-3-BADMETHODERROR: Cannot process accounting method SERVER_GROUP
followed by:
-Process= "AAA Server", ipl= XXX, pid= YYY
where XXX and YYY are arbitrary integers greater than or equal to zero. The router then produces a traceback.
This problem is observed when you configure and then attempt to use an authorization or accounting method list which refers to a server group which contains no servers, and which has never contained any servers since the router booted.
For example, if you configured:
aaa authorization network default group radius but did not configure any radius servers globally, you would see the error message every time a user attempted to perform network authorization.
Only 12.2B and 12.3B releases are affected.
Workaround: Make sure that the server group contains at least one server. To add a radius server to the global group “radius”, configure:
radius-server host <ipv4 address>
To add a tacacs+ server to the global group “tacacs+”, configure:
tacacs-server host <ipv4 address>
To add a server to a RADIUS server group named “foo”, configure:
aaa group server radius foo
server <ipv4 address>

To add a server to a tacacs+ server group named “bar”, configure:

```
aaa group server tacacs+ bar
server <ipv4 address>
```

There are no known workarounds.

- CSCin24965

PPPoE sessions does not come up when some debugs are enabled in the LAC. This could possibly due to the additional time lag introduced by enabling the debugs in the LAC.

This will not happen when “lcp re-negotiation” is not configured in the virtual-template in the LNS side.

There are no known workarounds.

- CSCin38040

SSG mis-behaves (and often crashes) after total number of connections on the box become 64K.

This problem occurs when the number of connections on the box is 64K+.

Workaround: Keep the number of connections to less than 64K.

- CSCin45858

SSG does not forward user traffic to service for certain networks.

When a user is connected to a service with certain networks, upstream packets from user towards service will be dropped.

The following error message will be displayed if “debug ssg data” is enabled:

```
SSG-DATA: CEF-UPST: Unable to find adjacency. Punt (FastEthernet0/0 :
10.0.1.1->10.1.1.1)
SSG-DATA: PROC-UPST : IDB is NULL. Drop (FastEthernet0/0 : 10.0.1.1->10.1.1.1)
This happens when the destination address falls into a service network of
0.0.0.0 with a non-zero netmask.
```

Workaround: Replace the service network so that at least one bit matches the destination address.

- CSCin50030

While using SSG, executing **show align<** indicates that a spurious memory access has occurred.

There are no known workarounds.

- CSCin54101

Some sessions may not come up with aa15snap encap. Does not appear to be related to CSCin45396, dupe of CSCeb0087, as speculated.

There are no known workarounds.

- CSCin54739

Abnormal termination of “show vpdn” output results in spurious access.

Normal config and unconfig does not result in spurious access

There are no known workarounds.

- CSCin54802

AVP 31 (Calling-station-id) is missing from accounting records to prepaid server when SSG radius-proxy users are accessing prepaid service. It happens only when no explicit calling station id is available to SSG.

This problem happens only if:

1. SSG users are radius-proxy users and accessing prepaid service.
2. No Calling station id is received in account logon and service logon.
3. Downlink interface is not a route bridged interface.

This problem was first reported on cisco 7200 platform but same exists on all cisco platforms supporting SSG functionality.

There are no known workarounds.

- CSCin56557

The accounting of input and output bytes/packets for a service connection is not correct. Only upstream traffic is accounted for that service access whereas downstream traffic from that service would be accounted for another service connection.

Could be seen when a user does autologon to 2 no-NAT/passthrough services.

There are no known workarounds.

- CSCin57846

SSG Crashes at ssg_search_conn.

Downstream traffic to a ssg host logged onto a proxyNATed service. This happens after a host logs off a service and immediately same/another host with same NATed IP address logs on to the proxy NATed service.

There are no known workarounds.

- CSCin58372

Memory leak was observed on 3745 platform.

Mem-leak is seen when SSG subscriber access his SOHO and the user is logged on to a Tunnel service.

There are no known workarounds.

- CSCin55922

For each authorization retry in timeout quota in SSG traceback at ServiceAuthorize() is seen.

There are no known workarounds.

- CSCin56055

In Cisco IOS Release 12.3(03)B PPP session is not terminated locally when attempt to authorize domain remotely via RADIUS fails.

The following configurations is present on the router:

```
!
username user1@domain1.com password <somepassword>
!
aaa authentication ppp default local group radius
aaa authorization network default local group radius
!
```

No profile for user1@domain1.com is defined remotely on RADIUS.

When a request is made by user user1@domain1.com, the session is not established since no profile exists for domain1.com on remote RADIUS server. However, the session is not terminated locally even though user1@domain1.com is present locally on the router and the authentication method list explicitly states local as the first authentication method.

There are no known workarounds.

- CSCin56817
Traceback is noticed for each login/logout of SSG user.
There are no known workarounds.
- CSCin57018
Spurious memory access when user logoff from the prepaid service.
This problem is seen only in the 12.3(3)B image.
There are no known workarounds.
- CSCin57036
SSG box crashes with __terminate trace.
This can happen if the box is running out of memory and TCP-Redirect is configured.
There are no known workarounds.
- CSCin57718
Real IP assigned by service for an ssg connection is sent as framed-ip attribute in the access-accept to SESM.
When a service (proxy or tunnel) accessing an IP Address for a connection SSG send it to the SESM in response to the service logon request in the framed-ip attribute. This hides the framed-ip of the host in the access-accept.
There are no known workarounds.
- CSCin57902
Any new Access Requests from NAS(GGSN) are not processed by SSG when SSG_dummy_pool fills up.
SSG_dummy_pool fills up when SSG is honoring an Acct-on/Accounting Off along with an accounting stop throttle configuration. Any new Access-Requests from NAS(GGSN) can create this condition.
Workaround: Unconfig and config “ssg radius-proxy” OR a Reload of SSG will clean up this pool.
- CSCin60510
c7200 with NSE-1 processor board or c7401 platform, system acts as LNS (L2TP termination end point), may unexpectedly reload.
With PXF on and IP to L2TP downstream traffic, issue shutdown and no shutdown on physical interface toward LAC router, or issue “clear adjacency”.
Workaround: Use “no ip pxf” or remove L2TP configuration.

Open Caveats—Cisco IOS Release 12.3(1a)B

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

- CSCdz54555

An integrated service adaptor (ISA) card resets itself intermittently. The IP Security (IPSec) connections are affected because of the switchover between the hardware crypto engine and the software crypto engine.

This problem is observed on a Cisco 7200 series router that is configured with an ISA card.

There are no known workarounds.

- CSCin39896

SSG may have extra service routes even after service is deleted.

When 2 services having overlapping networks are bound to the same uplink interface, SSG may have certain routes leftover in the internal tables after service deletion. Those are deleted while deleting the tables. This does not result in any memory leak. If one service is a subset of the other, then traffic to the smaller service network may still be routed via the next-hop for that service even after the service is deleted at some point.

There are no known workarounds.

- CSCin40354

The processor hangs when dir and copy for bootflash is performed at the same time from two different console.

There are no known workarounds, but this can be avoided by not performing read and write operation at same time from two different console.

Resolved Caveats—Cisco IOS Release 12.3(1a)B

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

- CSCdw85843

A Cisco router may reload when the firmware of an Integrated Services Adapter (ISA) generates an error message that indicates that the firmware is no longer synchronized with Cisco IOS software.

This problem is observed on a Cisco 7200 series that is running the IMIX (a mixed-packet definition) pattern with 1400-byte packets.

There are no known workarounds.

- CSCdx55178

Difficulties may occur when you attempt to log in to a Cisco 6400. After you have established a Telnet connection to a Node Route Processor 2 (NRP-2) and press the Enter key, the following user access verification sequence may be displayed, and you cannot log in:

```
Password:
Password:
Password:
% Bad passwords
```

This problem is observed on a Cisco 6400 that is running Cisco IOS Release 12.2(4)B3 only after an interactive ATM ping has occurred. The occurrence of the symptom may depend on the Telnet client.

Workaround: Instead of using an interactive ATM ping, enter the **ping atm interface atm interface vpi vci [seg- loopback | end-loopback] [repeat [timeout]]** privileged EXEC command.

- CSCdx95455

A memory leak may occur on a router after TCP-to-X.25 translation is configured.

This problem is observed if a user attempts to use TCP-to-X.25 translation while a router is already performing translation for the maximum number of configured users. The additional user will not be able to use translation, and the router will leak memory.

There are no known workarounds.

- CSCdz33874

LCP configuration packets are not received on Kumo linecard.

Workaround: If customer wants to tune on PXF while using the ISDN linecard, then the workaround is “turn off fair-queue” and then bring up the session.

Alternative workaround: Do not use this ISDN Kumo linecard while tune on the pxf.

- CSCdz74721

As5300 box crashed when issuing the **copy tftp run** command with the same file which was created with **copy run tftp** previously.

There are no known workarounds.

- CSCea12794

Link Control Protocol (LCP) keepalive functionality may not work properly.

This problem is observed when an LCP keepalive period is configured to last longer than 255 seconds on an interface.

Workaround: Configure the LCP keepalive period to last shorter than 255 seconds.

- CSCea25622

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

System was restarted by reload

This problem is observed on a Cisco 7200 series that is configured with an NPE-G1 and that is running Cisco IOS Release 12.1(14)E.

There are no known workarounds.

- CSCea26993

Multicast traffic may get dropped by a Cisco router that is running in dense mode. (Note that all routers have the multicast group in a pruned state even though interested receivers are present.)

This problem is observed when a T-flag is incorrectly set on an (S,G) entry.

A process that is used by dense mode and that is called an Assert process (referred to as Assert) is triggered, causing a designated forwarder (referred to as an Assert winner) to be elected. The Assert winner forwards multicast traffic onto a multiaccess segment when there is more than one router on the segment. If the router that becomes the Assert winner has the T-flag incorrectly set because traffic arrives on its outgoing interface (OIF) rather than on its incoming interface (IIF), multicast traffic is dropped as a result of Reverse Path Forwarding (RPF).

The Assert winner is based on the lowest administrative distance that is required to reach the source. When administrative distances are equal, the Interior Gateway Protocol (IGP) metric is used to determine how to reach the source. When both the administrative distance and the IGP metric are equal, the router with the highest IP address is used as a tiebreaker.

Workaround: Disable Protocol Independent Multicast (PIM) on the interface of the Assert winner that has incorrectly set the T-flag on its (S,G) entry as a result of receiving traffic on its OIF rather than on its IIF.

Alternative Workaround 1: Enter the **ip mroute** *source-address rpf-address distance* global configuration command with a value of 255 for the distance argument on the Assert winner.

Alternative workaround 2: Configure the **ip pim sparse-mode** interface configuration command on the interface of the Assert winner to prevent the interface from operating in dense mode.

- CSCea31186

The RADIUS “Acct-Session-Id” attribute may not be sent correctly.

This problem is observed in a Service Selection Gateway (SSG) configuration that is running Cisco IOS Release 12.2(15)T or a later release when you enter the **ip route-cache flow** interface configuration command on a virtual template. The symptom may also occur in other conditions.

Workaround: In the above-mentioned conditions, deconfigure the **ip route-cache flow** interface configuration command.

- CSCea40426

Encryption and decryption fail for maximum transmission unit (MTU) values between 1419 and 1420 (both inclusive), and the following error is generated:

```
%VPN_HW-1-PACKET_ERROR: slot: 2 Packet Encryption/Decryption error, Other error.
```

The output of the **show pas vam interface** privileged EXEC command displays the “Other Errors” counter; “Other Errors” occur when fragments are reassembled before decryption occurs.

This problem is observed when you use a Cisco router that is configured with a Virtual Private Network (VPN) acceleration module (VAM) to encrypt traffic through generic routing encapsulation (GRE) tunnel endpoints, which are also configured for tag switching.

Workaround: To enable the router to fragment packets differently, reduce the value of the tunnel MTU on the router to 1420 using the **ip mtu 1420** interface configuration command. Note that the MTU values between 1419 and 1420 for which the failure occurs are from the endpoints.

- CSCea42223

Some PVC’s may not come up with autoprovisioning enabled.

Some of the PVC’s may not come up when autopvc + autosense is configured on PA-A6.

Workaround: Reset the interface using the **clear int atm <x/y>** command.

- CSCea51540

The IP Control Protocol (IPCP) times out on a link control protocol (LCP) negotiation.

This problem is observed when dial-up networking (DUN) is used to connect to a Cisco router. Subsequent calls will fail in LCP. The problem is not observed if the user is using only PPP.

There are no known workarounds if both dialing methods are requested.

- CSCea53821

PPP Network Control Protocol negotiation may fail on a Cisco router.

This problem is observed for most PPP protocols on all platforms that are running an image of Cisco IOS Release 12.3 when PPP encapsulation is used via a serial interface.

Workaround: Complete the configuration of PPP protocols at both ends of a connection before you bring up the connection.

Alternative workaround: After you have completed the configuration of PPP protocols, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the serial interface.

- CSCea55600

A Frame Relay (FR) interface may go up and down continuously.

This problem is observed on an FR interface when the keepalive timeout is set to one second and fragmentation and traffic shaping are enabled on multiple permanent virtual circuits (PVCs).

Workaround: Increase the keepalive timeout to 5 seconds or more.

- CSCea56667

The memory that is held by the “RTT Responder” process may increase, as is indicated by the amount of memory in the “Hold” column in the output of the **show processes memory include {rtt | pid} EXEC** command.

This problem is observed when many jitter probes are sent simultaneously to the same destination port.

Workaround: Do not use the same destination port for all the probes.

Alternative workaround 1: To free memory once in a while, enter the **no rtr responder** global configuration command followed by the **rtr responder** global configuration command.

Alternative workaround 2: Lower the duration of the probes.

- CSCea56700

A Cisco router may restart with a bus error if the following conditions are met:

- Router is Layer 2 Tunneling Protocol (L2TP) network server (LNS) in an L2TP environment
- Cisco IOS Firewall (FW) Context-Based Access Control (CBAC) is active and applied to virtual interface template
- Access control list (ACL) for each L2TP client is downloaded from RADIUS, and there are a number of users connected that are producing live traffic

This problem is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(15)T.

There are no known workarounds.

- CSCea61004

Connection interim accounting records are drifted upto 60 secs.

When interm accounting is enabled for services and interim accounting records are not sent at the correct interval configured.

There are no known workarounds.

- CSCea64506

The following error message may be generated on a Cisco router:

```
%CLNS-3-BADPACKET: ISIS: L1 LSP, option 222 tlv length 2 is bad
```

This problem is observed in a multi-topology configuration when IP version 6 (IPv6) Intermediate System-to-Intermediate System (IS-IS) is enabled.

There are no known workarounds.

- CSCea65313
On 7301 router IPv6 packets are getting process switched, running 12.2(15)B or latest 12.2(16)B candidate image.
There are no known workarounds.
- CSCea66194
Traceback may show up when CNS events are sent.
When CNS events are sent tracebacks may show up.
There are no known workarounds.
- CSCea66336
A Cisco router may be unable to set up a Frame Relay or an ATM permanent virtual connection (PVC). When you enter the **debug ip rsvp traffic-control EXEC** command, the following message is displayed:

```
RSVP-TC: Unable to determine resource provider for tcsb
```


This problem is observed on a Cisco router that is running Cisco IOS Release 12.2(15)T.
There are no known workarounds.
- CSCea67382
A Cisco Session Initiation Protocol (SIP) gateway may not perform a “Call Hold” that is initiated by a SIP re-INVITE request when the Session Description Protocol (SDP) media port parameter is set to zero.
This problem is observed on a Cisco SIP gateway that is running Cisco IOS Release 12.2.
Workaround: Upgrade Cisco IOS software to Release 12.2(1.4).
- CSCea67751
SSG does not send error message code attributes in the Access Reject packets, if the service logon is not successful, such as if it fails due to an unsuccessful service activation or due to a soft rejection (e.g. zero quota, 26,9,253 “QV0” and “QT0”) from OCS (prepaid server). In case of tunnel service logon SSG does create an error message code in Access Reject packets, if a L2TP tunnel setup is unsuccessful.
There are no known workarounds.
- CSCea70033
The configuration of the **pri-group timeslots timeslot-range service mgcp** controller configuration command that is defined under an E1 controller may be deleted when you boot up a Cisco platform.
This problem is observed on a Cisco AS5400 that is running Cisco IOS Release 12.3 but may occur on any Cisco platform that is capable of supporting a Media Gateway Control Protocol (MGCP) PRI E1 connection.
There are no known workarounds.
- CSCea70473
A memory leak may occur in the PPP authorization process on a Cisco 7206VXR.
This problem is observed on a Cisco 7206VXR that is running Cisco IOS Release 12.2(16) and that is configured for PPP over Ethernet (PPPoE). The problem may occur on any Cisco router that is running Cisco IOS Release 12.2 (16).
There are no known workarounds.

- CSCea70885

A Cisco 7200 router running IOS version 12.2(16.1)B1 may print out lots of tracebacks and stop AAA records reporting when “radius-server source-ports 1645-1646” is deconfigured.

There are no known workarounds.
- CSCea71776

There is a know problem with **No SSG enable force** command.

If user tries to clear all the SSG related information on c10k using the **No ssg enable force** then the system may hang and cpu usage will go to 100%.

This can occur if the command **ssg direction downlink** is configured on a virtual-template.

Workaround: In this situation, user need to reboot the whole chassis to recover.
- CSCea72908

Mobile-ip (in CDMA) with SSG does not succeed in CMX solution - and anywhere port-bundle host-key is enabled.

Mobile-ip with SSG (in port-bundle host-key) fails with the following message in “deb ssg ctrl-event”:

```
Starting MSID retry timer
MSID retry timer expired for User/SessionID
```

There are no known workarounds.
- CSCea73696

Virtual Private Network (VPN) routing/forwarding (VRF) IP Security (IPSec) may fail when Rivest, Shamir, and Adleman (RSA) encryption is configured.

This problem is observed on a Cisco router that is running Cisco IOS Release 12.3(1).

There are no known workarounds.
- CSCea77302

An L2TP access concentrator (LAC) may reload under the following circumstances:

PPP over Ethernet (PPPoE) sessions are cleared simultaneously on a LAC from a client and L2TP network server (LNS) and there are a large number of PPPoE sessions.

A command like the **show ip dhcp pool EXEC** command is used on a unit under test (UUT) router when the scroll window is small.

This problem occurs because of a race condition between two threads that are clearing sessions simultaneously, or it occurs when a semaphore is obtained by one thread and the other thread tries to obtain the same semaphore and a block occurs during the deletion.

This problem is observed on a Cisco router that is running Cisco IOS Release 12.2T, Release 12.2(15)BX, or Release 12.3.

There are no known workarounds.
- CSCea78932

A Cisco router that has keepalives turned on and that is configured with the **cns event** global configuration command may not correctly display the termination of the Cisco Networking Services (CNS). The output of the **show cns event connection EXEC** command still shows that the event agent is connected even though the connection has been terminated. Some outgoing events may be lost when this symptom occurs.

This problem is observed on a Cisco 3640 router that has CNS configured.

Workaround: Use the **debug cns event** privileged EXEC command to determine if the event agent is actually connected. When the connection is established, there will be regular activity associated with the keepalives.

- CSCea79610

When Cisco Networking Services (CNS) commands fail authentication by an associated Cisco IE2100 series, two messages may be sent to the CNS event bus:

- The first message, which is the expected error message, misses a value for the identifier tag within the Extensible Markup Language (XML).
- The second message is an incorrect success message, and should be ignored by applications that are connected to the CNS event bus.

This problem is observed when the **cns config initial ip-address** global configuration command, **cns config partial ip-address** global configuration command, and **cns config retrieve** EXEC command fail authentication by the associated Cisco IE2100 series.

There are no known workarounds.

- CSCea86300

A Cisco router acting as a L2TP Network Server may unexpectedly reload under rare circumstances. There are no known workarounds.

- CSCea88409

A memory leak of approximately 20 bytes may occur on a Cisco platform that receives a Cisco Networking Services (CNS) event.

This problem is observed when the length of CNS events is greater than 500 bytes.

Workaround: Limit the length of CNS events to less than or equal to 500 bytes.

- CSCea90941

The EIGRP Stub Routing feature may be missing from the configuration.

This problem is observed when a Cisco router on which the EIGRP Stub Routing feature is enabled is reloaded, or when the Enhanced Interior Gateway Routing Protocol (EIGRP) process is restarted.

There are no known workarounds, you must re-enable the EIGRP Stub Routing feature.

- CSCea91695

When a Cisco Networking Services (CNS) event agent uses the backup gateway, it is not possible to configure the backup gateway to use keepalives. The link should use the same keepalive settings that are used with the primary gateway.

This problem is observed on a Cisco gateway that has the CNS event agent connected to the backup gateway.

There are no known workarounds.

- CSCea91920

Some of the XML tags in the output generated by the Cisco Networking Services (CNS) image agent are misspelled. Some of the XML tags accepted for input by the CNS image agent are misspelled.

This problem is observed on a Cisco router that is configured to run the CNS Image Agent.

Workaround: Send messages to the router with the misspelled tag names, and accept output from the image agent with the misspelled tag names.

- CSCea93108

SSG can reload due to a software forced error.

This can happen while using prepaid services in SSG with a separate radius server defined in the radius profile.

This can happen for services whose name is of length 3, 7, 11, 15 etc.

Workaround: For such services, use the global prepaid server.

- CSCea93882

If Cisco Express Forwarding (CEF) is disabled, a router may reload with the following error message upon the receipt of a malformed generic routing encapsulation (GRE) packet:

```
%ALIGN-1-FATAL: Illegal access to a low address addr=0xA30, pc=0x40992D3C,
ra=0x405E64B8, sp=0x43562838
```

This problem is observed on a Cisco router that has CEF disabled. The problem even occurs without a tunnel configuration on the router.

Workaround: Enable CEF on the router by entering the **ip cef** global configuration command.

- CSCeb00104

When configuration changes are made, a Cisco 7500 series Versatile Interface Processor (VIP) may pause indefinitely, produce large numbers of spurious memory accesses, or reload. This situation may cause the router to detect that interfaces on the VIP are not sending packets and to report that the output of the interfaces is stuck.

This problem is observed on a Cisco 7500 series that is configured for fragmentation and shaping on a Frame Relay interface using modular QoS CLI (MQC).

Workaround: Before you make quality of service (QoS) policy or Frame Relay fragmentation changes on an interface of the VIP, enter the shutdown interface configuration command on the interface.

- CSCeb00875

An ATM PVC configured for autodetection of PPPoA or PPPoE protocol may keep dropping the incoming PPP over ATM frames.

This bug could get triggered on a particular PVC, if PPPoA session is being brought from the other end of the PVC and if there is a change in PVC state for any reason; like ATM OAM taking the VC down.

Workaround: Re-configure the ATM PVC or don't use PPPoX autensing. Configure the PVC for either PPPoA or PPPoE.

Example 1:

```
interface atm 4/0.1
  no pvc 4/43
  pvc 4/43
  .....
```

If the vc is part of a range, configure first the pvc-in-range then the encaps.

Example 2:

```
conf t
range pvc 6/43 6/1000
  pvc-in-range 6/43
  encapsulation aal5mux ppp virtual-Template 1
```

- CSCeb01583

A Cisco router or Cisco universal gateway may reload when you enter the **show ppp multilink EXEC** command.

This problem is observed when Multilink PPP (MLP) bundles transition between the “up” and “down” state.

Workaround: Do not enter the **show ppp multilink EXEC** command.
- CSCeb01888

A call may fail because attributes may not be applied.

This problem is observed when the “template:ip-vrf,” “template:ip- unnumbered,” and “template:ip-addr” attributes are downloaded from the template authorization (that is, the **aaa authorization template** global configuration command is configured) but may not be applied.

Workaround: Configure the “template:ip-vrf,” “template:ip-unnumbered,” and “template:ip-addr” attributes under the virtual template.

Alternative workaround: Configure the “lcp:interface-config” attribute in the per-user profiles.
- CSCeb06567

The NetFlow microcode may be flawed and cause the Parallel Express Forwarding (PXF) engine to reload with the following error message:

```
IHB Exception - watchdog timer expired
```

This problem is observed on a Cisco 7200 series that is configured with a Network Service Engine (NSE) and on a Cisco 7401.

Workaround: Disable PXF if this is an option. Otherwise, there is no workaround.
- CSCeb09370

A Cisco router reloads when the Cisco Networking Services (CNS) image agent and CNS image agent password are unconfigured using the **no cns image** and **no cns image password password** global configuration commands.

This problem is observed on a Cisco router when the **cns image** global configuration commands are unconfigured.

Workaround: Do not unconfigure the **cns image password password** global configuration command after the image agent is unconfigured using the **no cns image** global configuration command.
- CSCeb61701

The “wlan reconnect” feature is not working for PWLAN users.

In the PWLAN scenario, a user performs EAPSIM authentication and is logged on. “ssg wlan reconnect” is configured on the SSG and the user then logs off.

On sending an Acct-Status-Query from the SESM the user is logged in again. The user has three Auto-logon services and is able to login to the Tunnel service but is unable to login to the Passthrough and Proxy Service.

There are no known workarounds.
- CSCeb18293

The Cisco Networking Services (CNS) exec agent configuration is lost after a Cisco router reloads.

This problem is observed on all Cisco routers that are running Cisco IOS Release 12.3.

Workaround: Always configure a host name or an IP address for the CNS exec agent, even if one is not needed. Use an IP address that is not known to have a device at that address or a string name that will fail upon DNS lookup.

- CSCeb26162

In some cases, a Cisco router terminating PPP sessions will delay the transmission of Radius Accounting-On message for too long, thus clearing the accounting data on the Radius server about the sessions which are already up.

Workaround: Reset the PPPoX clients that connected too early.

- CSCeb49148

When SSG is configured to do Session Identification with Framed IP in Radius Proxy mode, it is unable to proxy the Access Requests from the NAS(GGSN) whenever the NAS is reusing the Radius Packet ID. Since this ID can take a value from 0 to 255, the problem is seen when the NAS is sending more than 255 Access Requests at the rate of 10/sec. At slower activation rates from NAS the issue will not be seen.

Workaround: Use Session identification with MSID.

- CSCeb53162

c7200 with NSE-1 processor board or c7401 platform, acts as L2TP session termination end-point, system crashes due to memory corruption.

With PXF on, per-user rate-limit configuration is downloaded from AAA server, on high traffic rate (about 120Mbps) and high CPU load (about 70%). It happens as the sessions go up/down, when users log on/off.

There are no known workarounds.

- CSCin16800

Traffic from one Service Selection Gateway (SSG) host to another is routed directly to the second host.

This problem is observed for traffic from one subscriber to another subscriber. It occurs when the second subscriber's address falls into the service network to which the first subscriber is connected. The traffic is forwarded directly to the second subscriber instead of going to the service network. If the connections are Network Address Translation (NAT) connections, then NAT is not applied to user traffic.

There are no known workarounds.

- CSCin31767

A Cisco router may reload when you enter the **show atm map** privileged EXEC command.

This problem is observed on all Cisco routers after you have first deleted a subinterface on which a static map bundle was configured.

Workaround: First remove the static map bundle then delete the subinterface.

- CSCin40163

An ATM interface may remain administratively down.

This problem is observed when commands do not have any effect because the command-line interface (CLI) does not function. The problem are platform independent.

There are no known workarounds.

- CSCin40575

SSG may reload while using large number of prepaid connections.

If SSG runs out of memory when a large number of prepaid sessions are in use, it may cause a bus error.

There are no known workarounds.

- CSCin40647
Error messages appear when serial interface is configured as multilink on 7200 NSE-1 and 7401 platforms.
Only happens in the first few minutes when traffic is being sent.
Workaround: Turn off pxf.
- CSCin40652
After a Media Gateway Control Protocol (MGCP) channel-associated signaling (CAS) call is established, there may not be voice-path continuity; the call signaling is properly terminated, but there is only one-way voice traffic.
This problem is observed on a Cisco router that uses an MGCP CAS call flow.
There are no known workarounds.
- CSCin40713
On any platform which supports configuration on interface before the hardware is physically present, ATM PVC creation fails, reporting multiple users configuration.
There are no known workarounds.
- CSCin41018
The ignore counters on the Fast Ethernet interface increases when 30MBps traffic is passed through. About 0.14% packets are ignored on the ingress interface.
The problem is seen only when L2TP over FE is configured and if the packet size is 64 bytes. For packet size 128 bytes and above, expected throughput is obtained.
There are no known workarounds.
- CSCin41280
Under certain loading conditions, a router may reload as a result of issuing a command to clear a virtual access interface. This is a timing window, so the exact conditions are difficult to define, but the trigger event is a request to clear a virtual access interface.
There are no known workarounds.
- CSCin41414
A Cisco 7200 series may reload.
This problem is observed when you enter the **verify EXEC** command on a Flash card device.
There are no known workarounds.
- CSCin41855
Session Limit information is being downloaded from the RADIUS server during Pre-Authentication, but it is not being applied to the sessions.
There are no known workarounds.
- CSCin41510
An output service policy with a police feature may be rejected, and the following error message may be generated:

```
Cannot attach flat policy to pvc/sub-interface. Hierarchical policy with shape in class-default is recommended
```


This problem is observed when the output service policy is attached to multiple subinterfaces.
There are no known workarounds.

- CSCin41525

When packets are intercepted and replicated with IP version 6 (IPv6) encapsulation, packets that are replicated to the Mediation Device (MD) may be process switched at the MD interface instead of being switched by using Cisco Express Forwarding (CEF). This situation may affect the performance of the router.

This problem is observed on a Cisco router that is running Cisco IOS Release 12.3 and occurs when the intercepted packets are replicated with IPv6 encapsulation.

There are no known workarounds.

- CSCin42216

If tunnel accounting is enabled and an L2X tunnel is initiated, spurious memory access may be observed at the router.

There are no known workarounds.

- CSCin42253

Tracebacks are observed when a pppoe tunnel with Tunnel-Link accounting turned on shuts down.

There are no known workarounds.

- CSCin42549

If you configure the **radius-server host x.x.x.x backoff exponential key SomeKey** command and then enter the **copy run start** command, the configuration that is stored will be as follows:

radius-server host x.x.x.x key SomeKey backoff exponential

As a result, the router will use “SomeKey backoff exponential” as the key for communicating with the RADIUS server instead of “SomeKey.”

This prevents the RADIUS server from communicating with the router and results in the following symptoms, downloadable configurations are ignored:

- Users are unable to authenticate.
- Accounting records are dropped.

If the **service password-encryption** global configuration command is configured, you will see an error message that resembles the following message:

```
%Invalid encrypted key: 02050D480809 backoff exponential max-delay 3 backoff-
retry 8
```

This problem is observed any time you configure a RADIUS server with backoff exponential and a per-server key.

Workaround: Perform the following steps:

1. Configure the **radius-server host x.x.x.x backoff exponential key SomeKey** command.
2. Copy the running configuration to a TFTP or FTP server and edit the running configuration with a text editor to place the **key SomeKey** portion of the **radius-server host** configuration line at the end of the line.
3. Enter the **copy tftp start** or **copy ftp start** global configuration command to place the configuration in the router’s startup configuration.
4. Do not enter the **copy run start** global configuration command.

Alternative workaround: Do not configure a per-server key. Use a global key instead.

- CSCin42662
7200VXR having pri-group configuration may crash with bus error exception.
If we remove the Pri-group when all b-channels of pri-group are up and we are passing the bi-directional traffic.
There are no known workarounds.
- CSCin42824
When you configure a radius server, generate some radius traffic, configure a second radius server with the same ip address, but different ports, and then unconfigure the first radius server, the router will stop sending radius packets. When you then try to unconfigure the second radius server, the router will generate a traceback.
Workaround: Instead of configuring the second radius server before unconfiguring the first, unconfigure the first radius server, and then configure the second radius server.
- CSCin43411
SSG crashes with the tracebacks pointing to timerwheel code.
This problem is seen with 12.2(16)B image when interim accounting interval is changed at the same time a connection is inactive.
Workaround: Do not change the interim accounting interval, when SSG is trying to bring up the connections.
- CSCin43415
Router reloads due to bus error.
When an SSG user logs into a tunnel service and the tunnel session is cleared, SSG will encounter a bus error while trying to bring down the connection.
There are no known workarounds.
- CSCin43828
A Traceback and Register display with a cause listed as:
`Cause 0000041C (Code 0x7): Data Bus Error exception`
The condition reported was associated with a router being operated outside of its temperature parameters. Other physical or hardware associated issues could lead to this condition.
There are no known workarounds.
- CSCin44460
With “radius-server domain stripping” configured in the LNS, when a user (say user@cisco.com) initiates a session, the LNS should strip the domain part (cisco.com) and use only the user part (user) for authentication.
In Cisco IOS Release 12.3(0.5)B, the LNS sends the complete username (user@cisco.com) to the radius server.
There are no known workarounds.
- CSCin45728
When local forwarding is enabled on a Service Selection Gateway (SSG), router may reload.
This problem occurs on a Cisco 7200 that is running Cisco IOS Release 12.2(15)B, with SSG enabled. Also, local forwarding is enabled in SSG.
There are no known workarounds.

- CSCin45820
 Proxy-state attribute is not being sent by SSG when SSG is doing radius-proxy. This is inconsistent to the previous SSG behavior.
 Proxy-state attribute is not being sent with recent SSG images, i.e. after 12.2(16)B.
 There are no known workarounds.
- CSCin47430
 Router may reload when memory is exhausted or there is memory fragmentation while creating SSG host objects
 There are no known workarounds.
- CSCin47493
 Cisco 7200 router with NSE-1 might crash when PXF is enabled.
 When traffic is sent on ATM PA-A3 interface on Cisco 7200 router running 12.2(15)B1 image and PXF is enabled, the router may crash with ALIGN-1-FATAL error.
 There are no known workarounds.
- CSCin47884
 SSG does not activate the EAP-SIM user - after the SIM authentication has happened successfully.
 This happens with 12.2(16)B SSG image when AP accounting is enabled.
 Work-Around: Disable accounting on AP.
- CSCin50873
 Bunch of data packets gets punted to process path, when SSGTimeout process is scheduled.
 This problem will be seen in all the SSG images.
 There are no known workarounds.
- CSCin51366
 When there are two or more servers in a server group, all the servers in that group are dead, and transactions are being sent to those servers because the server group they are in (including the special groups radius and tacacs) is the last method in a method list, then the reference count of one server in the group will be increased dramatically, while the reference count of another server in the group will be reduced to zero.
 You can observe server reference count changes by turning on **debug aaa server-ref-count**
 After the reference count of a server reaches zero without the server being unconfigured, you may see the error message:

```
AAA/SG/REF_COUNT attempt to decrement ref count of invalid server handle XXXXXXXX
where 'XXXXXXXX' is a seemingly random hexadecimal number.
```

 In some IOS images, particularly those with the -g4js- feature set, the router may crash instead of producing the error message.
 Workaround: Pick one particular server from the group as your server of last resort, configure a special server group containing only that server, and configure that special server group as the last method in your method list.

For example, if you had:

```
aaa new-model
radius-server host x.x.x.x
radius-server host y.y.y.y
radius-server host z.z.z.z
radius-server key SECRET
aaa group server radius foo
  server x.x.x.x
  server y.y.y.y
  server z.z.z.z
aaa authentication login default group foo
```

You would instead configure:

```
aaa new-model
radius-server host x.x.x.x
radius-server host y.y.y.y
radius-server host z.z.z.z
radius-server key SECRET
aaa group server radius foo
  server x.x.x.x
  server y.y.y.y
  server z.z.z.z
aaa group server radius bar
  server z.z.z.z
aaa authentication login default group foo group bar
```

- CSCin53297

When the command **no radius-server unquie-ident <xx>** is issued, “interval 10” is appended to the previous radius-server command in the configuration.

Workaround: Reissue the **radius-server unquie-ident <yy>** command.



Note The value <yy> does not have to be identical to the previously issued 'no' version of the command.

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, and other documents.

Documentation is available as printed manuals or electronic documents.

Use these release notes with these documents:

- [Release-Specific Documents, page 97](#)
- [Platform-Specific Documents, page 97](#)
- [Feature Modules, page 98](#)
- [Cisco IOS Software Documentation Set, page 98](#)

Release-Specific Documents

For Use in T Train and Special Train Release Notes

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: Cisco IOS Release 12.3

On the Documentation CD-ROM at:

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

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

Technical Documents

- *Caveats for Cisco IOS Release 12.3* and *Caveats for Cisco IOS Release 12.3 T*

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

On Cisco.com at:

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

On the Documentation CD-ROM at:

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



Note

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

Platform-Specific Documents

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

- *Cisco 7000 Hardware Installation and Maintenance*
- *Cisco 7000 User Guide*
- *Cisco 7010 User Guide*
- *Cisco 7200 VXR Installation and Configuration Guide*
- *Cisco 7200 VXR Quick Start Guide*
- *Cisco 7202 Installation and Configuration Guide*

- *Cisco 7204 Installation and Configuration Guide*
- *Cisco 7206 Installation and Configuration Guide*
- *Cisco 7206 Quick Start Guide*
- *Cisco 7301 Installation and Configuration Guide*
- *Cisco 7301 Router Quick Start Guide*
- *Cisco 7401ASR Installation and Configuration Guide*
- *Cisco 7401ASR Quick Start Guide*
- *Quick Reference for Cisco 7204 Installation*
- *Quick Start Guide Cisco 7100 Series VPN Router*

Change the paths in this section so they go to your platform-specific documents.

On Cisco.com at:

Technical Documents: Documentation Home Page: Core/High-End Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: Core/High-End Routers

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.3(5a)B5 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

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

On the Documentation CD-ROM at:

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

Cisco 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 12](#) 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

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

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

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
<hr/> <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 12.3Based 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) <hr/>	

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 96.

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 © 2002-2007
Cisco Systems, Inc.
All rights reserved.

