Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 B

March 26, 2008

Cisco IOS Release 12.2(16)B2

OL-1907-12

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(16)B2. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(16)B2, see the "Caveats for Cisco IOS Release 12.2 B" section on page 99 and *Caveats for Cisco IOS Release 12.2 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 12.2 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/ to give us your feedback.

Contents

These release notes describe the following topics:

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

System Requirements

This section describes the system requirements for Cisco IOS Release l2.2 B and includes the following sections:

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.2(16)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	20 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	20 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	20 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	20 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	20 MB	128 MB	RAM

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.2(16)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	32 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	32 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	32 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	32 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	32 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	32 MB	128 MB	RAM

Table 2 Images and Memory Recommendations for Cisco IOS Release 12.2(16)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	20 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	20 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	20 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	20 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	20 MB	128 MB	RAM

Table 2 Images and Memory Recommendations for Cisco IOS Release 12.2(16)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	32 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	32 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	32 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	32 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	32 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	32 MB	128 MB	RAM

Table 3 Images and Memory Recommendations for Cisco IOS Release 12.2(16)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	20 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	20 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	20 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	20 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	20 MB	128 MB	RAM

Table 3 Images and Memory Recommendations for Cisco IOS Release 12.2(16)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	32 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	32 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	32 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	32 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	32 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	32 MB	128 MB	RAM

Table 4 Images and Memory Recommendations for Cisco IOS Release 12.2(15)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	20 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	20 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	20 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	20 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	20 MB	128 MB	RAM

Table 4 Images and Memory Recommendations for Cisco IOS Release 12.2(15)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	32 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	32 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	32 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	32 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	32 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	32 MB	128 MB	RAM

Table 5 Images and Memory Recommendations for Cisco IOS Release 12.2(4)B8

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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	16 MB	128 MB	RAM

Table 5 Images and Memory Recommendations for Cisco IOS Release 12.2(4)B8 (continued)

Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	16 MB	128 MB	RAM

Table 6 Images and Memory Recommendations for Cisco IOS Release 12.2(4)B7

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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	16 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	16 MB	128 MB	RAM

Table 7 Images and Memory Recommendations for Cisco IOS Release 12.2(4)B6

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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	16 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	16 MB	128 MB	RAM

Table 8 Images and Memory Recommendations for Cisco IOS Release 12.2(4)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	16 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	16 MB	128 MB	RAM

Table 9 Images and Memory Recommendations for Cisco IOS Release 12.2(4)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	16 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	16 MB	128 MB	RAM

Table 10 Images and Memory Recommendations for Cisco IOS Release 12.2(4)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	16 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	16 MB	128 MB	RAM

Table 11 Images and Memory Recommendations for Cisco IOS Release 12.2(4)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	16 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	16 MB	128 MB	RAM

Table 12 Images and Memory Recommendations for Cisco IOS Release 12.2(4)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	16 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	16 MB	128 MB	RAM

Table 13 Images and Memory Recommendations for Cisco IOS Release 12.2(4)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	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	16 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7400-jo3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 56	c7400-jk8o3s-mz	16 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7400-jk9o3s-mz	16 MB	128 MB	RAM
	SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	16 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(16)B2 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 7401ASR routers

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 42.

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 12.2(16)B2:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 B Software (c7200-is-mz), Version 12.2(16)B2, RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

http://www.cisco.com/warp/public/620/6.html

Feature Set Tables

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

Cisco IOS Release 12.2(16)B2 supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2(16)B2 can include new features supported by the Cisco 7000 family.

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

Table 14 through Table 17 lists the features and feature sets for Cisco 7200 series routers. Table 19 through Table 21 lists the features and feature sets for Cisco 7400 series routers.

The tables use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (4) means a feature was introduced in 12.2(4)B5. If a cell in this column is empty, the feature was included in the initial base release.

Note This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

Table 14 Feature List by Feature Set for the Cisco 7200 Series, Part 1

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
Dial					
VPDN Group Session Limiting	(4)	Yes	Yes	Yes	Yes
Quality of Service					
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	Yes	Yes	Yes	Yes
Miscellaneous					
ACFC and PFC Handling During PPP Negotiation	(15)	Yes	Yes	Yes	Yes
ATM OAM Ping	(4)	Yes	Yes	Yes	Yes
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	Yes	Yes	Yes	Yes
DHCP Relay Support for MPLS VPN Suboptions	(4)	Yes	Yes	Yes	Yes
Direct-Request (Domain Stripping) VRF Aware	(4)	Yes	Yes	Yes	Yes
EXEC Commands in Configuration Mode	(15)	Yes	Yes	Yes	Yes
Extended Support for Radius att 32	(4)	Yes	Yes	Yes	Yes
Hierarchical Policing in Service Selection Gateway	(4)	No	No	No	No
IP Pool Backup	(15)	Yes	Yes	Yes	Yes
ISDN PRI-SLT	(15)	Yes	Yes	Yes	Yes
L2TP Extended Failover	(4)	Yes	Yes	Yes	Yes
L2TP Redirect	(15)	Yes	Yes	Yes	Yes
Local Template-Based ATM PVC Provisioning	(15)	Yes	Yes	Yes	Yes
NSE-Broadband Aggregation Features	(4)	Yes	Yes	Yes	Yes
Packet Data Serving Node (PDSN)	(15)	Yes	Yes	Yes	Yes
PPPoE Session Limit Per NAS Port	(15)	Yes	Yes	Yes	Yes
RADIUS Attribute Screening	(4)	Yes	Yes	Yes	Yes
RADIUS Attributes 52 and 53 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS Attribute 77 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	Yes	Yes	Yes	Yes
RADIUS Logical Line ID	(15)	Yes	Yes	Yes	Yes
RFC-2867 RADIUS Tunnel Accounting	(15)	Yes	Yes	Yes	Yes
Service Selection Gateway	(4), (15)	No	No	No	No
Service Selection Gateway Accounting Update Interval Per Service	(4)	No	No	No	No
Session Limit Per VRF	(4)	Yes	Yes	Yes	Yes
SSG AAA Transaction Enhancements	(4)	No	No	No	No

Table 14 Feature List by Feature Set for the Cisco 7200 Series, Part 1

SSG Autodomain	(4)	No	No	No	No
SSG Autologoff	(4)	No	No	No	No
SSG AutoLogon Using Proxy Radius	(4)	No	No	No	No
SSG Changes to Accommodate New L2TP Error Codes	(16)	No	No	No	No
SSG Open Garden	(4)	No	No	No	No
SSG Port-Bundle Host Key	(4)	No	No	No	No
SSG Prepaid Billing	(4)	No	No	No	No
SSG PTA-MD Exclusion Lists	(4)	No	No	No	No
SSG Service Profile Caching	(15)	No	No	No	No
SSG Suppression of Ununsed Accounting Records	(16)	No	No	No	No
SSG TCP Redirect for Services	(4)	No	No	No	No
Tunnel Authentication via RADIUS on Tunnel Terminator	(15)	Yes	Yes	Yes	Yes
Virtual Template Limit Expansion to 200	(4)	Yes	Yes	Yes	Yes
VRF in PXF	(4)B8	Yes	Yes	Yes	Yes
VPDN Multihop by DNIS	(15)	Yes	Yes	Yes	Yes
VRF and MQC Hierarchical Shaping in PXF	(15)	Yes	Yes	Yes	Yes
VRF in Server Group	(4)	Yes	Yes	Yes	Yes
Multiservice Applications - Broadband DSL					
Dynamic Subscriber Bandwidth Selection	(4)	Yes	Yes	Yes	Yes
EAP SIM Enhancements	(16)	Yes	Yes	Yes	Yes
Framed Route VRF Aware	(4)	Yes	Yes	Yes	Yes
Multilink PPP Minimum Links Mandatory	(15)	Yes	Yes	Yes	Yes
PPPoE over Gigabit Ethernet	(4)	Yes	Yes	Yes	Yes
PPPoE Session Limit	(4)	Yes	Yes	Yes	Yes
SSG Complete ID	(16)	No	No	No	No
SSG Range Command for Bind Statements	(16)	No	No	No	No
SSG Support of NAS Port ID	(16)	No	No	No	No
VLAN Range	(4)	Yes	Yes	Yes	Yes
Security					
Per VRF AAA	(4)	Yes	Yes	Yes	Yes
Switching					
MPLS VPN ID	(4)	Yes	Yes	Yes	Yes
WAN					
SSG Autologoff Enhancement	(15)	No	No	No	No
SSG EAP Transparency	(16)	No	No	No	No
SSG L2TP Dialout	(15)	No	No	No	No
SSG Open Garden Configuration Enhancements	(16)	No	No	No	No

Table 14 Feature List by Feature Set for the Cisco 7200 Series, Part 1

SSG Prepaid Enhancements	(16)	No	No	No	No
SSG Prepaid Idle Timeout	(15)	No	No	No	No
SSG Proxy for CDMA2000	(15)	No	No	No	No
SSG Unconfig	(15)	No	No	No	No
SSG Unique Session ID	(16)	No	No	No	No

Table 15 Feature List by Feature Set for the Cisco 7200 Series, Part 2

		Software Images by Feature Sets			
Features	**In**	**IP/FW/IDS IPSec 56**	**IP/FW/IDS IPSec 3DES**	**Enterprise**	**Enterprise IPSec 56**
Dial					
VPDN Group Session Limiting	(4)	Yes	Yes	Yes	Yes
Quality of Service					
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	Yes	Yes	Yes	Yes
Miscellaneous					
ACFC and PFC Handling During PPP Negotiation	(15)	Yes	Yes	Yes	Yes
ATM OAM Ping	(4)	Yes	Yes	Yes	Yes
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	Yes	Yes	Yes	Yes
DHCP Relay Support for MPLS VPN Suboptions	(4)	Yes	Yes	Yes	Yes
Direct-Request (Domain Stripping) VRF Aware	(4)	Yes	Yes	Yes	Yes
EXEC Commands in Configuration Mode	(15)	Yes	Yes	Yes	Yes
Extended Support for Radius att 32	(4)	Yes	Yes	Yes	Yes
Hierarchical Policing in Service Selection Gateway	(4)	No	No	No	No
IP Pool Backup	(15)	Yes	Yes	Yes	Yes
ISDN PRI-SLT	(15)	Yes	Yes	Yes	Yes
L2TP Extended Failover	(4)	Yes	Yes	Yes	Yes
L2TP Redirect	(15)	Yes	Yes	Yes	Yes
Local Template-Based ATM PVC Provisioning	(15)	Yes	Yes	Yes	Yes
NSE-Broadband Aggregation Features	(4)	Yes	Yes	Yes	Yes
Packet Data Serving Node (PDSN)	(15)	Yes	Yes	Yes	Yes
PPPoE Session Limit Per NAS Port	(15)	Yes	Yes	Yes	Yes
RADIUS Attribute Screening	(4)	Yes	Yes	Yes	Yes
RADIUS Attributes 52 and 53 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS Attribute 77 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	Yes	Yes	Yes	Yes

Table 15 Feature List by Feature Set for the Cisco 7200 Series, Part 2 (continued)

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
RADIUS Logical Line ID	(15)	Yes	Yes	Yes	Yes
RFC-2867 RADIUS Tunnel Accounting	(15)	Yes	Yes	Yes	Yes
Service Selection Gateway	(4), (15)	No	No	No	No
Service Selection Gateway Accounting Update Interval Per Service	(4)	No	No	No	No
Session Limit Per VRF	(4)	Yes	Yes	Yes	Yes
SSG AAA Transaction Enhancements	(4)	No	No	No	No
SSG Autodomain	(4)	No	No	No	No
SSG Autologoff	(4)	No	No	No	No
SSG AutoLogon Using Proxy Radius	(4)	No	No	No	No
SSG Changes to Accommodate New L2TP Error Codes	(16)	No	No	No	No
SSG Open Garden	(4)	No	No	No	No
SSG Port-Bundle Host Key	(4)	No	No	No	No
SSG Prepaid Billing	(4)	No	No	No	No
SSG PTA-MD Exclusion Lists	(4)	No	No	No	No
SSG Service Profile Caching	(15)	No	No	No	No
SSG Suppression of Ununsed Accounting Records	(16)	No	No	No	No
SSG TCP Redirect for Services	(4)	No	No	No	No
Tunnel Authentication via RADIUS on Tunnel Terminator	(15)	Yes	Yes	Yes	Yes
Virtual Template Limit Expansion to 200	(4)	Yes	Yes	Yes	Yes
VRF in PXF	(4)B8	Yes	Yes	Yes	Yes
VPDN Multihop by DNIS	(15)	Yes	Yes	Yes	Yes
VRF and MQC Hierarchical Shaping in PXF	(15)	Yes	Yes	Yes	Yes
VRF in Server Group	(4)	Yes	Yes	Yes	Yes
Multiservice Applications - Broadband DSL					
Dynamic Subscriber Bandwidth Selection	(4)	Yes	Yes	Yes	Yes
EAP SIM Enhancements	(16)	Yes	Yes	Yes	Yes
Framed Route VRF Aware	(4)	Yes	Yes	Yes	Yes
Multilink PPP Minimum Links Mandatory	(15)	Yes	Yes	Yes	Yes
PPPoE over Gigabit Ethernet	(4)	Yes	Yes	Yes	Yes
PPPoE Session Limit	(4)	Yes	Yes	Yes	Yes
SSG Complete ID	(16)	No	No	No	No
SSG Range Command for Bind Statements	(16)	No	No	No	No

Table 15 Feature List by Feature Set for the Cisco 7200 Series, Part 2 (continued)

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
SSG Support of NAS Port ID	(16)	No	No	No	No
VLAN Range	(4)	Yes	Yes	Yes	Yes
Security					
Per VRF AAA	(4)	Yes	Yes	Yes	Yes
Switching					
MPLS VPN ID	(4)	Yes	Yes	Yes	Yes
WAN					
SSG Autologoff Enhancement	(15)	No	No	No	No
SSG EAP Transparency	(16)	No	No	No	No
SSG L2TP Dialout	(15)	No	No	No	No
SSG Open Garden Configuration Enhancements	(16)	No	No	No	No
SSG Prepaid Enhancements	(16)	No	No	No	No
SSG Prepaid Idle Timeout	(15)	No	No	No	No
SSG Proxy for CDMA2000	(15)	No	No	No	No
SSG Unconfig	(15)	No	No	No	No
SSG Unique Session ID	(16)	No	No	No	No

Table 16 Feature List by Feature Set for the Cisco 7200 Series, Part 3

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise/FW/ IDS	Enterprise/ FW/IDS IPSec 56	Enterprise /FW/IDS IPSec 3DES
Dial					
VPDN Group Session Limiting	(4)	Yes	Yes	Yes	Yes
Quality of Service					
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	Yes	Yes	Yes	Yes
Miscellaneous					
ACFC and PFC Handling During PPP Negotiation	(15)	Yes	Yes	Yes	Yes
ATM OAM Ping	(4)	Yes	Yes	Yes	Yes
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	Yes	Yes	Yes	Yes
DHCP Relay Support for MPLS VPN Suboptions	(4)	Yes	Yes	Yes	Yes
Direct-Request (Domain Stripping) VRF Aware	(4)	Yes	Yes	Yes	Yes

Table 16 Feature List by Feature Set for the Cisco 7200 Series, Part 3 (continued)

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise/FW/ IDS	Enterprise/ FW/IDS IPSec 56	Enterprise /FW/IDS IPSec 3DES
EXEC Commands in Configuration Mode	(15)	Yes	Yes	Yes	Yes
Extended Support for Radius att 32	(4)	Yes	Yes	Yes	Yes
Hierarchical Policing in Service Selection Gateway	(4)	No	No	No	No
IP Pool Backup	(15)	Yes	Yes	Yes	Yes
ISDN PRI-SLT	(15)	Yes	Yes	Yes	Yes
L2TP Extended Failover	(4)	Yes	Yes	Yes	Yes
L2TP Redirect	(15)	Yes	Yes	Yes	Yes
Local Template-Based ATM PVC Provisioning	(15)	Yes	Yes	Yes	Yes
NSE-Broadband Aggregation Features	(4)	Yes	Yes	Yes	Yes
Packet Data Serving Node (PDSN)	(15)	Yes	Yes	Yes	Yes
PPPoE Session Limit Per NAS Port	(15)	Yes	Yes	Yes	Yes
RADIUS Attribute Screening	(4)	Yes	Yes	Yes	Yes
RADIUS Attributes 52 and 53 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS Attribute 77 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	Yes	Yes	Yes	Yes
RADIUS Logical Line ID	(15)	Yes	Yes	Yes	Yes
RFC-2867 RADIUS Tunnel Accounting	(15)	Yes	Yes	Yes	Yes
Service Selection Gateway	(4), (15)	No	No	No	No
Service Selection Gateway Accounting Update Interval Per Service	(4)	No	No	No	No
Session Limit Per VRF	(4)	Yes	Yes	Yes	Yes
SSG AAA Transaction Enhancements	(4)	No	No	No	No
SSG Autodomain	(4)	No	No	No	No
SSG Autologoff	(4)	No	No	No	No
SSG AutoLogon Using Proxy Radius	(4)	No	No	No	No
SSG Changes to Accommodate New L2TP Error Codes	(16)	No	No	No	No
SSG Open Garden	(4)	No	No	No	No
SSG Port-Bundle Host Key	(4)	No	No	No	No
SSG Prepaid Billing	(4)	No	No	No	No
SSG PTA-MD Exclusion Lists	(4)	No	No	No	No
SSG Service Profile Caching	(15)	No	No	No	No
SSG Suppression of Ununsed Accounting Records	(16)	No	No	No	No

Table 16 Feature List by Feature Set for the Cisco 7200 Series, Part 3 (continued)

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise/FW/ IDS	Enterprise/ FW/IDS IPSec 56	Enterprise /FW/IDS IPSec 3DES
SSG TCP Redirect for Services	(4)	No	No	No	No
Tunnel Authentication via RADIUS on Tunnel Terminator	(15)	Yes	Yes	Yes	Yes
Virtual Template Limit Expansion to 200	(4)	Yes	Yes	Yes	Yes
VRF in PXF	(4)B8	Yes	Yes	Yes	Yes
VPDN Multihop by DNIS	(15)	Yes	Yes	Yes	Yes
VRF and MQC Hierarchical Shaping in PXF	(15)	Yes	Yes	Yes	Yes
VRF in Server Group	(4)	Yes	Yes	Yes	Yes
Multiservice Applications - Broadband DSL					
Dynamic Subscriber Bandwidth Selection	(4)	Yes	Yes	Yes	Yes
EAP SIM Enhancements	(16)	Yes	Yes	Yes	Yes
Framed Route VRF Aware	(4)	Yes	Yes	Yes	Yes
Multilink PPP Minimum Links Mandatory	(15)	Yes	Yes	Yes	Yes
PPPoE over Gigabit Ethernet	(4)	Yes	Yes	Yes	Yes
PPPoE Session Limit	(4)	Yes	Yes	Yes	Yes
SSG Complete ID	(16)	No	No	No	No
SSG Range Command for Bind Statements	(16)	No	No	No	No
SSG Support of NAS Port ID	(16)	No	No	No	No
VLAN Range	(4)	Yes	Yes	Yes	Yes
Security					
Per VRF AAA	(4)	Yes	Yes	Yes	Yes
Switching					
MPLS VPN ID	(4)	Yes	Yes	Yes	Yes
WAN					
SSG Autologoff Enhancement	(15)	No	No	No	No
SSG EAP Transparency	(16)	No	No	No	No
SSG L2TP Dialout	(15)	No	No	No	No
SSG Open Garden Configuration Enhancements	(16)	No	No	No	No
SSG Prepaid Enhancements	(16)	No	No	No	No
SSG Prepaid Idle Timeout	(15)	No	No	No	No
SSG Proxy for CDMA2000	(15)	No	No	No	No
SSG Unconfig	(15)	No	No	No	No
SSG Unique Session ID	(16)	No	No	No	No

Table 17 Feature List by Feature Set for the Cisco 7200 Series, Part 4

Features	In	Software Images by Feature Sets				
		Desktop/IBM	Desktop/IBM IPSec 56	Desktop/ IBM/FW/IDS	Desktop/IBM /FW/IDS IPSec 56	Desktop/IBM /FW/IDS IPSec 3DES
Dial						
VPDN Group Session Limiting	(4)	Yes	Yes	Yes	Yes	Yes
Quality of Service						
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	Yes	Yes	Yes	Yes	Yes
Miscellaneous						
ACFC and PFC Handling During PPP Negotiation	(15)	Yes	Yes	Yes	Yes	Yes
ATM OAM Ping	(4)	Yes	Yes	Yes	Yes	Yes
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	Yes	Yes	Yes	Yes	Yes
DHCP Relay Support for MPLS VPN Suboptions	(4)	Yes	Yes	Yes	Yes	Yes
Direct-Request (Domain Stripping) VRF Aware	(4)	Yes	Yes	Yes	Yes	Yes
EXEC Commands in Configuration Mode	(15)	Yes	Yes	Yes	Yes	Yes
Extended Support for Radius att 32	(4)	Yes	Yes	Yes	Yes	Yes
Hierarchical Policing in Service Selection Gateway	(4)	No	No	No	No	No
IP Pool Backup	(15)	Yes	Yes	Yes	Yes	Yes
ISDN PRI-SLT	(15)	Yes	Yes	Yes	Yes	Yes
L2TP Extended Failover	(4)	Yes	Yes	Yes	Yes	Yes
L2TP Redirect	(15)	Yes	Yes	Yes	Yes	Yes
Local Template-Based ATM PVC Provisioning	(15)	Yes	Yes	Yes	Yes	Yes
NSE-Broadband Aggregation Features	(4)	Yes	Yes	Yes	Yes	Yes
Packet Data Serving Node (PDSN)	(15)	Yes	Yes	Yes	Yes	Yes
PPPoE Session Limit Per NAS Port	(15)	Yes	Yes	Yes	Yes	Yes
RADIUS Attribute Screening	(4)	No	No	No	No	No
RADIUS Attributes 52 and 53 for DSL	(4)	No	No	No	No	No
RADIUS Attribute 77 for DSL	(4)	No	No	No	No	No
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	No	No	No	No	No

Table 17 Feature List by Feature Set for the Cisco 7200 Series, Part 4 (continued)

Features	In	Software Images by Feature Sets				
		Desktop/IBM	Desktop/IBM IPSec 56	Desktop/ IBM/FW/IDS	Desktop/IBM /FW/IDS IPSec 56	Desktop/IBM /FW/IDS IPSec 3DES
RADIUS Logical Line ID	(15)	No	No	No	No	No
RFC-2867 RADIUS Tunnel Accounting	(15)	Yes	Yes	Yes	Yes	Yes
Service Selection Gateway	(4), (15)	No	No	No	No	No
Service Selection Gateway Accounting Update Interval Per Service	(4)	No	No	No	No	No
Session Limit Per VRF	(4)	Yes	Yes	Yes	Yes	Yes
SSG AAA Transaction Enhancements	(4)	No	No	No	No	No
SSG Autodomain	(4)	No	No	No	No	No
SSG Autologoff	(4)	No	No	No	No	No
SSG AutoLogon Using Proxy Radius	(4)	No	No	No	No	No
SSG Changes to Accommodate New L2TP Error Codes	(16)	No	No	No	No	No
SSG Open Garden	(4)	No	No	No	No	No
SSG Port-Bundle Host Key	(4)	No	No	No	No	No
SSG Prepaid Billing	(4)	No	No	No	No	No
SSG PTA-MD Exclusion Lists	(4)	No	No	No	No	No
SSG Service Profile Caching	(15)	No	No	No	No	No
SSG Suppression of Ununsed Accounting Records	(16)	No	No	No	No	No
SSG TCP Redirect for Services	(4)	No	No	No	No	No
Tunnel Authentication via RADIUS on Tunnel Terminator	(15)	Yes	Yes	Yes	Yes	Yes
Virtual Template Limit Expansion to 200	(4)	Yes	Yes	Yes	Yes	Yes
VRF in PXF	(4)B8	Yes	Yes	Yes	Yes	Yes
VPDN Multihop by DNIS	(15)	Yes	Yes	Yes	Yes	Yes
VRF and MQC Hierarchical Shaping in PXF	(15)	Yes	Yes	Yes	Yes	Yes
VRF in Server Group	(4)	Yes	Yes	Yes	Yes	Yes
Multiservice Applications - Broadband DSL						
Dynamic Subscriber Bandwidth Selection	(4)	Yes	Yes	Yes	Yes	Yes
EAP SIM Enhancements	(16)	Yes	Yes	Yes	Yes	Yes

Table 17 Feature List by Feature Set for the Cisco 7200 Series, Part 4 (continued)

Features	In	Software Images by Feature Sets				
		Desktop/IBM	Desktop/IBM IPSec 56	Desktop/ IBM/FW/IDS	Desktop/IBM /FW/IDS IPSec 56	Desktop/IBM /FW/IDS IPSec 3DES
Framed Route VRF Aware	(4)	Yes	Yes	Yes	Yes	Yes
Multilink PPP Minimum Links Mandatory	(15)	Yes	Yes	Yes	Yes	Yes
PPPoE over Gigabit Ethernet	(4)	Yes	Yes	Yes	Yes	Yes
PPPoE Session Limit	(4)	Yes	Yes	Yes	Yes	Yes
SSG Complete ID	(16)	No	No	No	No	No
SSG Range Command for Bind Statements	(16)	No	No	No	No	No
SSG Support of NAS Port ID	(16)	No	No	No	No	No
VLAN Range	(4)	Yes	Yes	Yes	Yes	Yes
Security						
Per VRF AAA	(4)	Yes	Yes	Yes	Yes	Yes
Switching						
MPLS VPN ID	(4)	Yes	Yes	Yes	Yes	Yes
WAN						
SSG Autologoff Enhancement	(15)	No	No	No	No	No
SSG EAP Transparency	(16)	No	No	No	No	No
SSG L2TP Dialout	(15)	No	No	No	No	No
SSG Open Garden Configuration Enhancements	(16)	No	No	No	No	No
SSG Prepaid Enhancements	(16)	No	No	No	No	No
SSG Prepaid Idle Timeout	(15)	No	No	No	No	No
SSG Proxy for CDMA2000	(15)	No	No	No	No	No
SSG Unconfig	(15)	No	No	No	No	No
SSG Unique Session ID	(16)	No	No	No	No	No

Table 18 Feature List by Feature Set for the Cisco 7200 Series, Part 5

Features	In	Software Images by Feature Sets				
		Enterprise SSG				
Dial						
VPDN Group Session Limiting	(4)	No				
Quality of Service						
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	No				

Table 18 Feature List by Feature Set for the Cisco 7200 Series, Part 5 (continued)

Features	In	Software Images by Feature Sets				
		Enterprise SSG				
Miscellaneous						
ACFC and PFC Handling During PPP Negotiation	(15)	No				
ATM OAM Ping	(4)	No				
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	No				
DHCP Relay Support for MPLS VPN Suboptions	(4)	No				
Direct-Request (Domain Stripping) VRF Aware	(4)	No				
EXEC Commands in Configuration Mode	(15)	No				
Extended Support for Radius att 32	(4)	No				
Hierarchical Policing in Service Selection Gateway	(4)	Yes				
IP Pool Backup	(15)	No				
ISDN PRI-SLT	(15)	No				
L2TP Extended Failover	(4)	No				
L2TP Redirect	(15)	No				
Local Template-Based ATM PVC Provisioning	(15)	No				
NSE-Broadband Aggregation Features	(4)	No				
Packet Data Serving Node (PDSN)	(15)	No				
PPPoE Session Limit Per NAS Port	(15)	No				
RADIUS Attribute Screening	(4)	Yes				
RADIUS Attributes 52 and 53 for DSL	(4)	Yes				
RADIUS Attribute 77 for DSL	(4)	Yes				
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	Yes				
RADIUS Logical Line ID	(15)	No				
RFC-2867 RADIUS Tunnel Accounting	(15)	No				
Service Selection Gateway	(4), (15)	Yes				

Table 18 Feature List by Feature Set for the Cisco 7200 Series, Part 5 (continued)

Features	In	Software Images by Feature Sets				
		Enterprise SSG				
Service Selection Gateway Accounting Update Interval Per Service	(4)	Yes				
Session Limit Per VRF	(4)	Yes				
SSG AAA Transaction Enhancements	(4)	Yes				
SSG Autodomain	(4)	Yes				
SSG Autologoff	(4)	Yes				
SSG AutoLogon Using Proxy Radius	(4)	Yes				
SSG Changes to Accommodate New L2TP Error Codes	(16)	Yes				
SSG Open Garden	(4)	Yes				
SSG Port-Bundle Host Key	(4)	Yes				
SSG Prepaid Billing	(4)	Yes				
SSG PTA-MD Exclusion Lists	(4)	Yes				
SSG Service Profile Caching	(15)	Yes				
SSG Suppression of Ununsed Accounting Records	(16)	Yes				
SSG TCP Redirect for Services	(4)	Yes				
Tunnel Authentication via RADIUS on Tunnel Terminator	(15)	No				
Virtual Template Limit Expansion to 200	(4)	No				
VRF in PXF	(4)B8	No				
VPDN Multihop by DNIS	(15)	No				
VRF and MQC Hierarchical Shaping in PXF	(15)	No				
VRF in Server Group	(4)	No				
Multiservice Applications - Broadband DSL						
Dynamic Subscriber Bandwidth Selection	(4)	No				
EAP SIM Enhancements	(16)	No				
Framed Route VRF Aware	(4)	No				
Multilink PPP Minimum Links Mandatory	(15)	No				
PPPoE over Gigabit Ethernet	(4)	No				
PPPoE Session Limit	(4)	No				
SSG Complete ID	(16)	Yes				

Table 18 Feature List by Feature Set for the Cisco 7200 Series, Part 5 (continued)

Features	In	Software Images by Feature Sets				
		Enterprise SSG				
SSG Range Command for Bind Statements	(16)	Yes				
SSG Support of NAS Port ID	(16)	Yes				
VLAN Range	(4)	No				
Security						
Per VRF AAA	(4)	No				
Switching						
MPLS VPN ID	(4)	No				
WAN						
SSG Autologoff Enhancement	(15)	Yes				
SSG EAP Transparency	(16)	Yes				
SSG L2TP Dialout	(15)	Yes				
SSG Open Garden Configuration Enhancements	(16)	Yes				
SSG Prepaid Enhancements	(16)	Yes				
SSG Prepaid Idle Timeout	(15)	Yes				
SSG Proxy for CDMA2000	(15)	Yes				
SSG Unconfig	(15)	Yes				
SSG Unique Session ID	(16)	Yes				

Table 19 Feature List by Feature Set for the Cisco *7400 Series, Part 1*

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
Dial					
VPDN Group Session Limiting	(4)	Yes	Yes	Yes	Yes
Quality of Service					
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	Yes	Yes	Yes	Yes
Miscellaneous					
ACFC and PFC Handling During PPP Negotiation	(15)	Yes	Yes	Yes	Yes
ATM OAM Ping	(4)	Yes	Yes	Yes	Yes
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	Yes	Yes	Yes	Yes
DHCP Relay Support for MPLS VPN Suboptions	(4)	Yes	Yes	Yes	Yes
Direct-Request (Domain Stripping) VRF Aware	(4)	Yes	Yes	Yes	Yes

Table 19 Feature List by Feature Set for the Cisco ***7400 Series, Part 1***

EXEC Commands in Configuration Mode	(15)	Yes	Yes	Yes	Yes
Extended Support for Radius att 32	(4)	Yes	Yes	Yes	Yes
Hierarchical Policing in Service Selection Gateway	(4)	No	No	No	No
IP Pool Backup	(15)	Yes	Yes	Yes	Yes
ISDN PRI-SLT	(15)	Yes	Yes	Yes	Yes
L2TP Extended Failover	(4)	Yes	Yes	Yes	Yes
L2TP Redirect	(15)	Yes	Yes	Yes	Yes
Local Template-Based ATM PVC Provisioning	(15)	Yes	Yes	Yes	Yes
NSE-Broadband Aggregation Features	(4)	Yes	Yes	Yes	Yes
Packet Data Serving Node (PDSN)	(15)	Yes	Yes	Yes	Yes
PPPoE Session Limit Per NAS Port	(15)	Yes	Yes	Yes	Yes
RADIUS Attribute Screening	(4)	Yes	Yes	Yes	Yes
RADIUS Attributes 52 and 53 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS Attribute 77 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	Yes	Yes	Yes	Yes
RADIUS Logical Line ID	(15)	Yes	Yes	Yes	Yes
RFC-2867 RADIUS Tunnel Accounting	(15)	Yes	Yes	Yes	Yes
Service Selection Gateway	(4), (15)	No	No	No	No
Service Selection Gateway Accounting Update Interval Per Service	(4)	No	No	No	No
Session Limit Per VRF	(4)	Yes	Yes	Yes	Yes
SSG AAA Transaction Enhancements	(4)	No	No	No	No
SSG Autodomain	(4)	No	No	No	No
SSG Autologoff	(4)	No	No	No	No
SSG AutoLogon Using Proxy Radius	(4)	No	No	No	No
SSG Changes to Accommodate New L2TP Error Codes	(16)	No	No	No	No
SSG Open Garden	(4)	No	No	No	No
SSG Port-Bundle Host Key	(4)	No	No	No	No
SSG Prepaid Billing	(4)	No	No	No	No
SSG PTA-MD Exclusion Lists	(4)	No	No	No	No
SSG Service Profile Caching	(15)	No	No	No	No
SSG Suppression of Ununsed Accounting Records	(16)	No	No	No	No
SSG TCP Redirect for Services	(4)	No	No	No	No
Tunnel Authentication via RADIUS on Tunnel Terminator	(8)	Yes	Yes	Yes	Yes
Virtual Template Limit Expansion to 200	(4)	Yes	Yes	Yes	Yes
VRF in PXF	(4)B8	Yes	Yes	Yes	Yes

Table 19 Feature List by Feature Set for the* Cisco *7400 Series, Part 1

VPDN Multihop by DNIS	(15)	Yes	Yes	Yes	Yes
VRF and MQC Hierarchical Shaping in PXF	(15)	Yes	Yes	Yes	Yes
VRF in Server Group	(4)	Yes	Yes	Yes	Yes
Multiservice Applications - Broadband DSL					
Dynamic Subscriber Bandwidth Selection	(4)	Yes	Yes	Yes	Yes
EAP SIM Enhancements	(16)	Yes	Yes	Yes	Yes
Framed Route VRF Aware	(4)	Yes	Yes	Yes	Yes
Multilink PPP Minimum Links Mandatory	(15)	Yes	Yes	Yes	Yes
PPPoE over Gigabit Ethernet	(4)	Yes	Yes	Yes	Yes
PPPoE Session Limit	(4)	Yes	Yes	Yes	Yes
SSG Complete ID	(16)	No	No	No	No
SSG Range Command for Bind Statements	(16)	No	No	No	No
SSG Support of NAS Port ID	(16)	No	No	No	No
VLAN Range	(4)	Yes	Yes	Yes	Yes
Security					
Per VRF AAA	(4)	Yes	Yes	Yes	Yes
Switching					
MPLS VPN ID	(4)	Yes	Yes	Yes	Yes
WAN					
SSG Autologoff Enhancement	(15)	No	No	No	No
SSG EAP Transparency	(16)	No	No	No	No
SSG L2TP Dialout	(15)	No	No	No	No
SSG Open Garden Configuration Enhancements	(16)	No	No	No	No
SSG Prepaid Enhancements	(16)	No	No	No	No
SSG Prepaid Idle Timeout	(15)	No	No	No	No
SSG Proxy for CDMA2000	(15)	No	No	No	No
SSG Unconfig	(15)	No	No	No	No
SSG Unique Session ID	(16)	No	No	No	No

Feature List by Feature Set for the Cisco ***7400 Series, Part 2***

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
Dial					
VPDN Group Session Limiting	(4)	Yes	Yes	Yes	Yes
Quality of Service					
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	Yes	Yes	Yes	Yes
Miscellaneous					
ACFC and PFC Handling During PPP Negotiation	(15)	Yes	Yes	Yes	Yes
ATM OAM Ping	(4)	Yes	Yes	Yes	Yes
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	Yes	Yes	Yes	Yes
DHCP Relay Support for MPLS VPN Suboptions	(4)	Yes	Yes	Yes	Yes
Direct-Request (Domain Stripping) VRF Aware	(4)	Yes	Yes	Yes	Yes
EXEC Commands in Configuration Mode	(15)	Yes	Yes	Yes	Yes
Extended Support for Radius att 32	(4)	Yes	Yes	Yes	Yes
Hierarchical Policing in Service Selection Gateway	(4)	No	No	No	No
IP Pool Backup	(15)	Yes	Yes	Yes	Yes
ISDN PRI-SLT	(15)	Yes	Yes	Yes	Yes
L2TP Extended Failover	(4)	Yes	Yes	Yes	Yes
L2TP Redirect	(15)	Yes	Yes	Yes	Yes
Local Template-Based ATM PVC Provisioning	(15)	Yes	Yes	Yes	Yes
NSE-Broadband Aggregation Features	(4)	Yes	Yes	Yes	Yes
Packet Data Serving Node (PDSN)	(15)	Yes	Yes	Yes	Yes
PPPoE Session Limit Per NAS Port	(15)	Yes	Yes	Yes	Yes
RADIUS Attribute Screening	(4)	Yes	Yes	Yes	Yes
RADIUS Attributes 52 and 53 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS Attribute 77 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	Yes	Yes	Yes	Yes
RADIUS Logical Line ID	(15)	Yes	Yes	Yes	Yes
RFC-2867 RADIUS Tunnel Accounting	(15)	Yes	Yes	Yes	Yes
Service Selection Gateway	(4), (15)	No	No	No	No
Service Selection Gateway Accounting Update Interval Per Service	(4)	No	No	No	No
Session Limit Per VRF	(4)	Yes	Yes	Yes	Yes
SSG AAA Transaction Enhancements	(4)	No	No	No	No

Feature List by Feature Set for the Cisco ***7400 Series, Part 2***

SSG Autodomain	(4)	No	No	No	No
SSG Autologoff	(4)	No	No	No	No
SSG AutoLogon Using Proxy Radius	(4)	No	No	No	No
SSG Changes to Accommodate New L2TP Error Codes	(16)	No	No	No	No
SSG Open Garden	(4)	No	No	No	No
SSG Port-Bundle Host Key	(4)	No	No	No	No
SSG Prepaid Billing	(4)	No	No	No	No
SSG PTA-MD Exclusion Lists	(4)	No	No	No	No
SSG Service Profile Caching	(15)	No	No	No	No
SSG Suppression of Ununsed Accounting Records	(16)	No	No	No	No
SSG TCP Redirect for Services	(4)	No	No	No	No
Tunnel Authentication via RADIUS on Tunnel Terminator	(15)	Yes	Yes	Yes	Yes
Virtual Template Limit Expansion to 200	(4)	Yes	Yes	Yes	Yes
VRF in PXF	(4)B8	Yes	Yes	Yes	Yes
VPDN Multihop by DNIS	(15)	Yes	Yes	Yes	Yes
VRF and MQC Hierarchical Shaping in PXF	(15)	Yes	Yes	Yes	Yes
VRF in Server Group	(4)	Yes	Yes	Yes	Yes
Multiservice Applications - Broadband DSL					
Dynamic Subscriber Bandwidth Selection	(4)	Yes	Yes	Yes	Yes
EAP SIM Enhancements	(16)	Yes	Yes	Yes	Yes
Framed Route VRF Aware	(4)	Yes	Yes	Yes	Yes
Multilink PPP Minimum Links Mandatory	(15)	Yes	Yes	Yes	Yes
PPPoE over Gigabit Ethernet	(4)	Yes	Yes	Yes	Yes
PPPoE Session Limit	(4)	Yes	Yes	Yes	Yes
SSG Complete ID	(16)	No	No	No	No
SSG Range Command for Bind Statements	(16)	No	No	No	No
SSG Support of NAS Port ID	(16)	No	No	No	No
VLAN Range	(4)	Yes	Yes	Yes	Yes
Security					
Per VRF AAA	(4)	Yes	Yes	Yes	Yes
Switching					
MPLS VPN ID	(4)	Yes	Yes	Yes	Yes
WAN					
SSG Autologoff Enhancement	(15)	No	No	No	No
SSG EAP Transparency	(16)	No	No	No	No
SSG L2TP Dialout	(15)	No	No	No	No
SSG Open Garden Configuration Enhancements	(16)	No	No	No	No

Feature List by Feature Set for the Cisco *7400 Series, Part 2*

SSG Prepaid Enhancements	(16)	No	No	No	No
SSG Prepaid Idle Timeout	(15)	No	No	No	No
SSG Proxy for CDMA2000	(15)	No	No	No	No
SSG Unconfig	(15)	No	No	No	No
SSG Unique Session ID	(16)	No	No	No	No

Table 20 Feature List by Feature Set for the Cisco *7400 Series, Part 3*

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise/FW/ IDS	Enterprise/ FW/IDS IPSec 56	Enterprise/F W/IDS IPSec 3DES
Dial					
VPDN Group Session Limiting	(4)	Yes	Yes	Yes	Yes
Quality of Service					
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	Yes	Yes	Yes	Yes
Miscellaneous					
ACFC and PFC Handling During PPP Negotiation	(15)	Yes	Yes	Yes	Yes
ATM OAM Ping	(4)	Yes	Yes	Yes	Yes
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	Yes	Yes	Yes	Yes
DHCP Relay Support for MPLS VPN Suboptions	(4)	Yes	Yes	Yes	Yes
Direct-Request (Domain Stripping) VRF Aware	(4)	Yes	Yes	Yes	Yes
EXEC Commands in Configuration Mode	(15)	Yes	Yes	Yes	Yes
Extended Support for Radius att 32	(4)	Yes	Yes	Yes	Yes
Hierarchical Policing in Service Selection Gateway	(4)	No	No	No	No
IP Pool Backup	(15)	Yes	Yes	Yes	Yes
L2TP Extended Failover	(4)	Yes	Yes	Yes	Yes
L2TP Redirect	(15)	Yes	Yes	Yes	Yes
Local Template-Based ATM PVC Provisioning	(15)	Yes	Yes	Yes	Yes
NSE-Broadband Aggregation Features	(4)	Yes	Yes	Yes	Yes
Packet Data Serving Node (PDSN)	(15)	Yes	Yes	Yes	Yes
PPPoE Session Limit Per NAS Port	(15)	Yes	Yes	Yes	Yes
RADIUS Attribute Screening	(4)	Yes	Yes	Yes	Yes
RADIUS Attributes 52 and 53 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS Attribute 77 for DSL	(4)	Yes	Yes	Yes	Yes
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	Yes	Yes	Yes	Yes
RADIUS Logical Line ID	(15)	Yes	Yes	Yes	Yes

Table 20 Feature List by Feature Set for the* Cisco *7400 Series, Part 3

RFC-2867 RADIUS Tunnel Accounting	(15)	Yes	Yes	Yes	Yes
Service Selection Gateway	(4), (15)	No	No	No	No
Service Selection Gateway Accounting Update Interval Per Service	(4)	No	No	No	No
Session Limit Per VRF	(4)	Yes	Yes	Yes	Yes
SSG AAA Transaction Enhancements	(4)	No	No	No	No
SSG Autodomain	(4)	No	No	No	No
SSG Autologoff	(4)	No	No	No	No
SSG AutoLogon Using Proxy Radius	(4)	No	No	No	No
SSG Changes to Accommodate New L2TP Error Codes	(16)	No	No	No	No
SSG Open Garden	(4)	No	No	No	No
SSG Port-Bundle Host Key	(4)	No	No	No	No
SSG Prepaid Billing	(4)	No	No	No	No
SSG PTA-MD Exclusion Lists	(4)	No	No	No	No
SSG Service Profile Caching	(15)	No	No	No	No
SSG Suppression of Ununsed Accounting Records	(16)	No	No	No	No
SSG TCP Redirect for Services	(4)	No	No	No	No
Tunnel Authentication via RADIUS on Tunnel Terminator	(15)	Yes	Yes	Yes	Yes
Virtual Template Limit Expansion to 200	(4)	Yes	Yes	Yes	Yes
VRF in PXF	(4)B8	Yes	Yes	Yes	Yes
VPDN Multihop by DNIS	(15)	Yes	Yes	Yes	Yes
VRF and MQC Hierarchical Shaping in PXF	(15)	Yes	Yes	Yes	Yes
VRF in Server Group	(4)	Yes	Yes	Yes	Yes
Multiservice Applications - Broadband DSL					
Dynamic Subscriber Bandwidth Selection	(4)	Yes	Yes	Yes	Yes
EAP SIM Enhancements	(16)	Yes	Yes	Yes	Yes
Framed Route VRF Aware	(4)	Yes	Yes	Yes	Yes
Multilink PPP Minimum Links Mandatory	(15)	Yes	Yes	Yes	Yes
PPPoE over Gigabit Ethernet	(4)	Yes	Yes	Yes	Yes
PPPoE Session Limit	(4)	Yes	Yes	Yes	Yes
SSG Complete ID	(16)	No	No	No	No
SSG Range Command for Bind Statements	(16)	No	No	No	No
SSG Support of NAS Port ID	(16)	No	No	No	No
VLAN Range	(4)	Yes	Yes	Yes	Yes
Security					
Per VRF AAA	(4)	Yes	Yes	Yes	Yes

Table 20 Feature List by Feature Set for the Cisco *7400 Series, Part 3*

Switching					
MPLS VPN ID	(4)	Yes	Yes	Yes	Yes
WAN					
SSG Autologoff Enhancement	(15)	No	No	No	No
SSG EAP Transparency	(16)	No	No	No	No
SSG L2TP Dialout	(15)	No	No	No	No
SSG Open Garden Configuration Enhancements	(16)	No	No	No	No
SSG Prepaid Enhancements	(16)	No	No	No	No
SSG Prepaid Idle Timeout	(15)	No	No	No	No
SSG Proxy for CDMA2000	(15)	No	No	No	No
SSG Unconfig	(15)	No	No	No	No
SSG Unique Session ID	(16)	No	No	No	No

Table 21 Feature List by Feature Set for the Cisco 7400 Series, Part 4

		Software Images by Feature Sets				
Features	**In**	**Desktop/IBM**	**Desktop/IBM IPSec 56**	**Desktop/ IBM/FW/IDS**	**Desktop/IBM /FW/IDS IPSec 56**	**Desktop/IBM /FW/IDS IPSec 3DES**
Dial						
VPDN Group Session Limiting	(4)	Yes	Yes	Yes	Yes	Yes
Quality of Service						
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	Yes	Yes	Yes	Yes	Yes
Miscellaneous						
ACFC and PFC Handling During PPP Negotiation	(15)	Yes	Yes	Yes	Yes	Yes
ATM OAM Ping	(4)	Yes	Yes	Yes	Yes	Yes
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	Yes	Yes	Yes	Yes	Yes
DHCP Relay Support for MPLS VPN Suboptions	(4)	Yes	Yes	Yes	Yes	Yes
Direct-Request (Domain Stripping) VRF Aware	(4)	Yes	Yes	Yes	Yes	Yes
EXEC Commands in Configuration Mode	(15)	Yes	Yes	Yes	Yes	Yes
Extended Support for Radius att 32	(4)	Yes	Yes	Yes	Yes	Yes
Hierarchical Policing in Service Selection Gateway	(4)	No	No	No	No	No

Table 21 Feature List by Feature Set for the Cisco 7400 Series, Part 4 (continued)

Features	In	Software Images by Feature Sets				
		Desktop/IBM	Desktop/IBM IPSec 56	Desktop/ IBM/FW/IDS	Desktop/IBM /FW/IDS IPSec 56	Desktop/IBM /FW/IDS IPSec 3DES
IP Pool Backup	(15)	Yes	Yes	Yes	Yes	Yes
ISDN PRI-SLT	(15)	Yes	Yes	Yes	Yes	Yes
L2TP Extended Failover	(4)	Yes	Yes	Yes	Yes	Yes
L2TP Redirect	(15)	Yes	Yes	Yes	Yes	Yes
Local Template-Based ATM PVC Provisioning	(15)	Yes	Yes	Yes	Yes	Yes
NSE-Broadband Aggregation Features	(4)	Yes	Yes	Yes	Yes	Yes
Packet Data Serving Node (PDSN)	(15)	Yes	Yes	Yes	Yes	Yes
PPPoE Session Limit Per NAS Port	(15)	Yes	Yes	Yes	Yes	Yes
RADIUS Attribute Screening	(4)	No	No	No	No	No
RADIUS Attributes 52 and 53 for DSL	(4)	No	No	No	No	No
RADIUS Attribute 77 for DSL	(4)	No	No	No	No	No
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	No	No	No	No	No
RADIUS Logical Line ID	(15)	No	No	No	No	No
RFC-2867 RADIUS Tunnel Accounting	(15)	Yes	Yes	Yes	Yes	Yes
Service Selection Gateway	(4), (15)	No	No	No	No	No
Service Selection Gateway Accounting Update Interval Per Service	(4)	No	No	No	No	No
Session Limit Per VRF	(4)	Yes	Yes	Yes	Yes	Yes
SSG AAA Transaction Enhancements	(4)	No	No	No	No	No
SSG Autodomain	(4)	No	No	No	No	No
SSG Autologoff	(4)	No	No	No	No	No
SSG AutoLogon Using Proxy Radius	(4)	No	No	No	No	No
SSG Changes to Accommodate New L2TP Error Codes	(16)	No	No	No	No	No
SSG Open Garden	(4)	No	No	No	No	No
SSG Port-Bundle Host Key	(4)	No	No	No	No	No
SSG Prepaid Billing	(4)	No	No	No	No	No
SSG PTA-MD Exclusion Lists	(4)	No	No	No	No	No

Table 21 Feature List by Feature Set for the Cisco 7400 Series, Part 4 (continued)

Features	In	Software Images by Feature Sets				
		Desktop/IBM	Desktop/IBM IPSec 56	Desktop/ IBM/FW/IDS	Desktop/IBM /FW/IDS IPSec 56	Desktop/IBM /FW/IDS IPSec 3DES
SSG Service Profile Caching	(15)	No	No	No	No	No
SSG Suppression of Ununsed Accounting Records	(16)	No	No	No	No	No
SSG TCP Redirect for Services	(4)	No	No	No	No	No
Tunnel Authentication via RADIUS on Tunnel Terminator	(15)	Yes	Yes	Yes	Yes	Yes
Virtual Template Limit Expansion to 200	(4)	Yes	Yes	Yes	Yes	Yes
VRF in PXF	(4)B8	Yes	Yes	Yes	Yes	Yes
VPDN Multihop by DNIS	(15)	Yes	Yes	Yes	Yes	Yes
VRF and MQC Hierarchical Shaping in PXF	(15)	Yes	Yes	Yes	Yes	Yes
VRF in Server Group	(4)	Yes	Yes	Yes	Yes	Yes
Multiservice Applications - Broadband DSL						
Dynamic Subscriber Bandwidth Selection	(4)	Yes	Yes	Yes	Yes	Yes
EAP SIM Enhancements	(16)	Yes	Yes	Yes	Yes	Yes
Framed Route VRF Aware	(4)	Yes	Yes	Yes	Yes	Yes
Multilink PPP Minimum Links Mandatory	(15)	Yes	Yes	Yes	Yes	Yes
PPPoE over Gigabit Ethernet	(4)	Yes	Yes	Yes	Yes	Yes
PPPoE Session Limit	(4)	Yes	Yes	Yes	Yes	Yes
SSG Complete ID	(16)	No	No	No	No	No
SSG Range Command for Bind Statements	(16)	No	No	No	No	No
SSG Support of NAS Port ID	(16)	No	No	No	No	No
VLAN Range	(4)	Yes	Yes	Yes	Yes	Yes
Security						
Per VRF AAA	(4)	Yes	Yes	Yes	Yes	Yes
Switching						
MPLS VPN ID	(4)	Yes	Yes	Yes	Yes	Yes
WAN						
SSG Autologoff Enhancement	(15)	No	No	No	No	No
SSG EAP Transparency	(16)	No	No	No	No	No
SSG L2TP Dialout	(15)	No	No	No	No	No

Table 21 Feature List by Feature Set for the Cisco 7400 Series, Part 4 (continued)

Features	In	Software Images by Feature Sets				
		Desktop/IBM	Desktop/IBM IPSec 56	Desktop/ IBM/FW/IDS	Desktop/IBM /FW/IDS IPSec 56	Desktop/IBM /FW/IDS IPSec 3DES
SSG Open Garden Configuration Enhancements	(16)	No	No	No	No	No
SSG Prepaid Enhancements	(16)	No	No	No	No	No
SSG Prepaid Idle Timeout	(15)	No	No	No	No	No
SSG Proxy for CDMA2000	(15)	No	No	No	No	No
SSG Unconfig	(15)	No	No	No	No	No
SSG Unique Session ID	(16)	No	No	No	No	No

Table 22 Feature List by Feature Set for the Cisco 7400 Series, Part 5

Features	In	Software Images by Feature Sets				
		Enterprise SSG				
Dial						
VPDN Group Session Limiting	(4)	No				
Quality of Service						
Quality of Service Features for Parallel Express Forwarding (PXF)	(4)	No				
Miscellaneous						
ACFC and PFC Handling During PPP Negotiation	(15)	No				
ATM OAM Ping	(4)	No				
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	(15)	No				
DHCP Relay Support for MPLS VPN Suboptions	(4)	No				
Direct-Request (Domain Stripping) VRF Aware	(4)	No				
EXEC Commands in Configuration Mode	(15)	No				
Extended Support for Radius att 32	(4)	No				
Hierarchical Policing in Service Selection Gateway	(4)	Yes				
IP Pool Backup	(15)	No				
ISDN PRI-SLT	(15)	No				
L2TP Extended Failover	(4)	No				
L2TP Redirect	(15)	No				

Table 22 Feature List by Feature Set for the Cisco 7400 Series, Part 5 (continued)

Features	In	Software Images by Feature Sets				
		Enterprise SSG				
Local Template-Based ATM PVC Provisioning	(15)	No				
NSE-Broadband Aggregation Features	(4)	No				
Packet Data Serving Node (PDSN)	(15)	No				
PPPoE Session Limit Per NAS Port	(15)	No				
RADIUS Attribute Screening	(4)	Yes				
RADIUS Attributes 52 and 53 for DSL	(4)	Yes				
RADIUS Attribute 77 for DSL	(4)	Yes				
RADIUS-based Session/Idle Timer for L2TP LAC	(4)	Yes				
RADIUS Logical Line ID	(15)	Yes				
RFC-2867 RADIUS Tunnel Accounting	(15)	No				
Service Selection Gateway	(4), (15)	Yes				
Service Selection Gateway Accounting Update Interval Per Service	(4)	Yes				
Session Limit Per VRF	(4)	Yes				
SSG AAA Transaction Enhancements	(4)	Yes				
SSG Autodomain	(4)	Yes				
SSG Autologoff	(4)	Yes				
SSG AutoLogon Using Proxy Radius	(4)	Yes				
SSG Changes to Accommodate New L2TP Error Codes	(16)	Yes				
SSG Open Garden	(4)	Yes				
SSG Port-Bundle Host Key	(4)	Yes				
SSG Prepaid Billing	(4)	Yes				
SSG PTA-MD Exclusion Lists	(4)	Yes				
SSG Service Profile Caching	(15)	Yes				
SSG Suppression of Ununsed Accounting Records	(16)	Yes				
SSG TCP Redirect for Services	(4)	Yes				
Tunnel Authentication via RADIUS on Tunnel Terminator	(15)	No				

Table 22 Feature List by Feature Set for the Cisco 7400 Series, Part 5 (continued)

Features	In	Software Images by Feature Sets				
		Enterprise SSG				
Virtual Template Limit Expansion to 200	(4)	No				
VRF in PXF	(4)B8	No				
VPDN Multihop by DNIS	(15)	No				
VRF and MQC Hierarchical Shaping in PXF	(15)	No				
VRF in Server Group	(4)	No				
Multiservice Applications - Broadband DSL						
Dynamic Subscriber Bandwidth Selection	(4)	No				
EAP SIM Enhancements	(16)	No				
Framed Route VRF Aware	(4)	No				
Multilink PPP Minimum Links Mandatory	(15)	No				
PPPoE over Gigabit Ethernet	(4)	No				
PPPoE Session Limit	(4)	No				
SSG Complete ID	(16)	Yes				
SSG Range Command for Bind Statements	(16)	Yes				
SSG Support of NAS Port ID	(16)	Yes				
VLAN Range	(4)	No				
Security						
Per VRF AAA	(4)	No				
Switching						
MPLS VPN ID	(4)	No				
WAN						
SSG Autologoff Enhancement	(15)	Yes				
SSG EAP Transparency	(16)	Yes				
SSG L2TP Dialout	(15)	Yes				
SSG Open Garden Configuration Enhancements	(16)	Yes				
SSG Prepaid Enhancements	(16)	Yes				
SSG Prepaid Idle Timeout	(15)	Yes				
SSG Proxy for CDMA2000	(15)	Yes				
SSG Unconfig	(15)	Yes				
SSG Unique Session ID	(16)	Yes				

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 12.2 B.

New Hardware Features in Cisco IOS Release 12.2(16)B2

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(16)B2.

New Software Features in Cisco IOS Release 12.2(16)B2

There are no new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(16)B2.

New Hardware Features in Cisco IOS Release 12.2(16)B1

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(16)B1.

New Software Features in Cisco IOS Release 12.2(16)B1

There are no new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(16)B1.

New Hardware Features in Cisco IOS Release 12.2(16)B

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(16)B.

New Software Features in Cisco IOS Release 12.2(16)B

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(16)B:

L2TP Disconnect Cause Information

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

Extend L2TP disconnect cause codes as defined in RFC3145.

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 Changes to Accommodate New L2TP Error Codes

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 Changes to Accommodate New L2TP Error Codes

SSG need to accommodate and map the error code from L2TP to pass them on to SESM and Radius Authentication Server. These changes are to complete the L2TP error code work done in PPP/L2TP team. More specifically, in cases where the SSG tunnel (L2TP) service fails or the session setup is unsuccessful the SSG shall answer the service logon request with a radius access reject towards SESM or Radius Authentication Server with a reason describing an error code. The interface to report error code already exists. It needs to be extended to report more granular error codes required by customers. L2TP error codes are generated in compliance with RFC3145

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 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 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.

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.

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 Ununsed Accounting Records feature provides the ability to turn off those accounting records that are not needed on the router.

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.

New Hardware Features in Cisco IOS Release 12.2(15)B

The following new hardware feature is supported by the Cisco 7000 for Cisco IOS Release 12.2(15)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

PA-A6

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

The PA-A6 is a series of single-width, single-port, ATM port adapters for Cisco 7200 series and Cisco 7401ASR routers. With advanced ATM features, the PA-A6 supports broadband aggregation, WAN aggregation, and campus/MAN aggregation.

The PA-A6 port adapters include DS3, E3, and three hardware versions that support the OC-3 standards-based physical interfaces:

- OC-3/STM-1:
  - Multimode—PA-A6-OC3MM(=)
  - Single-mode intermediate reach—PA-A6-OC3SMI(=)
  - Single-mode long reach—PA-A6-OC3SML(=)
- E3—PA-A6-E3
- T3—PA-A6-T3

The PA-A6 supports the following features:

- Up to 8191 simultaneously available virtual circuits (VCs)
- Up to 2000 simultaneous segmentations and reassemblies (SARs)
- ATM adaptation layer 5 (AAL5) for data traffic
- Full available bit rate (ABR) support (Traffic Management 4.0), all modes
- Traffic shaping per VC rates from 2.3 kbps to 155 Mbps, in 2.3-kbps increments
- Line rate performance at 256-byte packets on Cisco 7200 series routers
- Line rate performance at 128-byte packets on a Cisco 7401ASR router
- New ATMizer (ATMizerII+) running at 100 MHz
- Increased SDRAM (32 MB) compared to PA-A3(4 MB)
- Increased SSRAM (1 MB per SAR) compared to PA-A3 (512 KB per SAR)
- Line rate performance at 64-byte packets on unidirectional traffic with trafficshaping
- IP-to-ATM class of service (CoS)
- Non-real-time variable bit rate (nrt-VBR), unspecified bit rate (UBR), constant bit rate (CBR), and available bit rate (ABR) quality of service (QoS)

- Operation, Administration, and Maintenance alarm indication signal (OAM AIS) cells
- Online insertion and removal (OIR) on Cisco 7200 series and Cisco 7401ASR routers
- LAN Emulation (LANE)

New Software Features in Cisco IOS Release 12.2(15)B

The following new software features are supported by the Cisco 7000 for Cisco IOS Release 12.2(15)B:

ACFC and PFC Handling During PPP Negotiation

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

Using the High-level data link (HDLC) Address and Control Field Compression (ACFC) and PPP Protocol Field Compression (PFC) Handling During PPP Negotiation feature you can control the negotiation and application of the Link Control Protocol (LCP) configuration options for HDLC address and control field compression (ACFC) and for PPP protocol field compression (PFC).

If ACFC is negotiated during PPP negotiation, Cisco routers may omit the HDLC header on links using HDLC encapsulation. If PFC is negotiated during PPP negotiation, Cisco routers may compress the PPP protocol field from two bytes to one byte.

The PPP commands described in this document allow ACFC and PFC to be disabled during PPP negotiation, thus allowing the HDLC framing and the protocol field to remain uncompressed.

Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

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

The Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs feature enhances PPP over ATM (PPPoA)/PPP over Ethernet (PPPoE) autosense functionality by providing autosense support on MUX- and SNAP-encapsulated ATM permanent virtual circuits (PVCs). Before the introduction of this feature, PPPoA/PPPoE autosense was supported on SNAP-encapsulated ATM PVCs only.

PPPoA/PPPoE autosense enables a router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) over ATM sessions and to create virtual access based on demand for both PPP types.

This new feature is supported on MUX- and SNAP-encapsulated ATM PVCs and enables the PVC encapsulation type to be autosensed by the router. The router determines the encapsulation type of a PVC by looking at the encapsulation type of the first incoming packet. If the PVC encapsulation type is changed while the PPPoA or PPPoE session on the network access server (NAS) is still up, the incoming packet is dropped, the encapsulation type is reset to autosense, and all sessions are removed from the PVC. The next incoming packet will then determine the new encapsulation type of the PVC.

EXEC Commands in Configuration Mode

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

You can now issue EXEC-level Cisco IOS commands (such as **show**, **clear**, and **debug** commands) from within global configuration mode or other modes by issuing the **do** command followed by the EXEC command.

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.

ISDN PRI-SLT

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

The ISDN PRI-SLT feature allows you to release the ISDN PRI signaling time slot for Redundant Link Manager (RLM) configurations, and for Signaling System 7 (SS7) applications in integrated Signaling Link Terminal (SLT) configurations. This feature supports the use of DS0 time slots for SS7 links, and allows the coexistence of SS7 links and PRI voice and data bearer channels on the same T1 or E1 controller span.

L2TP Redirect

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

The L2TP Redirect feature allows an L2TP network server (LNS) participating in Stack Group Bidding Protocol (SGBP) to send a redirect

message to the L2TP access concentrator (LAC) if another LNS wins the bid. The LAC will then re-initiate the call to the newly redirected LNS.

The feature provides two purposes:

- Allows the user to have more evenly load-balanced sessions among a stack of LNSs
- For multilink calls over Layer 2 Tunneling Protocol (L2TP), eliminates the need for multiple hops

Local Template-Based ATM PVC Provisioning

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

The Local Template-Based ATM Provisioning feature enables ATM permanent virtual circuits (PVCs) to be provisioned automatically as needed from a local configuration. ATM PVC autoprovisioning can be configured on a PVC, an ATM PVC range, or a VC class. If a VC class configured with ATM PVC autoprovisioning is assigned to an interface, all the PVCs on that interface will be autoprovisioned; this configuration is sometimes referred to as an *infinite range*.

Autoprovisioned ATM PVCs are not created until there is activity on the virtual path identifier (VPI)/virtual channel identifier (VCI) pair. When the interface is disabled and re-enabled using the **shutdown** and **no shutdown** commands, autoprovisioned PVCs that are part of a PVC range or infinite range are removed upon shutdown and are not reestablished until the first incoming packet triggers PVC creation. During router reload, autoprovisioned PVCs are created when there is activity on the connection.

The total number of VCs that can be configured on an ATM port adapter is limited by the capacity of port adapter. In cases of ATM link oversubscription, where a PVC range or infinite range is configured to provision more PVCs than the port adapter allows, the PVCs can be configured with a timeout so that they can be dynamically brought down as needed. When the timeout expires, the idle PVCs are removed, allowing the PVC range or infinite range of PVCs to share system resources.

ATM PVC local autoprovisioning supports the following applications: PPP over ATM, PPP over Ethernet, ATM routed bridge encapsulation, and routed RFC 1483.

Multilink PPP Minimum Links Mandatory

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

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

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

Packet Data Serving Node (PDSN)

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

Cisco PDSN is an IOS software feature that enables a Cisco 7206 router to function as a gateway between the wireless Radio Access Network

(RAN) and the Internet. With Cisco PDSN enabled on a router, a stationary or roaming mobile user can access the Internet, a corporate

network intranet, or Wireless Application Protocol (WAP) services. Cisco PDSN supports both Simple IP operation and Mobile IP operation.

PPPoE Session Limit Per NAS Port

Platforms: Cisco 7200 series routers, Cisco 7301 routers, and Cisco 7401ASR 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-authorizecommand. 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.

RADIUS Logical Line ID

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

The RADIUS Logical Line ID feature enables users to track their customers based on the physical lines in which the customer's calls originate. Thus, users can better maintain the profile database of their customers as they move from one physical line to another.

Logical Line Id (LLID) is an alphanumeric string (which must be a minimum of one character and a maximum of 253 characters) that is a logical identification of a subscriber line. The NAS-IP-Address attribute (attribute 4) and the NAS-Port-ID attribute (attribute 5) can be used as physical line identification. LLID is maintained in a customer profile database on a RADIUS server. When the RADIUS server receives a preauthorization request from the L2TP access concentrator (LAC), the server sends the LLID to the LAC as the Calling-Station-ID attribute (attribute 31).

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 AAA Transaction Enhancements

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

The SSG AAA transactions for host logon and service profile downloading have been enhanced. The AAA server can now handle multiple SSG host logon and service profile download requests without stopping SSG processes.

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 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 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.

For more information about CDMA, see the "CDMA Overview" knowledge byte on the Mobile Wireless Knowledge Bytes web page.

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.

For more information about CDMA2000, refer to the "CDMA2000 Overview" knowledge byte on the Mobile Wireless Knowledge Bytes web page.

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 autodomain 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 autodomain 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 autodomain 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 the *Service Selection Gateway* feature module.

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 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.

Tunnel Authentication via RADIUS on Tunnel Terminator

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

The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows the Layer 2 Tunneling Protocol (L2TP) network server (LNS) to perform remote authentication and authorization with RADIUS on incoming L2TP access concentrator (LAC) dialin connection requests. This feature also allows the L2TP LAC to perform remote authentication and authorization with RADIUS on incoming L2TP LNS dialout connection requests.

Before the introduction of this feature, the LNS could only perform L2TP tunnel authentication and authorization locally. These processes can be difficult to maintain across numerous LNSs, especially if the number of virtual private dialup network (VPDN) groups is large, because the LAC information must be configured under the VPDN group configurations of the LNS. Remote RADIUS authentication and authorization allows users to store the LAC configurations on the RADIUS server, thereby avoiding the need to store information locally. Thus, the new LAC information can be added to the RADIUS server as necessary, and the group of LNSs can authenticate and authorize by using a common user database on RADIUS.

VPDN Multihop by DNIS

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

The Cisco VPDN Multihop by DNIS feature allows dialed number identification service (DNIS)-based multihop capability in a virtual private dial-up network (VPDN), which enables customers that dial in to a network using a standard telephone line to take advantage of the aggregation capability offered by multihop switching.

VRF and MQC Hierarchical Shaping in PXF

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

VRF and MQC Hierarchical Shaping in PXF implements Virtual Route Forwarding (VRF) and 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*.

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.

New Hardware Features in Cisco IOS Release 12.2(4)B8

There are no new hardware features supported in Cisco IOS Release 12.2(4)B8.

New Software Features in Cisco IOS Release 12.2(4)B8

The following new software feature is supported in Cisco IOS Release 12.2(4)B8.

VRF in PXF

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

VRF in PXF implements Virtual Route Forwarding (VRF) 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*.

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.

New Hardware Features in Cisco IOS Release 12.2(4)B7

There are no new hardware features supported in Cisco IOS Release 12.2(4)B7.

New Software Features in Cisco IOS Release 12.2(4)B7

There are no new software features supported in Cisco IOS Release 12.2(4)B7.

New Hardware Features in Cisco IOS Release 12.2(4)B6

There are no new hardware features supported in Cisco IOS Release 12.2(4)B6.

New Software Features in Cisco IOS Release 12.2(4)B6

There are no new software features supported in Cisco IOS Release 12.2(4)B6.

New Hardware Features in Cisco IOS Release 12.2(4)B5

There are no new hardware features supported in Cisco IOS Release 12.2(4)B5.

New Software Features in Cisco IOS Release 12.2(4)B5

There are no new software features supported in Cisco IOS Release 12.2(4)B5.

New Hardware Features in Cisco IOS Release 12.2(4)B4

There are no new hardware features supported in Cisco IOS Release 12.2(4)B4.

New Software Features in Cisco IOS Release 12.2(4)B4

There are no new software features supported in Cisco IOS Release 12.2(4)B4.

New Hardware Features in Cisco IOS Release 12.2(4)B3

There are no new hardware features supported in Cisco IOS Release 12.2(4)B3.

New Software Features in Cisco IOS Release 12.2(4)B3

There are no new software features supported in Cisco IOS Release 12.2(4)B3.

New Hardware Features in Cisco IOS Release 12.2(4)B2

There are no new hardware features supported in Cisco IOS Release 12.2(4)B2.

New Software Features in Cisco IOS Release 12.2(4)B2

There are no new software features supported in Cisco IOS Release 12.2(4)B2.

New Hardware Features in Cisco IOS Release 12.2(4)B1

There are no new hardware features supported in Cisco IOS Release 12.2(4)B1.

New Software Features in Cisco IOS Release 12.2(4)B1

There are no new software features supported in Cisco IOS Release 12.2(4)B1.

New Hardware Features in Cisco IOS Release 12.2(4)B

The following new hardware features are supported by the Cisco 7000 for Cisco IOS Release 12.2(4)B:

7401ASR

Platform: Cisco 7401ASR routers

The Cisco 7400 ASR delivers exceptional price/performance to meet the requirements of both enterprise and service providers. With its combination of scalable performance, density, and low per-port pricing, the Cisco 7400 ASR allows network-layer capabilities to be extended to a much wider range of network configurations and environments. Customers can now gain the advantages of high-performance network-layer switching and services, including security, QoS, and traffic management, to more locations throughout the network. The Cisco 7400 ASR contains the following features:

- Form Factor (Stackable 1 rack unit, low power (under 50W), front to back airflow)
- Hardware accelerated network application service with PXF processing
- Cost effective GE to GE Layer 2-7 network services
- Ideal new world CPE with full MPLS and MPLS VPN support
- Flexible WAN connectivity with over 40 interfaces
- (Serial, Channelized, ISDN, Frame, ATM, IP, 64K to OC3)

The Cisco 7400 ASR delivers the full suite of Cisco IOS software services for managing network security, allocating QoS among applications or users, and providing value-added services such as NetFlow accounting and encryption. QoS applications such as committed access rate (CAR), Weighted Random Early Detection (WRED), and Weighted Fair Queuing (WFQ) can be flexibly applied to provide precedence across IP addresses, applications, or specific users with a high level of granularity.

The Cisco 7400 ASR offers scalable density with a very wide range of interfaces, including:

- Ethernet, Fast Ethernet, 100VG-AnyLAN, and Gigabit Ethernet
- Serial and Multichannel
- OC3 POS and OC3 ATM
- SDN Primary Rate Interface (PRI), Basic Rate Interface (BRI), High-Speed Serial Interface (HSSI), packet over T3/E3, multichannel T1/E1/T3, and ATM

The Cisco 7400 ASR uses the same port adapters as the Cisco 7500 Versatile Interface Processor (VIP), thus protecting customer investment in interfaces and simplifying sparing.

The Cisco 7400 ASR sets new standards in price/performance/rack density, meeting requirements for high-performance Layer 3 services at an affordable price. The NSE-1 engine powers the Cisco 7400 ASR. Network Services Engine (NSE-1) takes advantage of parallel processing in order to offer unprecedented price/performance. NSE-1 delivers wire rate OC3 throughput while running concurrent high-touch WAN edge services. It is the first Cisco processing engine to offer integrated hardware

acceleration, increasing Cisco 7400 ASR system performance by 50-300 percent for combined “high touch” edge services. NSE-1 takes advantage of a new technology called Parallel eXpress Forwarding (PXF).

PA-2FE

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The PA-2FE provides two 10/100-Mbps, 10/100BaseT Fast Ethernet/Inter-Switch Link (ISL) interfaces and supports both full-duplex and half-duplex operation. The PA-2FE comes in two models, the PA-2FE-TX and the PA-2FE-FX).

Each Fast Ethernet port on the PA-2FE-TX has an RJ-45 connector to attach to Category 5 unshielded twisted-pair (UTP) cable for 100BASE-TX. Each Fast Ethernet port on the PA-2FE-FX has an SC-type fiber-optic connector for 100BASE-FX.

PA-8PRI

Platforms: Cisco 7200 VXR routers and Cisco 7401ASR routers

The multichannel E1/PRI port adapters (PA-MC-2E1 and PA-MC-8E) integrate data service unit (DSU) functionality and E1 channel support into the Cisco router.

The PA-MC-2E1 or PA-MC-8E1 port adapter provides two or eight independent E1 (120-ohm) connections via RJ-48C connectors. (See Figure 1-1 and Figure 1-2.) The PA-MC-8E1 port adapter can provide up to 128 separate full-duplex High-Level Data Link Control (HDLC) channelized E1, fractional E1, full E1, or unframed E1 interfaces. The PA-MC-2E1 port adapter can provide up to 62 separate full-duplex HDLC channelized E1, fractional E1, full E1, or unframed E1 interfaces.

PA-MC-8TE1+

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The PA-MC-8TE1+ port adapter is a multichannel port adapter that provides eight DSX-1/DS1 or eight G.703 interfaces. The PA-MC-8TE1+ interfaces can be channelized, fractional, ISDN PRI, or nonframed.

The PA-MC-8TE1+ supports Facility Data Link (FDL) in Extended Superframe (ESF) framing on T1 networks, as well as network and payload loopbacks. Bit error rate testing (BERT) is supported on each of the T1 or E1 links. BERT can be run only on one port at a time.

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

New Software Features in Cisco IOS Release 12.2(4)B

The following new software features are supported by the Cisco 7000 for Cisco IOS Release 12.2(4)B:

ATM OAM Ping

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The ATM OAM Ping feature modifies the **ping atm interface atm** and **ping (privileged)** commands, which can be used to send an Operation, Administration, and Maintenance (OAM) packet and display success when the response is received.

This feature provides two ATM OAM ping options:

- End loopback—Verifies end-to-end PVC integrity.
- Segment loopback—Verifies PVC integrity to the neighboring ATM device.

DHCP Relay Support for MPLS VPN Suboptions

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies. The DHCP relay agent option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent.

In some environments, a relay agent resides in a network element that also has access to one or more MPLS Virtual Private Networks (VPNs). If a DHCP server wants to offer service to DHCP clients on those different VPNs, the DHCP server needs to know the VPN in which each client resides. The network element that contains the relay agent typically knows about the VPN association of the DHCP client and includes this information in the relay agent information option.

The DHCP relay agent forwards this necessary VPN-related information to the DHCP server using the following three suboptions of the DHCP relay agent information option:

- VPN identifier
- Subnet selection
- Server identifier override

The VPN identifier suboption is used by the relay agent to tell the DHCP server the VPN for every DHCP request it passes on to the DHCP server, and is also used to properly forward any DHCP reply that the DHCP server sends back to the relay agent.

The subnet selection option allows the separation of the subnet from the IP address used to communicate with the relay agent. In typical DHCP processing, the gateway address specifies both the subnet on which a DHCP client resides, as well as the IP address that the server can use to communicate with the relay agent. Situations exist where the relay agent needs to specify the subnet on which a DHCP client resides that is different from the IP address the server can use to communicate with the relay agent. The subnet selection suboption is included in the relay information option and passed on to the DHCP server. The gateway address is changed to the outgoing interface of the relay agent towards the DHCP server. The DHCP server uses this gateway address to send reply packets back to the relay agent.

The server identifier override suboption value is copied in the reply packet from the DHCP server instead of the normal server ID address. Using this information, the DHCP relay agent then sends the response back to the DHCP client on the correct VPN. The server identifier override suboption contains the incoming interface IP address, which is the IP address on the relay agent that is accessible from the client.

After adding these suboptions to the DHCP relay information option, the gateway address is changed to the outgoing interface of the relay agent towards the DHCP server. When the packets are returned from the DHCP server, the relay agent removes all options and forwards the packets to the DHCP client on the correct VPN.

Direct-Request (Domain Stripping) VRF Aware

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

Using the Direct-Request (Domain Stripping) VRF Aware feature, you can enable VRF aware domain-stripping configurations. Use domain-stripping to strip (truncate) the domain from the username. For example, if you configure Direct-Request (Domain Stripping) where the username is user1@cisco.com, only 'user1' will be sent out as the username.

Configure this feature using the **radius-server domain-stripping** command. Domain stripping can be applied to any particular VRF or non-VRFs users. See the Per VRF AAA feature module for more details.

Dynamic Subscriber Bandwidth Selection

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The Dynamic Subscriber Bandwidth Selection (DBS) feature enables wholesale service providers to sell different classes of service to retail service providers by controlling bandwidth at the ATM Virtual Circuit (VC) level. ATM Quality of Service (QoS) parameters from the subscriber domain are applied to the ATM PVC on which a PPPoE or PPPoA session is established.

Using DBS you can set the ATM permanent virtual circuit (PVC) traffic shaping parameters to be dynamically changed based on the RADIUS profile of a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) user logging in on the PVC. If the user is the first user on that PVC, then the RADIUS profile values override the default values of the PVC. If users already exist on the PVC, then the new value overrides the existing configuration only if it is higher than the existing value. If multiple PPPoE sessions are allowed on a subscriber VC, then the highest peak cell rate (PCR) and sustainable cell rate (SCR) of all the sessions is selected as the PCR and SCR of the VC.

Traffic shaping parameters can be configured locally by IOS CLI in VC-mode, VC-class, range mode, or PVC-in-range mode. These parameters have a lower priority and are overridden by the shaping parameters specified in the domain service profile. Traffic shaping parameters that are CLI configured at the VC class interface or subinterface level are treated as the default QoS parameters for the PVCs to which they apply. These parameters are overriden by the domain service profile QoS parameters of the domain the user is logged in to. If no VC class is configured, the default is the unspecified bit rate (UBR).

When a network access server (NAS) sends a domain authorization request and receives an affirmative response from the RADIUS server, this response may include a “QoS-management” string via vendor-specific attribute 26 for QoS management in the NAS. The QoS management values are configured as part of the domain service profile attributes on the RADIUS server. These values contain PCR and SCR values for particular PVCs. If the QoS specified for a domain cannot be applied on the PVC that the session belongs to, the session is not established.

Changing PVC traffic parameters because of new simultaneous PPPoE sessions on the PVC does not cause existing PPPoE sessions that are already established to disconnect. Changing domain service profile QoS parameters on the RADIUS server does not cause traffic parameters to automatically change for PVCs that have existing sessions.

When you enter the **dbs enable** or **no dbs enable** commands to configure or unconfigure DBS, existing sessions are not disconnected. If you have a session that has been configured for DBS and you configure the **no dbs enable** command on a VC, additional sessions that are configured will display DBS configured QoS values until the first new session is up. After the first session is brought up, the VC has default and locally configured values. If you configure the **dbs enable** command after multiple sessions are already up on the VC, all sessions on that VC have DBS QoS parameters.

Extended Support for Radius att 32

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The Extended Support for Radius att 32 feature adds attribute 32 support from Radius Tunnel Attribute Extensions to IOS Radius. The network access server (NAS) is now identifiable to the RADIUS server, whether the NAS is a Cisco component or not.

Framed Route VRF Aware

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The Framed-Route VRF Aware feature introduces support to make RADIUS Attribute 22 (Framed-Route) and a combination of Attribute 8 (Framed-IP-Address) and Attribute 9 (Framed-IP-Netmask) Virtual Routing Forwarding (VRF) aware. Thus, static IP routes can be applied to a particular VRF table rather than the global routing table.

Hierarchical Policing in Service Selection Gateway

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The Service Selection Gateway (SSG) feature 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.

SSG allows subscribers to choose one or more types of services. Each type of service has its own bandwidth requirements (for instance, suppose an ISP has two types of services, regular and premium. The regular service is cheaper for customers but is allocated less bandwidth per customer than the premium service, which provides more bandwidth and a higher quality connection). SSG, therefore, requires a mechanism to insure bandwidth is distributed properly for customers using different types of services.

Traffic Policing is the concept of limiting the input or output transmission rate of traffic entering or leaving a node. In SSG, Traffic Policing can be used to allocate bandwidth between subscribers and between services to a subscriber to insure all types of services are allocated a proper amount of bandwidth. SSG uses per-user and per-user per-service policing to insure bandwidth is distributed properly between subscribers (per-user policing) and between services to a particular subscriber (per-user per-service policing). Because these policing techniques are hierarchical in nature (bandwidth can be first policed between users and then policed again between services to a particular user), this complete feature is called Hierarchical Policing for SSG.

Per-user policing is used to police the aggregated traffic destined to or sent from a particular subscriber and can only police the bandwidth allocated to a subscriber. Per-user policing cannot identify services to a particular subscriber and police bandwidth between these services.

Per-user per-service policing is used to police the types of services available to a subscriber. Per-user per-service policing is useful when an SSG subscriber is subscribed to more than one service and the multiple services are allocated different amounts of bandwidth (for instance, suppose a single subscriber is paying separately for Internet access and video service but is receiving both services from the same service provider. The video service would likely be allocated more bandwidth than the Internet access service and would likely cost more to the subscriber). Per-user per-service policing provides a mechanism for identifying the types of services (such as video or Internet access in the example) and allocating a proper amount of bandwidth to a particular service.

Hierarchical Policing for SSG Token Bucket Scheme

The Hierarchical Policing for SSG feature limits the input or output transmission rate of traffic based on a token bucket algorithm.

The token bucket algorithm used in SSG Hierarchical Policing analyzes a packet and determines whether the packet should be forwarded to its destination or dropped. The amount of available tokens in the token bucket determine whether a packet is forwarded or dropped; if enough tokens are available, the tokens are removed from the token bucket and the packet is forwarded. The packet is dropped if the token bucket does not have enough available tokens for the packet. Tokens are replenished in the token bucket at regular intervals.

L2TP Extended Failover

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The L2TP Extended Failover feature enables a router to receive a Stop-Control-Connection-Notification (StopCCN) message from its peer during tunnel establishment. This feature also enables a box to receive a Call-Disconnect-Notify (CDN) message during session establishment.

In either case, the router marks the peer IP address as busy for 60 seconds, during which no attempt to establish a session or tunnel is made to that peer. After 60 seconds, the router selects an alternate peer to contact. If a tunnel is already established to this alternate peer, the router uses the existing tunnel to bring up the new session. Otherwise, the router sends a Start-Control-Connection-Request (SCCRQ) message to the alternate peer to initiate tunnel establishment.

MPLS VPN ID

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

Multiple VPNs can be configured in a router. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the router. Alternately, you can use a VPN ID to identify a particular VPN in the router. The VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the routers in the service provider network that services that VPN.

You can use several applications to manage VPNs by VPN ID. For more details on how server applications use the VPN ID, refer to the “Why Is a VPN ID Useful?” section.

Note Configuration of a VPN ID for a VPN is optional. You can still use a VPN name to identify configured VPNs in the router. The VPN name is not affected by the VPN ID configuration. These are two independent mechanisms to identify VPNs.

What Is a VRF?

For each VPN that is configured in a router, the router creates a Virtual Route Forwarding (VRF) instance. The VPN ID is stored in the corresponding VRF structure for the VPN.

The VRF table is a key element in the MPLS VPN technology. VRF tables exist on provider edge routers (PEs) only. More than one VRF table can exist on a PE. A VPN can contain one or more VRF tables on a PE.

A VRF contains the routing information that defines the customer VPN site that is attached to a PE router. A VRF consists of the following elements:

- An IP routing table
- A derived Cisco Express Forwarding (CEF) table
- A set of interfaces that use the forwarding table
- A set of rules and routing protocols that determine what goes into the forwarding table

An IP routing table and the CEF table store packet forwarding information for each VRF. Another routing table and CEF table for each VRF prevent information from being forwarded outside a VPN and prevent packets that are outside a VPN from being forwarded to a router within the VPN.

Components of the VPN ID

Each VPN ID defined by RFC 2685 consists of the following elements:

- An Organizational Unique Identifier (OUI), a three-octet hex number.

  The IEEE Registration Authority assigns OUIs to any company that manufactures components under the ISO/IEC 8802 standard. The OUI is used to generate universal LAN MAC addresses and protocol identifiers for use in local and metropolitan area network applications. For example, an OUI for Cisco Systems is 00-03-6B (hex).
- A VPN index, a four-octet hex number, which identifies the VPN within the company.

Use the vpn id command and specify the VPN ID in the following format:

```
vpn id oui:vpn-index
```

A colon separates the OUI from the VPN index. See the **vpn id** command for more information.

Why Is a VPN ID Useful?

Remote access applications, such as the Remote Authentication Dial-In User Service (RADIUS) and Dynamic Host Configuration Protocol (DHCP), can use the MPLS VPN ID feature to identify a VPN. RADIUS can use the VPN ID to assign dial-in users to the proper VPN, based on the user authentication information.

DHCP

Using DHCP network administrators can centrally manage and automate the assignment of IP addresses in an organization's network. The DHCP application uses the VPN ID as follows:

1. A VPN DHCP client requests a connection to a PE router from a VRF interface.
2. The PE router determines the VPN ID associated with that interface.
3. The PE router sends a request with the VPN ID and other information for assigning an IP address to the DHCP server.
4. The DHCP server uses the VPN ID and IP address information to processes the request.
5. The DHCP server sends a response back to the PE router, allowing the VPN DHCP client access to the VPN.

Remote Authentication Dial-In User Service

A Remote Authentication Dial-In User Service (RADIUS) server (or daemon) provides authentication and accounting services to one or more client network-attached storage (NAS) devices. RADIUS servers authenticate users and return all configuration information necessary for the client to deliver service to the users.

Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server.

- The Access-Request packet contains the user name, encrypted password, NAS IP address, VPN ID, and port. The format of the request also provides information on the type of session that the user wants to initiate.
- The RADIUS server returns an Access-Accept response if it finds the user name and verifies the password. The response includes a list of attribute-value pairs that describe the parameters to be used for this session.

NSE-Broadband Aggregation Features

Platform: Cisco 7200 VXR using a Network Services Engine (NSE) and Cisco 7401ASR routers

The NSE-Broadband Aggregation Features utilizes the functionality of the Parallel eXpress Forwarding (PXF) processor complex and PXF feeder Application-Specific Integrated Circuit (ASIC) on the NSE-1 board use as concentrator for DSL access.

The following NSE-Broadband Aggregation Features are being introduced for PXF:

- 802.1Q
- Layer 2 Tunneling Protocol (L2TP)
- Per VC queuing for ATM
- PPP over ATM (PPPoA)
- PPP over Ethernet over 802.1Q (PPPoEo802.1Q)
- PPP over Ethernet over Ethernet (PPPoEoE)
- PPP over Ethernet/PPP over Ethernet over ATM (PPPoE/PPPoEoA)
- Routed bridge encapsulation (RBE)

802.1Q

VLANs can now be implemented using 802.1Q encapsulation.

For information on 802.1Q, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/8021q.htm.

Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol that supports tunnel and user authentication. It can be used for implementing access VPNs.

For information regarding L2TP, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.htm

For information about access VPN technologies—including L2TP—refer to:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/l2tun_ds.htm.

Per VC queuing for ATM

The per-virtual circuit queuing for ATM feature allows you to apply ATM functionality to an individual virtual circuit.

PPP over ATM (PPPoA)

PPPoA allows tunneling and termination of PPP sessions over ATM permanent-virtual-circuit (PVC) and switched-virtual-circuit (SVC) links.

For more information on PPPoA, refer to:

http://www.cisco.com/warp/public/794/pppoa_arch.html.

PPP over Ethernet over 802.1Q (PPPoEo802.1Q)

PPPoEo802.1Q allows tunneling and termination of Ethernet PPP sessions across VLAN links.

For information about PPPoEo802.1Q, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtppp_1q.htm

PPP over Ethernet over Ethernet (PPPoEoE)

PPPoEoE allows tunneling and termination of PPP sessions over Ethernet links and allows for Ethernet PPP connections over Ethernet links.

PPP over Ethernet/PPP over Ethernet over ATM (PPPoE/PPPoEoA)

PPPoE—also known as PPPoEoA—allows tunneling and termination of Point-to-Point Protocol (PPP) sessions over Ethernet links and allows for Ethernet PPP connections over ATM links. The PPPoE feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator.

For more information on PPPoE/PPPoEoA (supported on the Cisco 7200 as well as the Cisco 6400), refer to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120dc/120dc3/pppoe.htm

and

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtpppoe.htm.

For information on PPP, refer to:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ppp.htm

Routed bridge encapsulation (RBE)

Routed bridge encapsulation (RBE) allows bridged RFC 1483 frames to be routed. The router ignores bridge headers.

RBE with unnumbered DHCP scales DHCP address allocation. RBE and RBE with unnumbered DHCP are available for acceleration on the Cisco 7200 and 7400.

For information on configuring RBE, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcfppp.htm.

For information on DSL network architectures, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/gsol_dsl/dsl_arch/gdslarch.htm.

Per VRF AAA

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

Using the Per VRF AAA feature, Internet Service Providers (ISPs) can partition authentication, authorization, and accounting (AAA) services based on Virtual Route Forwarding (VRF). This permits the Virtual Home Gateway (VHG) to communicate directly with the customer RADIUS server associated with the customer VPN, without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer need to proxy AAA to provide their customers the flexibility demanded.

To support Per VRF AAA, AAA must be VRF aware. ISPs must define multiple instances of the same operational parameters—such as AAA server groups, method lists, system accounting, and protocol-specific parameters—and secure the parameters to the VRF partitions.

If an AAA configuration, such as a method list, is uniquely defined many times across the network access server (NAS), the specification of an AAA server that is based on IP addresses and port numbers may create an overlapping of private addresses between VRFs. Securing AAA method lists to a VRF can be accomplished from one or more of the following sources:

- Virtual Template—Used as a generic interface configuration.
- Service Provider AAA server—Used to associate a remote user with a specific VPN based on the domain name or Dialed Number Identification Service (DNIS). The server then provides the VPN-specific configuration for the virtual access interface, which includes the IP address and port number of the customer AAA server.
- Customer VPN AAA server—Used to authenticate the remote user and to provide user-specific configurations for the virtual access interface.

Note Global AAA accounting configurations and some AAA protocol-specific parameters cannot be logically grouped under the Virtual Template configuration.

AAA Server Configurations

To prevent possible overlapping of private addresses between VRFs, AAA servers must be defined in a single global pool that is to be used in the server groups. Servers can no longer be uniquely identified by IP addresses and port numbers.

Private servers (servers with private addresses within the default server group that contains all the servers) can be defined within the server group and remain hidden from other groups. The list of servers in server groups includes references to the hosts in the global configuration as well as the definitions of private servers.

Note If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.

All server operational parameters can be configured per host, per server group, or globally. Per-host configurations have precedence over per-server group configurations. Per-server group configurations have precedence over global configurations.

PPPoE over Gigabit Ethernet

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The PPPoE over Gigabit Ethernet feature enhances PPP over Ethernet (PPPoE) functionality by adding support for PPPoE and PPPoE over IEEE 802.1Q VLANs on Gigabit Ethernet interfaces. The PPPoE over Gigabit Ethernet feature is supported on Cisco 7200 series routers with Gigabit Ethernet line cards.

PPPoE Session Limit

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The PPPoE Session Limit feature enables you to limit the number of PPPoE sessions that can be created on a router or on an ATM PVC, PVC range, or VC class.

Before the introduction of this feature, there was no way to limit the number of PPPoE sessions that could be created on a router. Not having a limit was potentially a problem because it was possible that the router could create so many PPPoE sessions that it would run out of memory.

To prevent the router from using too much memory for virtual access, the PPPoE Session Limit feature introduces a new command and a modification to an existing command that enable you to specify the maximum number of PPPoE sessions that can be created. The new **pppoe limit max-sessions** command limits the number of PPPoE sessions that can be created on the router. The modified **pppoe max-sessions** command limits the number of PPPoE sessions that can be created on an ATM PVC, PVC range, VC class, or Ethernet subinterface.

Quality of Service Features for Parallel Express Forwarding (PXF)

Platform: Cisco 7200 VXR using a Network Services Engine (NSE) and Cisco 7401ASR routers

The Modular Quality of Service Command-Line Interface (Modular QoS CLI) and many of the associated class-based QoS features are now available on PXF.

The following class-based QoS features are being introduced for PXF:

- Traffic Policing —the **police** command in policy map class configuration mode.
- Class-Based Weighted Fair Queueing (CBWFQ) —the **bandwidth** and **fair-queue** commands in policy map class configuration mode.
- Low Latency Queueing (LLQ) —the **priority** command used in policy map class configuration mode.
- Class-Based Marking —the **set** command used in policy map class configuration mode. Class-Based Marking support is limited to 32 traffic classes per traffic policy, and the QoS group marking (**set qos-group**) is not supported.
- Class-Based Weighted Random Early Detection (CBWRED) and Differentiated Services-Compliant Weighted Random Early Detection (DiffServ-Compliant WRED)—the **random-detect** command used simultaneously with the **bandwidth** command in policy map class configuration mode.
- Flow-Based Weighted Random Early Detection—the **random-detect** command used simultaneously with the **bandwidth** command in policy map class configuration mode.

The Committed Access Rate (CAR) feature configured to use an access list with rate-limiting policies (the **access-list rate-limit** command in interface configuration mode) is also now available on PXF. If you wish to rate-limit traffic without using an ACL, use the Modular QoS CLI to configure the Traffic Policing feature.

Because of the addition of the Modular QoS CLI, traditional WRED (the **random-detect** command in interface configuration mode) and Fair Queueing (the **fair-queue** command in interface configuration mode) are no longer configurable. If you would like to configure WRED or Fair Queueing, you can use the Modular QoS CLI to configure Class-Based WRED or Class-Based Weighted Fair Queueing on a per-class rather than a per-interface basis.

The Modular QoS CLI on PXF does not currently support the following match criteria that are available on other Modular QoS CLI-supported platforms:

- Destination address
- Input Interface
- Internet Protocol (IP) values
- Multi Protocol Label Switching (MPLS) values
- Protocol
- Quality of Service (QoS) group values
- Source address

For additional information on the Modular QoS CLI, see the *Modular Quality of Service Command-Line Interface* document.

RADIUS Attribute Screening

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The RADIUS Attribute Screening feature allows users to configure a list of “accept” or “reject” RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.

If a NAS accepts and processes all RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers' authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list

RADIUS Attributes 52 and 53 for DSL

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The RADIUS Attribute 52 and Attribute 53 for the DSL feature introduces support for Attribute 52 (Acct-Input-Gigawords) and Attribute 53 (Acct-Output-Gigawords). Attribute 52 keeps track of the number of times the Acct-Input-Octets counter has rolled over the 32-bit integer throughout the course of the provided service; attribute 53 keeps track of the number of times the Acct-Output-Octets counter has rolled over the 32-bit integer throughout the delivery of service. Both attributes can be present only in Accounting-Request records where the Acct-Status-Type is set to “Stop” or “Interim-Update.” These attributes can be used to keep accurate track of bill for usage.

RADIUS Attribute 77 for DSL

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The RADIUS Attribute 77 for DSL feature introduces support for Attribute 77 (Connect-Info) to carry the textual name of the virtual circuit class associated with the given permanent virtual circuit (PVC). (Although attribute 77 does not carry the unspecified bit rate (UBR), the UBR can be inferred from the classname used if one UBR is set up on each class.) Attribute 77 is sent from the network access server (NAS) to the RADIUS server via Accounting-Request and Accounting-Response packets.

RADIUS-based Session/Idle Timer for L2TP LAC

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The RADIUS-based Session/Idle Timer for L2TP LAC feature enables the LAC to receive the session timer from RADIUS via Radius Attribute 27 and an idle timer within Radius Attribute 28 upon receiving a call directed via a specific L2TP tunnel to a certain Service Provider LNS. The LAC should disconnect the session based on these timers.

A local configuration possibility of the idle timer (session timer is already implemented) would be desirable. In case both options are configured at the same time (a local configuration below the selected virtual template and session/idle timer received via RADIUS), the values received via RADIUS must override the local configuration. All processing should happen via a Virtual Template mechanism. After the time of the idle or session timer has expired, the LAC should send out a PADT towards the PPPoE client and the LNSs to terminate the session.

Service Selection Gateway

Platforms: Cisco 7200 series 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 digital subscriber lines, cable modems, or wireless to allow simultaneous access to network services.

SSG works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

The SESM operates in two modes:

- RADIUS mode—This mode obtains subscriber and service information from a RADIUS server. SESM in RADIUS mode is similar to the SSD.
- DESS mode—The Directory-Enabled Service Selection (DESS) mode provides access to a Lightweight Directory Access Protocol (LDAP)-compliant directory for subscriber and service profile information. This mode also has enhanced functionality for SESM web applications and uses a role-based access control (RBAC) model to manage subscriber access.

If your deployment uses SESM in DESS mode, refer to these documents for additional information about DESS-mode topics:

- For information on configuring SESM, see the Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide.
- For information on creating and maintaining subscriber, service, and policy information in an LDAP directory, see the Cisco Distributed Administration Tool Guide.

Note Note The SESM and SSD functionality described in this document is available only with SSG.

SSG communicates with the authentication, authorization, and accounting (AAA) management network where RADIUS, Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of SSG works with SESM to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This functionality improves flexibility and convenience for subscribers, and enables service providers to bill subscribers for connect time and services used, rather than charging a flat rate.

When SSG is used with SESM, the user opens an HTML browser and accesses the URL of the SESM web server application. SESM forwards the user login information to SSG, which forwards the information either to the AAA server, for the SSD or SESM in RADIUS mode, or to the RADIUS-DESS Proxy (RDP) component of SESM, for SESM in DESS mode.

- If the user is not valid, the AAA server or RDP sends an Access-Reject message.
- If the user is valid, the AAA server or RDP sends an Access-Accept message with information specific to the user profile about which services the user is authorized to use. SSG logs the user in, creates a host object in memory, and sends the response to SESM.

Based on the contents of the Access-Accept response, SESM presents a menu of services that the user is authorized to use, and the user selects one or more of the services. SSG then creates an appropriate connection for the user and optionally starts RADIUS accounting for the connection.

Note that when a non-PPP user, such as in a bridged-networking environment, disconnects from a service without logging out, the connection remains open and the user can reaccess the service without going through the login procedure, since no direct connection (PPP) exists between the subscribers and SSG. To prevent non-PPP users from being logged in to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout RADIUS attributes.

SSG supports the features and functionality described in the following sections:

- Web-Based Interface
- RADIUS Authentication and Accounting
- LDAP Directory
- Multiple Traffic-Type Support
- Packet Filtering
- Service Access Order
- Next Hop Gateway
- DNS Redirection
- Fault Tolerance for DNS
- Session-Timeout and Idle-Timeout RADIUS Attributes
- Concurrent or Sequential Service Access Mode
- Enhanced High System Availability
- Web Selection of L2TP Service Type
- Local Forwarding

- SSG Single Host Logon
- SSG User-Profile Caching
- IPCP Subnet

Web-Based Interface

SSG with Web Selection works with the Cisco SESM. The SESM is a specialized web server that allows users to log in to and disconnect from multiple pass-through and proxy services through a standard web browser.

After the user opens a web browser, SSG allows access to a single IP address or subnet, referred to as the default network. This is typically the IP address of SESM. The SESM prompts the user for a username and password. After the user is authenticated, SESM presents a list of available services.

The SESM provides all the functionality of its predecessor product, the SSD. SESM also introduces the following functionality:

- Policy-based service subscription and self-care. Service providers can grant users certain privileges, including these:
  - Subscribing to or unsubscribing from network services that the users are authorized to access
  - Creating subaccounts and subscribing them to services
  - Changing account details, such as password and billing address
- LDAP-compliant directory storage of service and subscriber information. LDAP provides the following:
  - Implementation of self-care by enabling dynamic user updates of subscriber and service information
  - Management of users as groups—service providers can simply add services to user group profiles instead of individual user profiles

RADIUS Authentication and Accounting

SSG is designed to work with RADIUS-based AAA servers that accept vendor-specific attributes (VSAs).

LDAP Directory

SSG using SESM in DESS mode can use an LDAP directory as the data repository for service, subscriber, and policy information.

Multiple Traffic-Type Support

SSG supports the following types of service:

- Pass-Through service

  SSG can forward traffic through any interface by means of normal routing or a next-hop table. Because Network Address Translation (NAT) is not performed for this type of traffic, overhead is reduced. Pass-through service is ideal for standard Internet access.

- Proxy service

  When a subscriber requests access to a proxy service, SSG proxies the Access-Request packet to the remote AAA server. Upon receiving an Access-Accept packet from the remote RADIUS server, the SSG logs the subscriber in. To the remote AAA server, SSG appears as a client.

  During remote authentication, if the RADIUS server assigns an IP address to the subscriber, the SSG performs NAT between the assigned IP address and the real IP address of the subscriber. If the remote RADIUS server does not assign an IP address, NAT is not performed.

When a user selects a proxy service, there is another prompt for username and password. After authentication, the service is accessible until the user logs out from the service, logs out from SESM, or times out.

- Transparent Pass-Through

  When enabled, transparent pass-through allows unauthenticated subscriber traffic to be routed through SSG in either direction. Filters can be specified to control transparent pass-through traffic. Some of the applications are as follow:

  - Making the SSG easy to integrate into an existing network by not requiring users who have authenticated with network access servers (NAS) to authenticate with SSG
  - Allowing management traffic (such as TACACS+, RADIUS, and SNMP) from NASes connected to the host network to pass through to the service provider network
  - Allowing visitors or guests to access certain parts of the network

- PPP Termination Aggregation (PTA) and PTA Multi-Domain (PTA-MD)

  PPP Termination Aggregation (PTA) can be used only by PPP-type users. AAA is performed exactly as in the proxy service type. A subscriber logs in to a service by using a PPP dialer application with a username of the form ‘user@service’. SSG recognizes ‘@service’ as a service profile and loads the service profile from the local configuration or a AAA server. The SSG forwards the AAA request to the remote RADIUS server as specified by the RADIUS-Server attribute of the service profile. An address is assigned to the subscriber through RADIUS attribute 8 or Cisco-AVpair “ip:addr-pool.” NAT is not performed, and all user traffic is aggregated to the remote network. With PTA, users can access only one service. Users do not have access to the default network or the SESM.

  Whereas PTA terminates the PPP session into a single routing domain, PTA-MD terminates the PPP sessions into multiple IP routing domains, thus supporting a wholesale Virtual Private Network (VPN) model in which each domain is isolated from the other by an ATM core and has the capability to support overlapping IP addresses.

Packet Filtering

SSG uses Cisco IOS access control lists (ACLs) to prevent users, services, and pass-through traffic from accessing specific IP addresses and ports.

- Services

  When an ACL attribute is added to a service profile, all users of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

- Users

  When an ACL attribute is added to a user profile, it applies globally to all traffic for the user.

- Transparent Pass-Through

  Upstream and downstream attributes, including the Upstream Access Control List and Downstream Access Control List attributes, can be added to a special pseudo-service profile that can be downloaded to SSG from a RADIUS server. Additionally, locally configured ACLs can be used. After the ACLs have been defined, they are applied to all traffic passed by the transparent pass-through feature.

Service Access Order

When users are accessing multiple services, SSG must determine the services for which the packets are destined. To do this, SSG uses an algorithm to create a service access order list that is stored in the user's host object. This list contains services that are currently open and the order in which they are to be searched. The algorithm that creates this list orders the open services based on the closest matching network address.

Next Hop Gateway

The Next Hop Gateway attribute is used to specify the next hop key for a service. Each SSG uses its own next hop gateway table, which associates this key with an actual IP address.

Note that this attribute overrides the IP routing table for packets destined to a service.

DNS Redirection

When the SSG receives a Domain Name Server (DNS) request, it performs domain name matching by using the Domain Name attribute from the service profiles of the currently logged-in services.

If a match is found, the request is redirected to the DNS server for the matched service.

If a match is not found and the user is logged in to a service that has Internet connectivity, the request is redirected to the first service in the user's service access order list that has Internet connectivity. Internet connectivity is defined as a service containing a Service Route attribute of 0.0.0.0/0.

If a match is not found and the user is not logged in to a service that has Internet connectivity, the request is forwarded to the DNS server defined in the client's TCP/IP stack.

Fault Tolerance for DNS

SSG can be configured to work with a single DNS server or with two servers in a fault-tolerant configuration. By means of an internal algorithm, DNS requests are switched to the secondary server if the primary server fails to respond with a DNS reply within a certain time limit.

Session-Timeout and Idle-Timeout RADIUS Attributes

In a dial-up networking or bridged (non-PPP) network environment, a user can disconnect from the NAS and release the IP address without logging out from SSG. If this happens, SSG continues to allow traffic to pass from that IP address, and this can be a problem if the IP address is obtained by another user.

SSG provides two mechanisms to prevent this problem from occurring:

- Idle-Timeout attribute—Specifies the maximum length of time for which a session or connection can remain idle before it is disconnected
- Session-Timeout attribute—Specifies the maximum length of time for which a host or connection object can remain continuously active

  The Session-Timeout and Idle-Timeout attributes can be used in either a user or service profile. In a user profile, the attribute applies to the user's session. In a service profile, the attribute applies individually to each service connection.

Concurrent or Sequential Service Access Mode

SSG services can be configured for concurrent or sequential access. Concurrent access allows users to log in to this service while simultaneously connected to other services. Sequential access requires that the user log out of all other services before accessing a service configured for sequential access.

Concurrent access is recommended for most services. Sequential access is ideal for services that require security, such as corporate intranet access, or for those that might have a possibility of overlapping address space.

Enhanced High System Availability

SSG supports enhanced high system availability (EHSA) redundancy. You can configure this chassis redundancy at the slot level of the router for adjacent slot or subslot pairs. For example, if you have SSGs installed in slots 1 and 2, you can set a preferred device between the two. To ensure that configuration is consistent between redundant SSGs, you can configure automatic synchronization between the two SSGs. You can also manually force the primary and secondary devices in a redundant pair to switch roles.

Web Selection of L2TP Service Type

SSG supports Layer 2 Tunnel Protocol (L2TP). When a subscriber selects a service through SESM, the router serves as an L2TP access concentrator (LAC) and sends the PPP session through the service-specific L2TP tunnel. If the tunnel does not already exist, the LAC creates the proper tunnel to the L2TP network server (LNS).

Local Forwarding

SSG can be enabled to forward packets locally between directly connected subscribers.

SSG Single Host Logon

To log in to a service through SESM, a subscriber has to log in only twice: once for the PPP session and once for the service.

SSG User-Profile Caching

SSG user-profile caching allows SSG to cache the user profiles of non-PPP users. User profiles of PPP and RADIUS proxy users are always cached by SSG by default. In situations in which the user profile is not available from other sources, SSG user-profile caching makes the user profile available for RADIUS status queries, providing support for single-sign-on functionality and for failover from one SESM to another.

IPCP Subnet

IP Control Protocol (IPCP) subnet support allows SSG to populate a host DHCP server with a pool of IP addresses. The PPP session from the host is terminated at the SSG. During IPCP negotiations, SSG uses the IPCP subnet mask negotiation option to send a range of IP addresses to the customer premises equipment (CPE) device at the host network. The CPE assigns IP addresses to the users in the SSG domain, thus avoiding the need for NAT at the CPE device.

To enable IPCP subnet mask, the Framed-IP-Netmask attribute (standard RADIUS attribute 9) and Framed-IP-Address attribute (standard RADIUS attribute 8) must be included in the user profile. The Framed-IP-Netmask value is passed during IPCP negotiation as an option.

Service Selection Gateway Accounting Update Interval Per Service

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The Service Selection Gateway (SSG) Accounting Update Interval Per Service feature enhances SSG accounting by allowing users to configure an accounting interval for a particular service. Without the SSG Accounting Update Interval Per Service feature, all accounting information is sent simultaneously, and accounting information for a particular SSG service cannot be sent at a separate, independent interval.

SSG Accounting sends information such as billing, auditing, and reporting, so the SSG Accounting feature allows for more granular accounting interval options for all of these functions.

Session Limit Per VRF

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The Session Limit Per VPN Routing/Forwarding instance (VRF) feature enables session limits to be applied on all VPDN groups associated with a common VPDN virtual template. Before the implementation of Session Limit Per VRF, a single default template carrying the configuration values of a subset of VPDN group commands were associated with all VPDN groups configured on the router. Session Limit Per VRF enables you to create, define and name multiple VPDN templates. You can then associate a specific template with a VPDN group. A session limit can be configured at the VPDN template level to specify a combined session limit for all VPDN groups associated with the configured VPDN template.

SSG Autodomain

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

When you configure SSG Autodomain, users can automatically connect to a service based on either Access Point Name (APN) or the domain part of the structured username specified in an Access-Request. When SSG Autodomain is configured, user authentication is not performed at the Network Access Server (NAS) AAA, but instead at the service (for example, at a AAA server within a corporate network).

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.

The SSG with Web Selection works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

The SSG acts as a central control point for Layer 2 and Layer 3 services. This can include services available through ATM virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

The SSG communicates with the authentication, authorization, and accounting (AAA) management network where Remote Access Dial-In User Service (RADIUS), Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside. The SSG also communicates with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of the SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This improves flexibility and convenience for subscribers, and enables service providers to bill subscribers based on connect time and services used, rather than charging a flat rate.

The user opens an HTML browser and accesses the URL of the SESM or SSD web server application. SESM or SSD forwards user login information to the SSG, which forwards the information to the AAA server.

- If the user is not valid, the AAA server sends an Access-Reject message.
- If the user is valid, the AAA server sends an Access-Accept message with information specific to the user profile about which services the user is authorized to use. The SSG logs the user in, creates a host object in memory, and sends the response to SESM or SSD.

Based on the contents of the Access-Accept response, SESM or SSD presents a dashboard menu of services that the user is authorized to use, and the user selects one or more of the services. The SSG then creates an appropriate connection for the user and starts RADIUS accounting for the connection.

Note that when a non-Point-to-Point Protocol (non-PPP) user, such as in a bridged-networking environment, disconnects from a service without logging off, the connection remains open and the user can reaccess the service without going through the login procedure, since no direct connection (PPP) exists between the subscribers and the SSG. To prevent non-PPP users from being logged in to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout RADIUS attributes.

Access Point Names

An APN identifies a Packet Data Network (PDN) that is configured on and accessible from a Gateway GPRS Support Node (GGSN). An access point is identified by its APN name. The Global System for Mobile Communication (GSM) standard 03.03 defines the following two parts of an APN:

- APN Network Identifier
- APN Operator Identifier

The APN Network Identifier is mandatory. The name of an access point in the form of an APN Network Identifier must correspond to the fully-qualified name in the Domain Name System (DNS) configuration for that network, and it must also match the name specified for the access point in the GGSN configuration. The GGSN also uniquely identifies an APN by an index number. The APN Operator Identifier is an optional name that consists of the fully-qualified DNS name, with the ending ".gprs."

The access points that are supported by the GGSN are preconfigured on the GGSN. When a user requests a connection in the GPRS network, the APN is included in the Create Packet Data Protocol (PDP) Request message. The Create PDP Request message is a GPRS Tunneling Protocol (GTP) message that establishes a connection between the Serving GPRS Support Node (SGSN) and the GGSN.

An APN has several attributes associated with its configuration that define how users can access the network at that entry point. For more information about configuring APNs, see the *APN Manager Application Programming Guide*.

SSG Autodomain

When using SSG Autodomain, you can automatically log in a user to a service based on either the APN or a structured username. Users can bypass the Service Selection Dashboard (SSD) and access a service, such as a corporate intranet.

SSG Autodomain makes it possible to log in a user to either Layer 2 Tunnel Protocol (L2TP) or proxy services. The username and password used to log in a user with Autodomain is the username and password provided by the user when logging into the General Packet Radio Service (GPRS) network. This password can be a dynamically generated password.

SSG Autodomain does not require SSG Vendor Specific Attributes (VSAs) when using a domain name as a means to determine which service to log in the user.

Autodomain uses a heuristic to determine the service into which the user is logged. When using Autodomain, the host object is not activated until successfully authenticated with the service. If the auto-service connection fails for any reason, the user login is rejected and an Access-Reject is returned to the Gateway GPRS Support Node (GGSN).

Autodomain service first checks for an APN (Called-Station-ID) and then for a structured username.

If Autodomain is enabled and the received Access-Request specifies an APN, then this APN is used for Autodomain selection unless it is a member of the APN Autodomain exclusion list. If an Autodomain is not selected based on APN, then the structured username is used. If a structured username is not supplied, or the supplied structured username is a member of the domain name exclusion list, then no Autodomain is selected and normal SSG user login proceeds. You can override these Autodomain selection defaults by configuring the **ssg auto-domain select** command. You can define the APN Autodomain exclusion list and the domain name exclusion list with the **ssg auto-domain exclude** command.

When Autodomain is enabled, an Autodomain profile is downloaded from the local AAA server. This profile is specified as an outbound service and the password is the globally configured service password.

You can configure SSG Autodomain in basic or extended mode. In basic mode, the Autodomain profile downloaded from the AAA server is a service profile. In extended Autodomain mode, the profile downloaded from the AAA server is a “virtual user” profile which contains one auto-service to an authenticated service such as a proxy or a tunnel. The “virtual user” profile defines the Autodomain service. Connection to this auto-service occurs as it does for basic Autodomain, where the host object is not activated until the user is authenticated at the proxy or tunnel service. The presence of the SSD in extended Autodomain mode enables the user to access any other service in the specified user profile. If the “virtual user” profile does not have exactly one auto-service or the auto-service is not authenticated, the Autodomain login is rejected.

The Autodomain service profile can be a proxy or tunnel service. If the downloaded Autodomain service profile is a proxy service, the access-request is proxied to the appropriate domain AAA server. If the downloaded Autodomain service profile is a tunnel service, a PPP session is regenerated into an L2TP tunnel for the selected service. If no SSG-specific attributes are returned indicating the type of service required, the SSG uses a default set of attributes to regenerate the PPP session for the specified service.

SSG Autodomain attempts to log the user onto the remote service using the username and password specified in the original Access-Request. For structured user names, only the “user” part of the name is used unless the “X” attribute is present in the service profile. For VPDN-only type services (where no SSG attributes are present), it is not possible to specify use of the full structured username.

If you configure basic SSG Autodomain with a nonauthenticated service type such as passthrough, SSG rejects the login request because Autodomain bypasses user authentication at the local AAA server and requires that authentication be performed elsewhere.

SSG Autologoff

Platform: Cisco 7200 series routers and Cisco 7401ASR routers

The SSG Autologoff feature enables the Cisco Service Selection Gateway (SSG) to verify connectivity with each host or user at configured intervals. If SSG detects that the connection has terminated, SSG will automatically initiate the logoff for that host or user.

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.

The SSG with Web Selection works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco SESM. Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

The SSG acts as a central control point for Layer 2 and Layer 3 services. This can include services available through ATM virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

The SSG communicates with the authentication, authorization, and accounting (AAA) management network where RADIUS, Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of the SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This improves flexibility and convenience for subscribers, and enables service providers to bill subscribers based on connect time and services used, rather than charging a flat rate.

For more information about SSG, refer to the *Service Selection Gateway* feature module in the "New Features in Release 12.2(4)B" area of Cisco.com.

SSG Autologoff

When SSG autologoff is configured, the SSG will check the status of the connection with each host at configured intervals. If SSG finds that a host has been disconnected, SSG will automatically initiate the logoff of that host. SSG has two methods of checking the connectivity of hosts: ARP ping and ICMP ping.

ARP Ping

The Address Resolution Protocol (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 some configured interval. If a table entry is not found, SSG initiates autologoff for the host.

Note Note ARP ping should be used only in deployment scenarios where all hosts are directly connected.

Cisco recommends using ARP ping when possible because ARP entries are refreshed whenever there is network activity. In addition, ARP request packets are smaller than ICMP ping packets.

ICMP Ping

The Internet Control Message Protocol (ICMP) is a network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. An ICMP ping is the echo message and echo-reply message used to check for connectivity between devices.

When SSG autologoff is configured to use the ICMP ping mechanism, SSG invokes the callback function for successful pings or timeouts. In the case of timeout or ping error, the callback function checks the number of retries remaining and initiates ping again. If all the retries all used up, then SSG initiates logoff for the host. If the ping is successful, then SSG assumes the host has connectivity and no more attempts are made until the next ping interval.

ICMP ping will work in all types of deployment scenarios and supports overlapping IP users.

SSG AutoLogon Using Proxy Radius

Platforms: Cisco 7200 series 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.

The SSG with Web Selection works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

The SSG acts as a central control point for Layer 2 and Layer 3 services. This can include services available through ATM virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

The SSG communicates with the authentication, authorization, and accounting (AAA) management network where Remote Access Dial-In User Service (RADIUS), Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside. The SSG also communicates with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of the SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This improves flexibility and convenience for subscribers, and enables service providers to bill subscribers based on connect time and services used, rather than charging a flat rate.

The user opens an HTML browser and accesses the URL of the SESM or SSD web server application. SESM or SSD forwards user login information to the SSG, which forwards the information to the AAA server.

- If the user is not valid, the AAA server sends an Access-Reject message.
- If the user is valid, the AAA server sends an Access-Accept message with information specific to the user profile about which services the user is authorized to use. The SSG logs the user in, creates a host object in memory, and sends the response to SESM or SSD.

Based on the contents of the Access-Accept response, SESM or SSD presents a dashboard menu of services that the user is authorized to use, and the user selects one or more of the services. The SSG then creates an appropriate connection for the user and starts RADIUS accounting for the connection.

Note that when a non-Point-to-Point Protocol (non-PPP) user, such as in a bridged-networking environment, disconnects from a service without logging off, the connection remains open and the user can reaccess the service without going through the login procedure. This is because no direct connection (PPP) exists between the subscribers and the SSG. To prevent non-PPP users from being logged in to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout RADIUS attributes.

SSG AutoLogon Using Proxy Radius

Before the introduction of the SSG AutoLogon Using Proxy Radius feature, the SSG effectively acted as a RADIUS proxy for the Service Selection Dashboard (SSD). In this mode, when SSD needs to authenticate a user, it forwards an Access-Request to the SSG. The Access-Request uses the IP address and port number configured for RADIUS authentication on the SSG as well as the configured shared secret between the SSG and the SSD. When SSG receives a request from the SSD to authenticate a user, the SSG uses AAA to construct an Access-Request and send it to the AAA server. When SSG receives the Access-Accept, it processes it and forwards it to the SSD. In this implementation, SSG is far from acting as a generic RADIUS proxy and standard RADIUS protocol must be extended by the use of Vender Service Attributes (VSAs) to provide a control plane between the SSG and SSD. Without the VSA in the Access-Request, SSG did not function as a RADIUS proxy.

The SSG AutoLogon Using Proxy Radius feature enables the SSG to act as a RADIUS proxy for non-SSD clients whose Access-Requests do not contain VSAs. Non-SSD Access-Requests must originate from configured, trusted, downstream Network Access Server (NAS) IP addresses which share a RADIUS secret key with the SSG. This shared secret key is a different secret than the one shared between SSG and the SSD. You must configure the IP addresses for each router for which SSG is acting as a RADIUS proxy. Packets received from unrecognized sources are discarded.

When the SSG receives a valid Access-Request, it forwards it to the RADIUS server. The SSG performs a full, transparent proxy of the Access-Request to the RADIUS server, faithfully reproducing the attributes provided originally by the RADIUS client. If the Access-Request is successful, the AAA server responds with an Access-Accept and an SSG host object is created.

RADIUS Authentication and Authorization

A RADIUS client can be configured to use a RADIUS AAA server for user authentication. In a Cisco RADIUS client, the RADIUS server can be configured as a global AAA server for General Packet Radio System (GPRS) or individual servers per Access Point Name (APN). The RADIUS client sends an Access-Request to the AAA server to authenticate a user. The Access-Request contains attributes depending on whether the router is using CHAP or PAP.

After a successful authentication, the RADIUS AAA server responds to the Access-Request by sending an Access-Accept containing a RADIUS attribute.

The RADIUS attributes are part of the user database held on the RADIUS AAA server and can be modified or extended as required. You can configure the AAA server to select a user profile based on Called-Station-ID (Access Point Name [APN]) or Calling-Station-ID (MSISDN header field type for wireless clients using the Wireless Application Protocol [WAP]).

If the AAA is configured to select profiles based on Called-Station-ID, all users connecting to the same APN are given the same profile even though they have different assigned IP addresses.

The supplied username does not have to be unique for WAP users on the RADIUS client. These users are granted anonymous access and all have the same user name and password.

AAA authorization involves extracting all of the parameters needed to create the Packet Data Protocol (PDP) context. The authorization extracts the Framed-IP-Address and the Framed-IP-Netmask.

SSG Vendor-Specific Attributes

The SSG uses vendor-specific RADIUS attributes. If using the SSG with Cisco User Control Point (UCP) software, specify settings that allow processing of the SSG attributes while configuring the CiscoSecure Access Control Server (ACS) component. If using another AAA server, you must customize that server RADIUS dictionary to incorporate the SSG vendor-specific attributes.

SSG Open Garden

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The SSG Open Garden feature enables you to use the Cisco Service Selection Gateway (SSG) to implement open gardens. An open garden is a collection of domains that a subscriber can access without providing authentication information.

SSG

SSG is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as digital subscriber lines, cable modems, or wireless to allow simultaneous access to network services.

SSG works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

SSG acts as a central control point for Layer 2 and Layer 3 services. These can include services available through ATM virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

SSG communicates with the authentication, authorization, and accounting (AAA) management network where RADIUS, Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This functionality improves flexibility and convenience for subscribers and enables service providers to bill subscribers for connect time and services used, rather than charging a flat rate.

For more information about SSG, refer to the *Service Selection Gateway* feature module in the "New SSG Features in Release 12.2(4)B" area of Cisco.com.

Open Gardens

An open garden is a collection of websites or networks that subscribers can access as long as they have physical access to the network. Subscribers do not have to provide authentication information before accessing the websites in an open garden. In contrast, a walled garden refers to a collection of websites or networks that subscribers can access after providing minimal authentication information.

When SSG receives a packet destined for an open garden, SSG simply forwards the packet to the open garden. SSG determines whether a packet is headed for the open garden by comparing the packet IP prefix with the IP addresses for the open garden in the routing table.

If SSG receives a packet that is not destined for the open garden, SSG checks the source IP address of the packet to see if the subscriber is authenticated. If SSG recognizes the IP address, then the subscriber is authenticated and SSG forwards the packet. If the subscriber is not authenticated and the packet is not a Domain Name Server (DNS) packet, then SSG drops the packet.

SSG handles open gardens as services that have associated domain names and DNS addresses. As many as 100 domains can be associated with an open garden. When SSG receives a DNS request for one of the open garden domain names, SSG forwards the request to the open garden DNS server, where the domain name is resolved.

While most SSG services must be bound to an interface or next hop, it is not necessary to bind open garden services that are directly connected to the SSG router. Service binding is mandatory, however, for open garden services that are routed through a next hop.

SSG Port-Bundle Host Key

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The SSG Port-Bundle Host Key feature enhances communication and functionality between the Service Selection Gateway (SSG) and the Cisco Subscriber Edge Services Manager (SESM) by introducing a mechanism that uses the host source IP address and source port to identify and monitor subscribers.

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 digital subscriber lines, cable modems, or wireless to allow simultaneous access to network services.

SSG works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco SESM. Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

SSG acts as a central control point for Layer 2 and Layer 3 services. These can include services available through ATM virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

SSG communicates with the AAA management network where RADIUS, Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This functionality improves flexibility and convenience for subscribers and enables service providers to bill subscribers for connect time and services used, rather than charging a flat rate.

For more information about SSG, refer to the *Service Selection Gateway* feature module in the "New SSG Features in Release 12.2(4)B" area of Cisco.com.

Host Key Mechanism

Note All references to SESM also apply to SSD unless a clear distinction is made.

With the SSG Port-Bundle Host Key feature, SSG performs port-address translation (PAT) and network-address translation (NAT) on the HTTP traffic between the subscriber and the SESM server. When a subscriber sends an HTTP packet to the SESM server, SSG creates a port map that changes the source IP address to a configured SSG source IP address and changes the source TCP port to a port allocated by SSG. SSG assigns a bundle of ports to each subscriber because one subscriber can have several simultaneous TCP sessions when accessing a web page. The assigned host key, or combination

of port bundle and SSG source IP address, uniquely identifies each subscriber. The host key is carried in RADIUS packets sent between the SESM server and SSG in the Subscriber IP vendor-specific attribute (VSA).

For each TCP session between a subscriber and the SESM server, SSG uses one port from the port bundle as the port map. Port mappings are flagged as eligible for reuse on the basis of inactivity timers, but are not explicitly removed once assigned. The number of port bundles is limited, but you can assign multiple SSG source IP addresses to accommodate more subscribers.

SSG assigns the base port of the port bundle to a port map only if SSG has no state information for the subscriber or if the state of the subscriber has changed. When the SESM server sees the base port of a port bundle in the host key, SESM queries SSG for new subscriber state information.

Local Forwarding

When the SSG Port-Bundle Host Key feature is not configured, SSG local forwarding enables SSG to forward packets locally between any directly connected subscribers. When the SSG Port-Bundle Host Key feature is configured, local forwarding only works for directly connected subscribers that are connected to at least one common service. The hosts need to be connected to a common service because if the destination host has an overlapping IP address, then SSG will not know to which of the overlapping hosts to forward the traffic. In order for SSG to forward packets from one SSG host to another SSG host that has an overlapping IP address, then the overlapping host cannot share any common services with the other overlapping hosts.

SSG Prepaid Billing

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The SSG Prepaid feature expands Service Selection Gateway (SSG) accounting features to allow service providers to offer prepaid billing for their services.

SSG

SSG is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as digital subscriber lines, cable modems, or wireless to allow simultaneous access to network services.

SSG works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

SSG acts as a central control point for Layer 2 and Layer 3 services. These can include services available through ATM virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

SSG communicates with the authentication, authorization, and accounting (AAA) management network where RADIUS, Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This functionality improves flexibility and convenience for subscribers and enables service providers to bill subscribers for connect time and services used, rather than charging a flat rate.

For more information about SSG, refer to the *Service Selection Gateway* feature module in the "New SSG Features in Release 12.2(4)B" area of Cisco.com.

How SSG Prepaid Works

The SSG Prepaid feature allows SSG to determine whether to connect a subscriber to a service and for how long, based on how much credit a subscriber has. The credit, also called quota, is measured in either seconds for time or bytes for volume.

To obtain the quota for a connection, SSG submits an authorization request to the 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 provides SSG with more quota if it is available; if the quota has run out, SSG logs the user off.

The following sections describe in more detail how authorization and reauthorization work:

- Service Authorization
- Service Reauthorization

Service Authorization

SSG differentiates prepaid services from postpaid services by the presence of a vendor specific attribute (VSA) called the Service Authorization VSA in the service profile. The presence of this attribute in the service profile means that SSG needs to perform authorization to get the quota values for the connection. Once a prepaid service has been identified, SSG generates an Access-Request called a Service Authorization Request.

In a mobile wireless scenario, where SSG is acting as a radius proxy to the gateway GPRS support node (GGSN), the calling-station ID of the user is sent in the authorization request to the AAA server. In a non-RADIUS proxy environment where the access technology might not provide an MSISDN, SSG copies the value from the User-Name attribute into the Calling-Station-ID attribute field in the authorization request. The AAA server uses the Calling-Station-ID attribute in the Access-Request to perform authorization and return the quota parameters for that connection.

If a non-zero quota is returned, SSG creates a connection to the service with the initial quota value. The units for the quotas will be seconds for time and bytes for volume. A value of zero in a quota means the user has insufficient credit and is not authorized to use that service and the connection is not made. If the Quota attribute is not present in the authorization response, SSG will treat the connection as postpaid. However, if SSG receives an access reject or a quota of zero, SSG will not allow any further connection to that service.

Service Reauthorization

During the connection, if the quota is based on volume, SSG decrements the available quota until it runs out. If the quota is based on time, the connection is allowed to proceed for the quota duration. When the quota reaches zero, SSG issues a Service Reauthorization Request to the billing server. The Service Reauthorization Request includes a new SSG VSA called Quota Used.

If service reauthorization is unsuccessful, the billing server will respond to the Service Reauthorization Request with an Access-Accept containing a quota of zero. SSG will terminate the connection to the service at this point. If service reauthorization is successful, the billing server will return more quota to SSG and the connection will be allowed to continue.

SSG TCP Redirect for Services

Platforms: Cisco 7200 series 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.

The SSG with Web Selection works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

The SSG acts as a central control point for Layer 2 and Layer 3 services. This can include services available through Asynchronous Transfer Mode (ATM) virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

The SSG communicates with the authentication, authorization, and accounting (AAA) management network where Remote Access Dial-In User Service (RADIUS), Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of the SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This improves flexibility and convenience for subscribers, and enables service providers to bill subscribers based on connect time and services used, rather than charging a flat rate.

For more information about SSG, refer to the *Service Selection Gateway* feature module. For more information about SESM, refer to the Cisco Subscriber Edge Services Manager documentation.

TCP Redirect for Services

The SSG TCP Redirect for Services feature redirects certain packets, which would otherwise be dropped, to captive portals that can handle the packets in a suitable manner. For example, packets sent upstream by unauthorized users are forwarded to a captive portal that can redirect the users to a logon page. Similarly, if users try to access a service to which they have not logged on, the packets are redirected to a captive portal that can provide a service logon screen.

The captive portal can be any server that is programmed to respond to the redirected packets. If the Cisco Subscriber Edge Services Manager (SESM) is used as a captive portal, unauthenticated subscribers can be sent automatically to the SESM logon page when they start a browser session. In SESM Release 3.1(3), captive portal applications can also redirect to service logon pages, advertising pages, and message pages. The SESM captive portal application can also capture a URL in a subscriber's request and redirect the browser to the originally requested URL after successful authentication. Redirected packets are always sent to a captive portal group that consists of one or more servers. SSG selects one server from the group in a round robin fashion to receive the redirected packets.

Virtual Template Limit Expansion to 200

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

The Virtual Template Limit Expansion to 200 featuretts increases the maximum number of virtual template interfaces from 25 to 200.

See the *Per VRF AAA* feature module for more details.

VLAN Range

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

Using the VLAN Range feature, you can group VLAN subinterfaces together so that any command entered in a group applies to every subinterface within the group. This simplifies configurations and reduces command parsing.

VPDN Group Session Limiting

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

Before the introduction of the VPDN Group Session Limiting feature, you could only globally limit the number of VPDN sessions on a router with limits applied equally to all VPDN groups. Using the VPDN Group session limiting feature, you can limit the number of VPDN sessions allowed per VPDN group. This feature is implemented with the introduction of the **session-limit** *number* command in VPDN configuration mode. VPDN group session limiting is applied after the global VPDN session limiting (which is configured via the **vpdn session-limit** *session* command in configuration mode) is enforced.

VRF in Server Group

Platforms: Cisco 7200 series routers and Cisco 7401ASR routers

Before the introduction of VRF in the Server Group feature, per VRF AAA configurations did not allow dial users to utilize AAA servers in different VRFs. The dial user VRF was referred to whenever AAA requests were sent to the servers. This simplifies the configuration but limits users to utilizing AAA servers in the same routing domains.

With the introduction of VRF in Server Group feature, AAA servers have their own configurable per server-group VRF references. See the *Per VRF AAA* feature module for more details.

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 23.

Table 23 Deprecated and Replacement MIBs

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

Important Notes

SNMP Version 1 BGP4-MIB Limitations

You may notice incorrect BGP trap OID output when using the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends out BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). The problem is not due to any error with Cisco IOS software. This problem occurs because the BGP4-MIB does not follow RFC 1908 rules regarding version 1 and version 2 trap compliance. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

Configuring MD5 Authentication for BGP Peering Sessions

This section provides general information about deploying MD5 authentication for a BGP session. You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection. If authentication is invoked and a segment fails authentication, then an error message will be displayed in the console.

Old Behavior

In previous versions of Cisco IOS software, configuring MD5 authentication for a BGP peering session was generally considered to be difficult because the initial configuration and any subsequent MD5 configuration changes required the BGP neighbor to be reset.

New Behavior

This behavior has been changed in current versions of Cisco IOS software. CSCdx23494 (integrated in Cisco IOS release 12.2[15]B) introduced a change to MD5 authentication for BGP peering sessions. The BGP peering session does not need to be reset to maintain or establish the peering session for initial configuration or after the MD5 configuration has been changed. However, the configuration must be completed on both the local and remote BGP peer before the BGP hold timer expires. If the hold down timer expires before the MD5 configuration has been completed on both BGP peers, the BGP session will time out.

The following example enables the authentication feature between this router and the BGP neighbor at 10.108.1.1. The password that must also be configured for the neighbor is *bla4u00=2nkq*. The remote peer must be configured before the holddown timer expires.

```
router bgp 109
 neighbor 10.108.1.1 password bla4u00=2nkq
```

When the password has been configured, the MD5 key is applied to the tcp session immediately. If one peer is configured before the other, the TCP segments will be discarded on both the local and remote peers due to an authentication failure. The peer that is configured with the password will print an error message in the console similar to the following:

```
00:03:07: %TCP-6-BADAUTH: No MD5 digest from 10.0.0.2(179) to 10.0.0.1(11000)
```

The time period in which the password must changed is typically the life time of a stale BGP session. When the password or MD5 key is configured, incoming TCP segments will only be accepted if the key is known. If the key is unknown on both the remote and local peer, the TCP segments will be dropped, and the BGP session will time out when the holddown timer expires.

If the BGP session has been preconfigured with a hold time of 0 seconds, no keepalive messages will be sent. The BGP session will stay up until one of the peers, on either side, tries to transmit a message (For example, a prefix update).

Note Configuring a new timer value for the holddown timer will only take effect after the session has been reset. So, it is not possible to change the configuration of the holddown timer to avoid resetting the BGP session.

Upgrading from Cisco IOS Release 12.2(2)B to Cisco IOS Release 12.2(4)B

If you have a Cisco 6400 series router, or Cisco 7000 family routers with Cisco 6400 series routers within the same network running Cisco IOS Release 12.2(2)B, and you are upgrading to Cisco IOS Release 12.2(4)B, please note the configuration differences detailed in the table below.

Table 24 Differences Between Clsco IOS Release 12.2(2)B and Cisco IOS Release 12.2(4)B

Cisco IOS Release 12.2(2)B	Cisco IOS Release 12.2(4)B
Cisco Express Forwarding (CEF) Configuration Support	

You must enable CEF before Service Selection Gateway (SSG) can be enabled.	You must enable CEF on the router before you can enable SSG functionality. If CEF is not enabled and you attempt to configure SSG, the following error message is displayed:
	`SSG : Please enable ip cef first`
	You can enable CEF in global configuration mode using the following command:
	`Router(config)# ip cef`
	However, if required, you can disable CEF at the individual interface level without affecting SSG.

Data Packet Forwarding	
When a data packet is received from a user, SSG checks in the default network and open garden networks. If the check fails, the packet is checked and forwarded to the connected services of the user.	When a data packet is received from a user, SSG attempts to forward the packet by doing a longest match in the connected services of the user. If the packet is not destined for the connected services, SSG attempts to forward the packet to the configured default network or open garden networks. If the user is connected to an Internet service, SSG checks if the destination IP address of the packet falls in the default network or open garden networks. If so, the packet is forwarded to the respective destination; otherwise, the packet is forwarded to the Internet service.

Table 24 Differences Between CIsco IOS Release 12.2(2)B and Cisco IOS Release 12.2(4)B (continued)

Cisco IOS Release 12.2(2)B	Cisco IOS Release 12.2(4)B
Data Packet Processing Overhead	
When SSG is enabled, there is an extra packet processing overhead for packets from non-SSG interfaces. Every packet from a non-SSG interface is intercepted and minimally processed by SSG. This introduces an extra latency for packets from non-SSG interfaces.	There is no extra packet processing latency for packets from non-SSG configured interfaces. Only packets from configured SSG interfaces are intercepted and processed by SSG.
DNS Packet Processing in Open Garden Configuration	
Domain Name System (DNS) domain lookup is done first in the domains configured in the open garden services. If a match is not found, then DNS domain lookup is done in the connected services of the user.	DNS domain lookup is done first in the connected services of the user. If a match is not found, then DNS domain lookup is done in the domains configured in the open garden services.
DNS Packet Accounting	
DNS packets from a client are not accounted in the host or connection. This may cause erroneous accounting statistics at the host or connection level.	DNS packets are treated and accounted as any other data packets.
Host Timestamp Update	
The timestamp in the host object is updated only when a packet from the client is forwarded to a connected service. If a host is accessing the Cisco Subscriber Edge Services Manager (SESM) and an idle timeout is configured, the host may get logged off.	The timestamp is updated for any packet from the client, preventing an erroneous logoff. The only exception is if the packet is destined for the SSG router itself, in which case the timestamp is not updated.
L2TP Tunnel Support	

The **aaa new-model** command is not required to configure SSG to establish L2TP tunnels.	SSG uses a new application program interface (API) to support API tunnel-type services. You must use the following commands in global configuration mode to configure SSG to establish L2TP tunnels:
	`Router(config)# aaa new-model`
	`Router(config)# vpdn-enable`

Multiple Service Binding	
Only one service can be bound to a single interface or subinterface. If multiple services are bound to a single interface and a user connects to these services, the packets are not accounted correctly in the per-connection statistics maintained by SSG.	Multiple services can be bound to a single interface or subinterface without affecting connection accounting.

Table 24 Differences Between Clsco IOS Release 12.2(2)B and Cisco IOS Release 12.2(4)B (continued)

Cisco IOS Release 12.2(2)B	Cisco IOS Release 12.2(4)B
RADIUS Authentication for PPP Users	

User authentication is attempted by SSG using RADIUS protocol. To configure SSG to intercept user PPP authentication requests, you must configure PPP authentication. You do not need to specify RADIUS as the authentication protocol.
`Router(config)# aaa authentication ppp default local`
`Router(config)# aaa authorization network default group radius`
In the preceding configuration, SSG still sends an authentication request to the RADIUS server for a PPP user, even though a local authentication is specified in the CLI.
	User authentication is done by Cisco IOS PPP leveraging AAA RADIUS protocol for authenticating all PPP users. Using 12.2(2)B configuration, PPP will attempt to find the user configuration on the router itself.
	You must issue the following command in global configuration mode for authentication to be attempted:
	`Router(config)# aaa authentication ppp default group radius`

Replaced command: debug http-redirect	
The **debug ssg http-redirect** command is available.	The **debug ssg http-redirect** command is not available and has been replaced by the **debug ssg tcp-redirect** *options* command to debug issues related to redirection.
Virtual Route-Forwarding (VRF) Support for GRE tunnels	
SSG does not leverage Cisco IOS CEF and does not create CEF tables.	SSG leverages Cisco IOS CEF for data forwarding. This necessitates the use of CEF tables for data path switching. SSG creates and maintains a CEF table on each service (uplink) interface or subinterface. This is a VRF scalability issue, whereby the number of CEF tables that SSG can create and support is limited by VRF scalability on a given platform or NRP card. For example, if GRE tunnels are configured on the service side, SSG attempts to create a CEF table per GRE tunnel, which, due to memory resource limitation on the router, may prevent SSG from creating CEF tables.

Caveats for Cisco IOS Release 12.2 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 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*.

All caveats in Cisco IOS Release 12.2 are also in Cisco IOS Release 12.2 T.

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*, 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 12.2 and Cisco IOS Release 12.2 T are also in Cisco IOS Release 12.2(4)B.

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*.

For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 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, l**og 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 25 Caveats Reference for Cisco IOS Release 12.2 B

DDTS Number	Open in Release	Resolved in Release
CSCdr00817		12.2(4)B4
CSCdu14530		12.2(4)B4
CSCdu33067		12.2(4)B4
CSCdu34891	12.2(4)B	
CSCdu44023	12.2(4)B	
CSCdu45504		12.2(4)B8
CSCdu46694		12.2(4)B5
CSCdu57873		12.2(4)B5
CSCdu63338	12.2(4)B	
CSCdu63623		12.2(4)B3
CSCdu66646		12.2(4)B3
CSCdu69834		12.2(4)B1

Table 25 Caveats Reference for Cisco IOS Release 12.2 B (continued)

CSCdu77971		12.2(4)B4
CSCdu81007		12.2(4)B3
CSCdu81314		12.2(4)B5
CSCdu81936		12.2(4)B3
CSCdu88327	12.2(4)B	
CSCdv00283		12.2(4)B
CSCdv02925		12.2(4)B3
CSCdv04999		12.2(4)B8
CSCdv06104		12.2(4)B1
CSCdv06458		12.2(4)B5
CSCdv08146	12.2(4)B	
CSCdv10805		12.2(4)B5
CSCdv18634		12.2(4)B7
CSCdv22628		12.2(4)B5
CSCdv22980		12.2(4)B3
CSCdv24983		12.2(4)B5
CSCdv25288		12.2(4)B3
CSCdv25305	12.2(4)B	
CSCdv30101		12.2(4)B3
CSCdv36427		12.2(4)B6
CSCdv37058		12.2(4)B7
CSCdv37075	12.2(4)B	
CSCdv37414		12.2(4)B3
CSCdv38563		12.2(4)B3
CSCdv33310		12.2(4)B6
CSCdv40244		12.2(4)B8
CSCdv40395		12.2(4)B5
CSCdv43856		12.2(4)B1
CSCdv46135		12.2(4)B4
CSCdv46891		12.2(4)B4
CSCdv47047		12.2(4)B5
CSCdv50649		12.2(4)B4
CSCdv53408	12.2(4)B	
CSCdv55144		12.2(4)B3
CSCdv57565		12.2(4)B3
CSCdv59309		12.2(4)B5
CSCdv60768		12.2(4)B5

Table 25 Caveats Reference for Cisco IOS Release 12.2 B (continued)

CSCdv62649		12.2(4)B4
CSCdv62742		12.2(4)B4
CSCdv63941		12.2(4)B5
CSCdv64668		12.2(4)B3
CSCdv70007	12.2(4)B	
CSCdv71453		12.2(4)B5
CSCdv75160	12.2(4)B	
CSCdv76946		12.2(4)B5
CSCdv78557		12.2(4)B
CSCdv79009		12.2(4)B4
CSCdv83402		12.2(4)B5
CSCdv86531		12.2(4)B
CSCdv86601	12.2(4)B	
CSCdv88009		12.2(4)B4
CSCdv89039		12.2(4)B3
CSCdv89182	12.2(4)B	
CSCdv90477		12.2(4)B4
CSCdv90584		12.2(4)B3
CSCdv91266		12.2(4)B4
CSCdw00722		12.2(4)B3
CSCdw00924		12.2(4)B5
CSCdw01472	12.2(4)B	
CSCdw01593	12.2(4)B	
CSCdw02017		12.2(4)B3
CSCdw04802	12.2(4)B, 12.2(4)B1	12.2(4)B3
CSCdw05784	12.2(4)B	
CSCdw07263		12.2(4)B8
CSCdw09685		12.2(4)B4
CSCdw09799	12.2(4)B	
CSCdw10106		12.2(4)B5
CSCdw11263	12.2(4)B	
CSCdw12504	12.2(4)B	
CSCdw16275	12.2(4)B	
CSCdw19522		12.2(4)B3
CSCdw20470	12.2(4)B	
CSCdw20648		12.2(4)B3

Table 25 Caveats Reference for Cisco IOS Release 12.2 B (continued)

CSCdw22547	12.2(4)B	
CSCdw22714		12.2(4)B5
CSCdw23718	12.2(4)B	
CSCdw24835	12.2(4)B	
CSCdw26306		12.2(4)B5
CSCdw27563		12.2(4)B3
CSCdw28811		12.2(4)B
CSCdw29624		12.2(4)B
CSCdw35046		12.2(4)B4
CSCdw39118		
CSCdw40164		12.2(4)B4
CSCdw42091		12.2(4)B4
CSCdw45491		12.2(4)B5
CSCdw52218		12.2(4)B1
CSCdw52832		12.2(4)B4
CSCdw52890		12.2(4)B5
CSCdw53590		12.2(4)B8
CSCdw54872		12.2(4)B5
CSCdw57301		12.2(4)B3
CSCdw59858		12.2(4)B3
CSCdw61367		12.2(4)B3
CSCdw61510		12.2(4)B3
CSCdw62647		12.2(4)B3
CSCdw62692		12.2(4)B3
CSCdw63287		12.2(15)B
CSCdw65799		12.2(4)B5
CSCdw65903		12.2(4)B2
CSCdw69187		12.2(4)B3
CSCdw70202		12.2(4)B5
CSCdw72786		12.2(4)B3
CSCdw76955		12.2(4)B4
CSCdw78219		12.2(4)B3
CSCdw81149		12.2(16)B
CSCdw87320		12.2(4)B3
CSCdw87704		12.2(4)B3
CSCdw89981		12.2(4)B3
CSCdw90521		12.2(4)B3

Table 25 Caveats Reference for Cisco IOS Release 12.2 B (continued)

CSCdw93992		12.2(4)B5
CSCdx00274		12.2(4)B6
CSCdx04161		12.2(4)B3
CSCdx08399		12.2(4)B5
CSCdx09654		12.2(4)B4
CSCdx16143		12.2(4)B4
CSCdx21401		12.2(4)B8
CSCdx24485		12.2(4)B5
CSCdx24523		12.2(4)B5
CSCdx24528		12.2(4)B4
CSCdx33179		12.2(4)B4
CSCdx34233		12.2(4)B5
CSCdx35300		12.2(4)B5
CSCdx37849		12.2(4)B5
CSCdx38190		12.2(4)B4
CSCdx42856		12.2(4)B5
CSCdx52693		12.2(4)B5
CSCdx56527		12.2(4)B4
CSCdx57829		12.2(4)B4
CSCdx59130		12.2(4)B5
CSCdx61867		12.2(4)B5
CSCdx69995		12.2(4)B5
CSCdx74432		12.2(4)B6
CSCdx86654		12.2(4)B6
CSCdx88866		12.2(4)B5
CSCdy00765		12.2(4)B6
CSCdy02662		12.2(4)B6
CSCdy05118		12.2(4)B7
CSCdy07358		12.2(4)B6
CSCdy15222		12.2(4)B6
CSCdy17135		12.2(4)B7
CSCdy18112		12.2(16)B
CSCdy18641		12.2(4)B6
CSCdy31671		12.2(4)B6
CSCdy50235		12.2(16)B
CSCdz04280		12.2(16)B
CSCdz08582		12.2(4)B8

Table 25 Caveats Reference for Cisco IOS Release 12.2 B (continued)

CSCdz18063		12.2(4)B8
CSCdz28101		12.2(15)B
CSCdz34487		12.2(15)B
CSCdz30226		12.2(15)B
CSCdz45158		12.2(15)B
CSCdz45729		12.2(4)B8
CSCdz45785		12.2(15)B
CSCdz46364		12.2(15)B
CSCdz50451		12.2(15)B
CSCdz52550		12.2(15)B
CSCdz54159		12.2(15)B
CSCdz60229		12.2(4)B8
CSCdz71127		12.2(16)B1, 12.2(16)B
CSCdz71437		12.2(15)B
CSCdz73922		12.2(15)B
CSCdz74545		12.2(15)B
CSCdz76138		12.2(16)B
CSCdz85719		12.2(15)B
CSCdz86646		12.2(15)B
CSCea01845		12.2(16)B
CSCea02355		12.2(16)B1, 12.2(16)B
CSCea07370		12.2(16)B
CSCea07503		12.2(16)B
CSCea12794		12.2(16)B
CSCea15243		12.2(16)B
CSCea17870		12.2(16)B
CSCea21199		12.2(16)B
CSCea24313		12.2(16)B
CSCea24742		12.2(16)B
CSCea25265		12.2(16)B
CSCea25622		12.2(16)B
CSCea30311		12.2(16)B
CSCea31724		12.2(16)B
CSCea32437		12.2(16)B
CSCea33654		12.2(16)B
CSCea34526		12.2(16)B
CSCea34862		12.2(16)B

Table 25 Caveats Reference for Cisco IOS Release 12.2 B (continued)

CSCea35840		12.2(16)B
CSCea35922		12.2(16)B
CSCea38882		12.2(16)B
CSCea38967		12.2(16)B
CSCea39209		12.2(16)B
CSCea39211		12.2(16)B
CSCea41221		12.2(16)B2
CSCea49915		12.2(16)B
CSCea53122		12.2(16)B
CSCea56675		12.2(16)B
CSCea59313		12.2(16)B
CSCea61004		12.2(16)B
CSCea63661		12.2(16)B
CSCea65313		12.2(16)B
CSCea67751		12.2(16)B
CSCea71773		12.2(16)B
CSCea72908		12.2(16)B
CSCea81955		12.2(16)B
CSCea82153		12.2(16)B
CSCea91076		12.2(16)B2
CSCea93108		12.2(16)B
CSCeb00875		12.2(16)B2
CSCeb06567		12.2(16)B2
CSCeb26162		12.2(16)B2
CSCeb64770		12.2(16)B2
CSCin00170		12.2(4)B
CSCin00381		12.2(4)B
CSCin00405	12.2(4)B	
CSCin02189		12.2(4)B3
CSCin02516		12.2(4)B5
CSCin03065		12.2(4)B4
CSCin04547		12.2(4)B4
CSCin04907		12.2(4)B3, 12.2(16)B
CSCin05032		12.2(4)B3
CSCin05105		12.2(4)B3
CSCin05326		12.2(4)B3
CSCin05660		12.2(4)B3

Table 25 Caveats Reference for Cisco IOS Release 12.2 B (continued)

CSCin07365		12.2(4)B7
CSCin07972		12.2(4)B4
CSCin08083		12.2(4)B4
CSCin09724		12.2(4)B4
CSCin10233		12.2(4)B4
CSCin10258		12.2(4)B4
CSCin10403		12.2(4)B5
CSCin12283		12.2(4)B5
CSCin16553		12.2(4)B6
CSCin22337		12.2(16)B
CSCin25155		12.2(15)B
CSCin25855		12.2(16)B
CSCin26392		12.2(15)B
CSCin29336		12.2(15)B
CSCin30310		12.2(15)B
CSCin31094		12.2(15)B
CSCin32530		12.2(16)B
CSCin34074		12.2(16)B
CSCin34382		12.2(16)B
CSCin34478		12.2(16)B
CSCin36229		12.2(16)B
CSCin36807		12.2(16)B
CSCin37162		12.2(16)B
CSCin37586		12.2(16)B
CSCin37959		12.2(16)B
CSCin39190		12.2(16)B
CSCin39954		12.2(16)B
CSCin41018		12.2(16)B2
CSCin42549		12.2(16)B
CSCin43411		12.2(16)B
CSCin43415		12.2(16)B
CSCuk27655		12.2(15)B
CSCuk27669		12.2(4)B5
CSCuk30302		12.2(4)B8
CSCuk31098		12.2(4)B3
CSCuk41239		12.2(16)B

Open Caveats—Cisco IOS Release 12.2(16)B2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(16)B2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(16)B2.

Resolved Caveats—Cisco IOS Release 12.2(16)B2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(16)B2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea41221

  Spurious access caused in pppoe show vc. This problem occurs on all platforms in 12.2(15)B and geo t pi1 near branch

  There are no known workarounds.

- CSCea91076

  On some occasions, a router with an NM-4T1-IMA will fail to create a vc offering the following message:

  ```
  (Cause of the failure: vpi/vci pair already in use)
  ```
  Additional tracebacks will also be seen.

  The message is also seen on a 7200 router with NPE400 running 12.2.16B.

  There are no known workarounds.

- 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 sate for any reason; like ATM OAM taking the VC down.

  Workaround: Re-configure the ATM PVC or don't use PPPoX autsensing. 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
  ```

- 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.

- 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.

- CSCeb64770

  Upon reload of a router, System accounting-on is not sent as the first packet out of the box. This happens only during boot up time.

  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.

  This 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.

Open Caveats—Cisco IOS Release 12.2(16)B1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(16)B1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(16)B1.

Resolved Caveats—Cisco IOS Release 12.2(16)B1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(16)B1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea02355

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

Open Caveats—Cisco IOS Release 12.2(16)B

This section documents possible unexpected behavior by Cisco IOS Release 12.2(16)B and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(16)B.

Resolved Caveats—Cisco IOS Release 12.2(16)B

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(16)B. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw81149

  Large (>1500 bytes) pings cause the vpdn session received counters (packets/bytes) to be incorrect.

  There are no known workarounds.

- CSCdy18112

  When using a PVC range command, traceback message may appear while configuring **range pvc** command.

  There are no known workarounds.

- CSCdy50235

  SNMP always reports 0 for the delay (casAuthenResponseTime).

  The problem happens when you try to monitor the average authentication response delay using SNMP.

  Workaround: Use the **show radius statistics** command to get the value of the delay.

- CSCdz04280

  QOS policies will not be applied to traffic if service-policy contains an access-list which is based on time. Traffic will flow through the router as if the QOS policy does not exist. This could allow a greater throughput than anticipated.

  This symptom is observed on a Cisco 7200/7400 series router which contain PXF forwarding technology. The PXF must be enabled for the symptom to experienced.

  Workaround: Disable the PXF “no ip pxf”. Note that there can be a performance impact when disabling the PXF.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCdz76138

  With a 7400 use as LNS, when PXF is actif, the virtual-interface output counter, and the radius Acct-Output-Octets are aprox 2.5 time less than reality.

  When the PXF is disable, the counter works well.

  The problem exist in 12.2.4B5 B6 & B7.

  Workaround: Disable PXF

- CSCea01845

  IPCP negotiation is failing between client and LNS when with L2F protocol between LAC and multihop and L2F protocol between multihop and LNS. The LNS is sending IPCP request and the client is receiving them. The client also sends IPCP request and acknowledges the IPCP packets from LNS. But the LNS is not receiving any IPCP request or ack from client.

  There are no known workarounds.

- CSCea02355

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea07370

  A 7400 router may record output drops, when matches are made against an ACL.

  This happens when packets match an Access list

  Workaround: Disable PXF via the **no ip pxf command**, but this may drive the CPU up and is not suggested.

- CSCea07503

  tcp-redirect is not working anymore.

  If the tcp-redirect server's route has got changed, SSG does not update its database and downstream packets may not get properly reverse-mapped.

  The way you can check this is using the following CLI:

  ```
  show ssg tcp-redirect group <group-name>
  ```
  There are no known workarounds.

- CSCea12794

  LCP keepalive does not work correctly.

  This symptom is observed when configuring keepalive over 256sec at virtual-template. The following table is a test result of this symptom:

  ```
  config     : actual interval
   keepalive 256 : not output ECHOREQ
   keepalive 260 : every 4sec
   keepalive 300 : every 45sec
  ```
  Workaround : Make sure that the keepalive vaule is under 255sec.

- CSCea15243

  Ping fails for aal5mux ppp dial encapsulation when the ATM interface is with aal5mux ppp dial encapsulation.

  The problem happens under the following:

  - Client is pppoa with dialer.
  - Server is pppoa with vtemplate.
  - When the client is pppoa with vtemplate and the server is pppoa with vtemplate the problem never happens.

  Problem does not exist in 12.2(14.5)T even when the client is pppoa with dialer. The problem is introduced in 12.2(14.6)T and has been observed in 827 by the submitter and on a 7200 NPE 300

  Workaround: When the client is pppoa with vtemplate the problem never happens even with a 12.2(14.6)T image.

- CSCea17870

  When Parallel Express Forwarding (PXF) is enabled, a variety of symptoms may occur depending on the Cisco router or switch:

  - A router may reload.
  - A router may not forward packets correctly.
  - The “IPFAST-2-PAKSTICK: Corrupted pak header” error message may be generated.

  This symptom is observed when a packet is punted to the Route Processor (RP) and occurs because the paktype was not properly scrubbed after its last use.

  Workaround: Disable PXF. If this is not an option, then there is no workaround.

- CSCea21199

  RADIUS proxy logon fails for CDMA2000 Mobile IP users. This occurs when the host object activation fails for Mobile IP users. This only occurs for auto-domain when PBHK is not enabled

  Workaround: Enable PBHK.

- CSCea24313

  A router may incorrectly move a default static route from one upstream router to another upstream router and then back again, and may continue to flap the route every 60 seconds.

  This symptom is observed in the following configuration:

  A Cisco router (referred to as router A) is connected to two upstream routers (referred to as router B and router C) via a common interface. Router A is configured with two default recursive static routes, one via an address that is advertised by router B, the other one via an address that is advertised by router C.

  The administrative distances of the static routes are set in such a way that if both router B and router C are reachable, router A installs the default static route via router B. If router B becomes unreachable, router A installs the default static route via router C.

  Router B is advertising X::1. Router C is advertising X::2. Router A is configured in the following way:

  ```
  ipv6 route ::/0 X::1
  ipv6 route ::/0 X::2 2
  ```

When router B stops advertising X::1, router A removes the default static route via router B and installs the default static via router C. This is correct behavior. However, 60 seconds after the transition, router A incorrectly reinstalls the default static route via router B and removes the default static route via router C. Another 60 seconds later, router A removes the static route via router B and reinstalls the static route via router C. This route flap occurs every 60 seconds.

Workaround: Do not rely on recursive static routes for the default route. For example, configure Interior Gateway Protocol (IGP) on routers B and C to advertise the default route. Appropriate configuration of metrics may ensure that the default route via router B is preferred to the one via router C, providing the same preference as the one that is obtained via static routes.

- CSCea24742

  A memory leak may be observed on a router.

  The system memory will decrease and become increasingly fragmented over time. The output of the **show memory** EXEC command will display an increasing number of objects that are of the "MLP bundle name" object type.

  One "MLP bundle name" object is lost each time a forwarded connection is established. Hence, systems that have high call rates (with several dynamically created sessions) are more severely impacted than systems that have low call rates (with a few semi permanent sessions).

  This symptom is observed on routers that are the local termination points for PPP sessions that have been forwarded by virtual private dialup network (VPDN) or Subscriber Service Switching (SSS) and where the PPP sessions in question have negotiated to use multilink.

  There are no known workarounds.

- CSCea25265

  The pxf crashes on NSE-1. This occurs when the router receives a large number of streaming video feeds.

  There are no known workarounds.

- CSCea25622

  A NPE-G1 may reload by itself and reports the reload as a "System was restarted by reload".

  This problem occurs on c7200 with NPE-G1 running IOS release 12.1(14)E.

  There are no known workarounds.

- CSCea30311

  A Cisco 7200 may crash due to a Bus error with PPPoA using 12.2(15)B image.

  When pppoa context gets deleted when printf suspends inside pppoa_show_specific_vc_info the crash happens when we access the non-null freed pointer. This fix also ensures all freed memory is made null prior to freeing to prevent crashes in other places not reported in this ddts.

  There are no known workarounds.

- CSCea31724

  If all configured Radius servers (within a server-group or globally, if server groups are not used) have been declared DEAD, the router will no longer issue Radius requests until at least one server's deadtime has expired. In this state, the router issues the error message %RADIUS-3-NOSERVERS: No Radius hosts configured. This problem can also be observed after booting-up when connectivity to the Radius servers hasn't been established and initial Radius requests (ex: accounting-start record) have already timed out.

  This problem only occurs in Cisco IOS releases 12.2(13.7)T1 and later and if a deadtime is configured globally or within the server-group. With earlier IOS releases, the router skips the deadtime if all servers are declared DEAD.

  Workaround: do not use radius-server deadtime.

- CSCea32437

  When policing/marking is configured on main interface, but traffic is switched on its subinterfaces, QoS policing/marking on the Cisco 7200 NSE1 does not work.

  Workaround: Use the main interface only.

- CSCea33654

  Memory leak found in radius code while doing stress testing using Radius server.

  There are no known workarounds.

- CSCea34526

  A user does Radius Proxy Logon from GGSN through SSG to AAA. HO is created and on autologon, service is activated. User does a Radius Proxy Logon again from the same GGSN SSG to AAA. SSG logs off existing HO & logs in new user. But during logoff, SSG only sends an Accounting-Stop to AAA for the active service and not for the HO.

  The problem is seen when a user tries to logon from the same GGSN through SSG to AAA. when the user was logged on through another GGSN through SSG to AAA, SSG does send Accounting-Stop to AAA.

  There are no known workarounds.

- CSCea34862

  When running a Cisco IOS image with the fix for CSCdy65156, there may be messages stating that AAA is not supported with the image during bootup.

  ```
  Example:
  % Image does not support any AAA protocols.
  ```
  This is a cosmetic issue and does not prevent AAA from operating correctly once the main IOS image is loaded.

  There are no known workarounds.

- CSCea35840

  If a Mobile Node roams from one PCF to another PCF but remains on the same PDSN and the accounting start arrives at the SSG before the accounting stop, then the PPP session may be terminated

  This occurs when SSG is running Cisco IOS version 12.2(8)B1 or earlier.

  There are no known workarounds.

- CSCea35922

  PCR does not get applied to UBR ATM PVCs using radius.

  If radius is used to apply PCR for UBR ATM PVCs, it does not change the PCR values of those PVCs.

  There are no known workarounds.

- CSCea38882

  A Cisco 7200 router may reload because the packet cleanup is not performed completely in the interrupt path of the ATMDX PA.

  This symptom is observed on a Cisco 7200 series router that is running Cisco IOS 12.2 release and is configured with a PA-A3 port adapter

  There are no known workarounds.

- CSCea38967

  A Cisco 7200 NSE or 7401 ASR router may reload because the packet cleanup is not performed in Toaster punt path for serial drivers.

  Workaround: Turn off PXF using the **no ip pxf** command.

- CSCea39209

  Incorrect service activation when there is a mismatch between the auto-domain mode configured on SSG and the type of auto-domain profile retrieved from the AAA server.

  Auto-domain can operate in 2 modes: basic and extended. In basic mode SSG expects a normal service profile to be downloaded in response to the auto-domain profile request. In extended mode it expects a “Virtual User Profile” (i.e. an account profile).

  If SSG detects a mismatch (i.e. the downloaded profile is not of the expected type) then the auto-domain logon should fail i.e. An Access-Reject returned an no host object created. This is not happening.

  Workaround: Ensure that SSG and the AAA server are configured correctly such that the correct type of auto-domain profile is downloaded.

- CSCea39211

  When SSG receives an Account Logoff from the SESM for a Host which is not present on the box, tracebacks are seen. This is seen only when the CLI “ssg wlan reconnect” is enabled.

  There are no known workarounds.

- CSCea49915

  Cisco SSG box does not send out framed ip address in re-auth req for services. This is specific to c6400_oxygen branch.

  There are no known workarounds.

- CSCea53122

  Router reloads while switching TCP traffic in cef path.

  When TCP redirection for unauthenticated user is enabled, with CEF siwtching enabled for downlink interface, SSG can reload.

  Workaround: Disable CEF switching on the downlink interface.

- CSCea56675

  For the second transmission of an EAP based authentication, the error message %RADIUS-3-NOSERVERS is seen, the RADIUS packet is not transmitted, and the authentication fails. This happens despite at least one RADIUS server being properly configured, and as per 'show aaa servers' that RADIUS server is UP.

  There are no known workarounds.

- CSCea59313

  A Cisco SSG router (which is acting a proxy RADIUS server) running c7200-g4js-mz.v122_15_bw_throttle may encrypt the PAP password of user in a wrong manner. Some junk characters are visible towards the end of the attribute conents.

  The root cause of the problem has been found and it will be fixed in the next release i.e. 12.2(16)B. User Password is < 8 characters long.

  Workaround: Use long PAP passwords

  Alternative workaround 1: Use CHAP authentication

  Alternative workaround 2: Ignore the password check at server

- 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.

- CSCea63661

  RADIUS proxy logon fails for CDMA2000 MSID-based access, Cisco variant.

  The Cisco variant of MSID-based access will fail if SSG is configured to use a “session-identifier” that does not include the username. Note that this includes the default configuration which not use the username as part of the “session-identifier”.

  In the RADIUS proxy configuration for the RADIUS client(s) specify one of the following CLIs:

  - session-identifier username
  - session-identifier auto username
  - session-identifier msid username
  - session-identifier acct-sess-id username
  - session-identifier correlation-id username

- 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.

- CSCea67751

  SSG does not send error message code attributes in the Access Reject packets, if the service logon is not successful, eg if it fails due to an unsuccessful service activation or due to a soft rejection (eg 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.

- CSCea71773

  SSG does not include re-authorisation reason “QR0” in re-authorisation packet which is sent to prepaid server (here: OCS, online charging server).

  The re-authorization is caused by a time quota expiry.

  This attribute should be contained because previous Access-Accept packet contains:

  – Idle timeout attribute with value “0”

  – Volume quota attribute “QV” having the value “0”

  – Time quota attribute “QT” having the value “>0”

  Workaround: Enable prepaid threshold for time with the following SSG config command:

  ssg prepaid threshold time <seconds>

- 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”:

  ```
  <snip>
  Starting MSID retry timer
  MSID retry timer expired for User/SessionID
  </snip>
  ```

  There are no known workarounds.

- CSCea81955

  Even at low rate and throughput, there may be large output drops on ATM interface.

  A Cisco 7301 series configured with 4000 PVCs and running 12.3 based release may see large output drops on ATM interface even at low rate and CPU throughput. This defect is observed after a high traffic rate at which drops normally occur, is reduced.

  Workaround: Use the **shut/noshut** command on the ATM interface.

- CSCea82153

  While pinging to 7401ASR(NSE-1) through PPPoE, "%PXF-2-EXCEPTION" was observed at 7401ASR router. After "%PXF-2-EXCEPTION" was observed, L2TP cannot be connected from the other end router. The 7401ASR is using IOS 12.2(16.1)B2.

  Workaround: Remove PPP PFC/ACFC configurations.

- CSCea93108

  SSG can reload due to a software forced error.

  This can happen while using prepaid services in SSG with a seperate 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.

- CSCin04907

  In carbon_04 image, process switched internet service packets are dropped.

  The above problem can be seen only if SSG processes the packets properly in the CEF path and the packets get punted to the process later. Typically this can happen with natted connections.

  Workaround: Add a network specific route either in the service profile, or in the global routing table(using **ip route** command).

- CSCin22337

  When radius vpdn attributes are configured as cisco-AV pairs, attribute Acct-Tunnel-Connection-Id (68) is being printed as " " in Radius debugs, although the Radius server will get the correct value.

  Workaround: Configure vpdn attributes as IETF attributes.

- CSCin25855

  The VLAN implementation for the 7200 fast-/gigabit-ethernet drivers on the affected release trains is currently written in a manner that imposes a performance penalty even on plain ethernet (i.e. non VLAN encapsulated) packets.

  There is no impact on the functionality due this problem, but the throughput might suffer by around 15%.

  There are no known workarounds.

- CSCin32530

  When there are 1000 host objects created on SSG and the **no ssg enable force-clean** command is executed, tracebacks are seen.

  These tracebacks are seen when accounting is enabled for the users. Without accounting enabled, the tracebacks are not seen.

  There are no known workarounds.

- CSCin34074

  Help may give misalligned output in a c4gwy running c4gwy-isx3-mz.122-16.1.T image.

  There are no known workarounds.

- CSCin34382

  c7200 (with NSE-1 board) or c7401 router crashes on "Bus Error exception".

  With turning Parallel Express Forwarding (PXF) on, using Fast-Ethernet (dec21140 chip. PA-FE or FE-IO), and running traffic to FE line rate.

  There are no known workarounds.

- CSCin34478

  SSG box crashes with 12.2(16)B image on disabling SSG and enabling SSG within a few seconds timeframe.

  This happens when “no ssg enable force-cleanup” function is called and SSG is enabled again with proper configs (say “copy startup run”) with no time-delay.

  Workaround: Do not disable SSG using the “no ssg enalble force-cleanup” funciton. If the function is useed, please wait for radius-timeout value configured for AAA server before enabling SSG again (radius-timeout = timeout * number of retransmits).

- CSCin36229

  If a **show atm pvc** command is issued twice, it causes the system to reboot.

  There are no known workarounds. However, the problem can be avoided by not issuing the **show atm pvc** command.

- CSCin36807

  The accounting records for connections and the prepaid authorization records have different formats for accounting-session ids.

  Prepaid reauthorization is of the form:

  ```
  RADIUS:  Acct-Session-Id     [44]  22  "1/0/0/1.100_00000003"
  ```
  while connection accounting records have the format:

  RADIUS: Acct-Session-Id   [44] 29 "00000003"

  if the port-bundle host key is disabled or the format:

  ```
  RADIUS:  Acct-Session-Id     [44]  29  "1/0/0/1.100        00000003"
  ```
  when port-bundle host-key is enabled.

  This problem occurs for prepaid connections when the **radius-server attribute nas-port format d** command is enabled.

  Workaround: Disable the **radius-server attribute nas-port format d** command.

- CSCin37162

  Inactive host objects with no IP address remain after failed RADIUS proxy logon.

  SSG is acting as a RADIUS proxy for CDMA2000 devices with basic mode auto- domain enabled. The auto-domain profile retrieved from the AAA server does not contain the required '3GPP2' attribute “IP-Technology”.

  Workaround: Ensure the AAA server is configured correctly such that the correct value for the “IP-Technology” attribute is returned in all auto-domain profiles.

- CSCin37586

  ISDN/L2TP session does not come up in LAC. If “debug l2x error” is turned on, “L2TP: Error setting up the L2HW Switching API” is seen. This occurs with or without PXF.

  There are no known workarounds.

- CSCin37959

  PPPoA sessions does not comeup after unconfiguring create on-demand. This happens only for autosensing pvc on the LAC when the peer’s encap is MUX type.

  Workaround : Uncofnigure the pvc on lac and recreate the pvc. (i.e. do a no pvc x/y and then reconfigure pvc).

- CSCin39190

  In a ISDN/L2TP topology, the ISDN layer 2 will go down as soon as send some downstream traffic when pxf is on.

  Workaround: Turn off pxf.

- CSCin39954

  When SSG proxies a radius transaction, and the router does not recieve a response from the radius server within the configured timeout, the router will produce the error message followed by a traceback:

  ```
  Apr  3 20:11:32.389: %AAA-3-SERVER_INTERNAL_ERROR: Server '0.0.0.14': Bad transaction
  type
  ```
  There are no known workarounds.

- CSCin42549

  If you configure:

  ```
  radius-server host x.x.x.x backoff exponential key SomeKey
  ```
  and then do:

  ```
  copy run start
  ```
  The configuration stored will be:

  ```
  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 will prevent the radius server from communicating with the router, resulting in users being unable to authenticate, accounting records to be dropped, and downloadable configuration to be ignored.

  If 'service password-encryption' is configured, you will see an error message resembling:

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

  Workaround: After configuring “radius-server host x.x.x.x backoff exponential key SomeKey” copy the running configuration to a tftp or tftp server, and edit it with a text editor to place the “key SomeKey” portion of the “radius-server host ...” configuration line at the end of the line.

  Then perform a “copy tftp start” or “copy ftp start” to place the configuration in the router’s startup configuration.

  Do not perform a copy run start

- 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 bingup 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.

- CSCuk41239

  Performance of tunnel decapsulation performed in software by Cisco Express Forwarding (CEF) has fallen by approximately 3% in the case of 64-byte packets (less in the case of larger packets) since 12.2(11)T2.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(15)B

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)B and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(15)B.

Resolved Caveats—Cisco IOS Release 12.2(15)B

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)B. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw63287

  c7400 acting as an L2TP tunnel endpoint may crash.

  This may be seen on a c7400 begining with 12.2(12.14)T1 when there are multiple L2TP tunnels on the router and the same local L2TP session id is used in different tunnels.

  There are no known workarounds.

- CSCdz28101

  A number of different memory access violations, including “align-3- spurious” errors, may occur on a Cisco 7400 series router, and the router may reload.

  This symptom is observed on a Cisco 7400 series router that is configured as a Virtual Private Network (VPN) Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) and that supports Parallel Express Forwarding (PXF). The symptom may occur independent of whether PXF is enabled or disabled.

  There are no known workarounds.

- CSCdz30226

  6400 NRP may crash when bringing up lots of PPPoA sessions with a high number of tunnels. This crash reportedly happens only when keepalives are turned off - typically keppalives are used in a PPPoA environment.

  Workaround: Have some keepalive on the virtual template for PPPoA interfaces.

- CSCdz34487

  The password change sequence does not work as expected when it is used with Cisco Secure Access Control Server software. The user can still access the router with the old password. He can change the existing password to a new password at a later time.

  This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(11)T.

  This problem was not noticed in 12.2(13)T image with cisco secure running on a NT box.

  There are no known workarounds.

- CSCdz45158

  NRP2 is crashing while Unconfiguring from PPP Access mode to Bridge Access Mode.

  There are no known workarounds.

- CSCdz45785

  “protocol ppp virtual-template” has disappeared.

  There are no known workarounds.

- CSCdz46364

  A Cisco router acting as a PPTP Network Server may experience spurious memory access and high CPU utilization if it receives PPTP data packets for a session that no longer exists.

  There are no known workarounds.

- CSCdz50451

  7200 box running 12.2(13.2)S1 code reports spurious memory access:

  ```
  Dec  6 10:25:58: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x604455E8 reading
  0x40
  Dec  6 10:25:58: %ALIGN-3-TRACE: -Traceback= 604455E8 605BF308 605ADC60 605A27E0
  605BF440 605A2914 605ADC60 605BD7F8
  Dec  6 10:25:58: %ALIGN-3-TRACE: -Traceback= 604455EC 605BF308 605ADC60 605A27E0
  605BF440 605A2914 605ADC60 605BD7F8
  Dec  6 10:25:58: %ALIGN-3-TRACE: -Traceback= 602B6910 604455F8 605BF308 605ADC60
  605A27E0 605BF440 605A2914 605ADC60
  ```

  There are no known workarounds.

- CSCdz52550

  Process thrashing on watched message event occurs. When VPDN and failure log is enabled.

  There are no known workarounds.

- CSCdz54159

  Slow memory leak on the VPDN SSS Manager process when terminating L2TP tunnels.

  This may appear on a LNS under heavy load conditions when running Cisco IOS version 12.2(12.14)T. The VPDN SSS Manager process will increase the memory consumption at a slowly but steady rate.

  There are no known workarounds.

- CSCdz71437

  Session-timeout value configured higher than the max limit (which is 35790 min) is causing the user to disconnect immediately.

  Work-around: Lower the session-timeout value to 35790 min or below for the affected users.

- CSCdz73922

  A router acting as a PPTP access concentrator will experience CPU utilization which gradually increases over time. How quickly it increases depends on how many PPTP sessions are brought up on the router. Eventually, CPUHOG messages pointing to the PPTP Mgmt process will be seen and the CPU utilization will go to 100%.

  There are no known workarounds.

- CSCdz74545

  When bringing up 2000 PPP sessions on a ATM interface, the following is seen:

  ```
  %ATMPA-3-BADVCD: ATM6/0 bad vcd 65283 packet - FF03C021 0A01000C 028ECB60 7888C767
  00000000 00000000
  ```

  This was found in a 7200 and nrp.

  There are no known workarounds.

- CSCdz85719

  When Auto-Domain(radius-proxy) user tries to logon to a Tunnel type of Service, Host object does not get created.

  This is an internally found defect while regressing an 12.2(13)B throttle image January 19. When the CLI is configured with “nat user-address” in SSG-Auto-Domain submode.

  The workaround available would be to make the Tunnel Service as no-NAT service.

- CSCdz86646

  On a c7200 with an NPE-G1 processing engine and an GigabitEthernet I/O controller, users cannot configure GigabitEthernet0/0.

  There are no known workarounds.

- CSCin25155

  Router can get reloaded by watchdog event at radius_find_attr.

  There are no known workarounds.

- CSCin26392

  In IOS Version 12.2(13.4)T1, with “tacacs-server directed-request” enabled and if the username is used to specify the directed Tacacs+server address, by including the “@” symbol to specify the Tacacs+ host, the system reloads at Tacacs+ subsystem.

  Workaround: Disable the “directed-request” feature in the router; this will make the router use all servers specified in the configured global list of Tacacs+ servers, instead of directing a request to any of the configured servers.

- CSCin29336

  Flapping ATM interface or clearing all PPPoA sessions may cause some SWIDB leak. After many times it may eventually run out of SWIDB.

  There are no known workarounds.

- CSCin31094

  After change in encap of peer side, PPPoA session never comes up in the autosensing side.

  Configure autosensing on one side of PPPoA config. After establishement of a session, change the encap in peer side (i.e. from mux ot snap or vice versa).

  Workaround : Unconfigure the pvc and configure it again in the autosensing side.

- CSCin30310

  SSG undergoes an unexpected system reload. This occurs sometimes when tunnel service activation fails.

  There are no known workarounds.

- CSCuk27655

  GRE implementation of Cisco IOS is compliant with RFC2784 and RFC2890 and backward compatible with RFC1701.

Open Caveats—Cisco IOS Release 12.2(4)B8

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)B8 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(4)B8.

Resolved Caveats—Cisco IOS Release 12.2(4)B8

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)B8. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu45504

  High CPU when doing CB-wfq with shaping on tunnel interface.

  Workaround: Use police instead of shape in the definition of the policy-map.

  Example of workaround:

```
policy-map lab_test
  class class-default
     police 768000 24000 24000 conform-action transmit exceed-action drop
!
interface Tunnel0
 ip address 10.1.1.5 255.255.255.252
 no ip route-cache cef
 load-interval 30
 service-policy output lab_test
 tunnel source 172.16.1.1
 tunnel destination 172.16.2.1
The following config cause HIGH CPU
-----------------------------------
policy-map lab_test
  class class-default
     shape average 768000 19200
!
interface Tunnel0
 ip address 10.1.1.5 255.255.255.252
 no ip route-cache cef
 load-interval 30
```

```
 service-policy output lab_test
 tunnel source 172.16.1.1
 tunnel destination 172.16.2.1
```

Alternative workaround: Performing shaping on the physical interface rather than on the tunnel, or use IPIP rather than GRE encapsulation.

- CSCdv04999

  The username, accounting record type, and service attributes in the command accounting record do not have the appropriate values.

  There are no known workarounds.

- CSCdv40244

  The following continuous stream of "%POT1E1-3-FWFATAL" error messages may occur on a router:

  ```
  %POT1E1-3-FWFATAL: Bay 5: firmware needsresetdue to fw watchdog timeout
  %POT1E1-3-FWFATAL: Bay 4: firmware needsresetdue to fatal software errors
  ```

  This symptom is observed on a Cisco 7206VXR router that is running

  Cisco IOS Release 12.1(8.04)and a Cisco 7500 router running Cisco IOS release 12.0(21)S2 configured with a PA-MC-8T1 port adapter, but may also affect the PA-MC-2T1, PA-MC-4T1, PA-MC-8DSX1, PA-MC-2E1/120, and PA-MC-8E1/120 port adapters.

  There are no known workarounds.

- CSCdw07263

  The following error message is observed when there's an interface which has been configured with VRF and helper address(es):

  ```
  01:21:00: %SYS-3-NULLIDB: Null IDB in ipsendnet
  -Process= "IP Input", ipl= 0, pid= 41
  -Traceback= 606F17FC 606B9E58 606B9604 606B8C78 606E1D70 606DFBEC 606DFCE8 606DFE64
  ```

  There are no known workarounds.

- CSCdw53590

  When using a RADIUS server for authentication, IOS will not use the configured "aaa authentication username-prompt" and "aaa authentication password-prompt" in 12.2(2)XB and 12.2(4)T and later.

  There are no known workarounds.

- CSCdx21401

  The Local exec authorization doesn't work correctly when used as a secondary authorization method, and the Local user privilege levels are ignored. However, the Local authorization works fine when used as the primary authorization method.

  There are no known workarounds.

- CSCdz08582

  In some rare case, when SWIDB or system memory is exhausted, PPTP sessions and tunnels are cleaned up improperly in one corner case, crashing the system.

  There are no known workarounds.

- CSCdz18063

  Two bytes of username was sent though RFC 2058 says that the usenrname should be >= 3 bytes. The same problem happens when using radius-server domain-stripping command.

  There are no known workarounds.

- CSCdz45729

  A network access server (NAS) running Cisco IOS Release 12.2(04)B08 crashes when attempting to establish a Layer 2 Forwarding (L2F) tunnel with no RADIUS class attribute (25) configured in the authentication, authorization, and accounting (AAA) server.

  Workaround: Configure a RADIUS class attribute (25) on the AAA server.

- CSCdz60229

  Cisco devices which run IOS and contain support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS is disabled by default.

  Cisco will be making free software available to correct the problem as soon as possible.

  The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

  This advisory is available at
  http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

- CSCuk30302

  This DDTS extends the fix in CSCdu45504 to cover a remaining spurious access on the pas platforms (7200 etc.) that impacts performance of traffic shaping on gre tunnels.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(4)B7

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)B7 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(4)B7.

Resolved Caveats—Cisco IOS Release 12.2(4)B7

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)B7. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv18634

  When system is running Debitcard Application under high stress with CPU utilization in the 98% to 99%, it may reload. This occur when the Radius server port numbers other than default ports(1645/1646) is used.

  Workaround: Use Call Admission Control feature to reject calls when CPU utilization goes above 95%.

  Example Configuration:

  ```
  call treatment on
  call threshold global cpu-5sec low 95 high 98 treatment
  call threshold global cpu-avg low 95 high 98 treatment
  ```

  Alternative workaround: Use only Radius default ports(1645/1646) for the Radius servers configured.

- CSCdv37058

  As a solution to CSCds81473, we arrived at a solution that no WORDS will start with comment characters. This causes problems like CSCdu18402, CSCdv27051.

  There are no known workarounds.

- CSCdy05118

  A per-user interface configuration that is loaded from an authentication, authorization, and accounting (AAA) server can have a maximum length of 600 bytes. If if the maximum length is exceeded and the AAA profile is in the "old-style" format "lcp:interface-config=....," the router will reload.

  If the maximum length is exceeded and the AAA profile is in the "new-style" format "lcp:interface-config#<n>=..." (in which <n> is the is the sequence number of the lines sent), the router will not reload, but the user will be rejected.

  This symptom is observed on a router that is running Cisco IOS Release 12.2(4)B or Release 12.2(10.7)T.

  There are no known workarounds.

- CSCdy17135

  A router may reload if a per-user interface configuration line is greater than 80 characters.

  Workaround: Ensure that each line is less than 80 characters.

- CSCin07365

  Router crashes with "Show queue interface". This happens at LAC when the heavy data traffic is there towards client from LNS (downstream). This happens in CEF, Fast switch and Process switch paths.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(4)B6

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)B6 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(4)B6.

Resolved Caveats—Cisco IOS Release 12.2(4)B6

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)B6. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv33310

  Certain PXF code issues cause the “show pxf crash” to leave minimal information.

  There are no known workarounds.

- CSCdv36427

  A router acting as an L2TP LAC may crash as L2TP tunnels are created and destroyed.

  There are no known workarounds.

- CSCdw39118

  A router that is configured with generic routing encapsulation (GRE) tunnels may pause indefinitely and continuously scroll the following messages on the console:

  ```
  %SYS-2-NOTQ: unqueue didnít find 0 in queue 62360144 -Process= "<interrupt
  level>", ipl= 1 -Traceback= 60538810 60536468 60536468 6015DB10 60431D64
  60433D04 60433DC8
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=0, count=0 -Traceback=
  60672220 60538818 60536468 60536468 6015DB10 60431D64 60433D04 60433 DC8
  ```

  The conditions under which these symptoms occur are not known at this time.

  There are no known workarounds.

- CSCdx00274

  A single-port Fast Ethernet 100BASETX port adapter (PA-FE-TX) on a Cisco 7206VXR router that has a Network Processing Engine (NPE-300) may stop receiving burst traffic packets.

  This symptom is observed on a PA-FE-TX of a Cisco 7206VXR that has an NPE-300.

  Workaround: This symptom can be cleared by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the PA-FE-TX interface.

- CSCdx74432

  Memory allocation (MALLOC) failures may be observed when Border Gateway Protocol (BGP) updates are generated, and the following error message may be displayed:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 2093048 bytes failed from 0x602BDB08,
  alignment 0 Pool: Processor  Free: 1546596  Cause: Not enough free memory
  Alternate Pool: None  Free: 0  Cause: No Alternate pool
  ```

  There are no known workarounds.

- CSCdx86654

  An old bestpath may incorrectly remain in the routing table.

  This condition is observed if internal Border Gateway Protocol (iBGP) multipath is used for a Virtual Private Network version 4 (VPNv4) route.

  Workaround: There are no known workarounds, but the situation can be cleared by clearing the route.

- CSCdy00765

  On a 7400 running 12.2(4)B4, the following errors may occur:

```
Jun 25 21:10:07.892: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x613EC03C
reading 0xC
Jun 25 21:10:07.892: %ALIGN-3-TRACE: -Traceback= 613EC03C 613EA290 613EB2A8 613EB578
613EB848 613EB98C 60632C2C 60632C18
Jun 25 21:10:07.892: %ALIGN-3-TRACE: -Traceback= 613EC040 613EA290 613EB2A8 613EB578
613EB848 613EB98C 60632C2C 60632C18
Jun 25 21:10:07.892: %ALIGN-3-TRACE: -Traceback= 61415114 6140C450 6140C4C4 6140C668
6140DCF0 61408BAC 6140A240 60632C2C
Jun 25 21:10:07.892: %ALIGN-3-TRACE: -Traceback= 61415134 6140C450 6140C4C4 6140C668
6140DCF0 61408BAC 6140A240 60632C2C
Jun 25 21:10:07.892: %ALIGN-3-TRACE: -Traceback= 6140514C 614051A4 61415164 6140C450
6140C4C4 6140C668 6140DCF0 61408BAC
Jun 25 21:10:07.892: %ALIGN-3-TRACE: -Traceback= 61405158 614051A4 61415164 6140C450
6140C4C4 6140C668 6140DCF0 61408BAC
Jun 25 21:10:07.892: %ALIGN-3-TRACE: -Traceback= 6140515C 614051A4 61415164 6140C450
6140C4C4 6140C668 6140DCF0 61408BAC
```

  There are no known workarounds.

- CSCdy02662

  A router may reload when two simultaneous Telnet sessions are used to modify the traffic shaping parameters on a virtual circuit (VC) class.

  This symptom is observed on a Cisco 7200 router and a Cisco Node Route Processor (NRP).

  There are no known workarounds.

- CSCdy07358

  A 7200 router running 12.1(15.5) configured as a LNS in a VPDN environment may suffer alignment errors in the ipfrag_init function.

  The problem does not have any adverse reaction on the router but could impact the performance slightly.

  There are no known workarounds.

- CSCdy15222

  A routed bridge encapsulation (RBE) client is allowed to continue using a lease even after the lease has expired if users have statically configured the address to the device before it expires.

  This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(3.1)T or Release 12.2(2)B. The symptom has also been reproduced in Cisco IOS Release 12.2(11.7)T and Release 12.2(4)B4.

  Workaround: Configure the Address Resolution Protocol (ARP) timeout to 50 seconds or fewer.

Caution For a large number of RBE users, this workaround could cause a very high CPU utilization, which makes this workaround unsuitable.

- CSCdy18641

  A router may reload unexpectedly when a Layer 2 Tunneling Protocol (L2TP) connection is established.

  This symptom is observed on a Cisco 7401ASR router that is used as a Layer 2 Tunneling Protocol (L2TP) network server (LNS).

  There are no known workarounds.

- CSCdy31671

  A 7401 with large number of pvcs to create using “range pvc” configuration on atm sub-interfaces may take a long time to boot.

  There are no known workarounds.

- CSCin16553

  SSG box can reset when it gets an invalid prepaid quota from billing server.

  This happens only when ssg gets invalid response from the billing server.

  Workaround: Billing server should only return a valid prepaid quota.

Open Caveats—Cisco IOS Release 12.2(4)B5

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)B5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(4)B5.

Resolved Caveats—Cisco IOS Release 12.2(4)B5

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)B5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu46694

  A Cisco 7500 router may experience some packet loss between hosts after Cisco Express Forwarding (CEF) is enabled.

  There are no known workarounds.

- CSCdu57873

  This problem is observed when faulty servers respond to RADIUS requests using a different port than the one on which they received a request.

  It can also be observed in NAT environments if the source port of a response is something other than the port for the request.

  There are no workarounds to this problem.

- CSCdu81314

  This defect occurs when a Dynamic Host Configuration Protocol (DHCP) relay agent receives a DHCP request from a client on an unnumbered interface numbered to a loopback interface that is configured with two IP addresses. With smart relay enabled, the relay agent sets the gateway address to the secondary IP address of the loopback interface and the client obtains an IP address based on this address. The relay agent adds a host route to the client with the route expiry time set to the lease time. When the same client sends a DHCPREQUEST for RENEW message and when the server replies with a DHCPACK message, the relay does not extend the route expiry time with the new lease time. This behavior causes the relay to automatically delete the route after the initial lease time expires.

  Workaround: Release the address and obtain a new address.

- CSCdv06458

  Under rare circumstances, a Cisco Catalyst 3550 switch may reload if the **show ip eigrp neighbors** EXEC command is issued repeatedly while Enhanced Interior Gateway Routing Protocol (EIGRP) adjacencies are coming up. The **show ip eigrp neighbors** EXEC command has to be issued at just the right time for this condition to occur.

  There are no known workarounds.

- CSCdv10805

  A gatekeeper may reload if the show gatekeeper **gw-type-prefix** EXEC command is entered on the gatekeeper while there is a large routing table on the gatekeeper.

  There are no known workarounds.

- CSCdv22628

  Router might crash on bootup during ATA filesystem initialization. This is only noticeable only with High end routers like 7200, 7500, GSR, ESR and so on. This was introduced by CSCdt97325 as part of inode feature commit.

  There are no known workarounds.

- CSCdv24983

  Authorization may fail in certain Large Scale Dialout (LSDO) cases.

  There are no known workarounds.

- CSCdv40395

  If stack compression is enabled on an ISDN BRI interface on a Cisco 7200 router that is running Cisco IOS Release 12.2(3), 12.2(3.6) or 12.2(5), the router may reload unexpectedly because of a bus error at a very low address.

  Workaround: Disable compression on the interface to prevent the router from reloading because of this bus error.

- CSCdv47047

  A Cisco router may reload if the Point-to-Point Tunneling Protocol (PPTP) Access Concentrator (PAC) is configured to perform compulsory tunneling. Currently, compulsory tunneling is not supported by Cisco.

  There are no known workarounds.

- CSCdv59309

  Two vulnerabilities exist in the virtual private dial-up network (VPDN) solution when Point-to-Point Tunneling Protocol (PPTP) is used in certain Cisco IOS releases prior to 12.3. PPTP is only one of the supported tunneling protocols used to tunnel PPP frames within the VPDN solution.

  The first vulnerability is a memory leak that occurs as a result of PPTP session termination. The second vulnerability may consume all interface descriptor blocks on the affected device because those devices will not reuse virtual access interfaces. If these vulnerabilities are repeatedly exploited, the memory and/or interface resources of the attacked device may be depleted.

  Cisco has made free software available to address these vulnerabilities for affected customers.

  There are no workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml

- CSCdv60768

  If the target address is longer than 92 bytes for Response Time Reporter (RTR) Domain Name System (DNS) probes, the Cisco IOS software will reload.

  Workaround: Avoid looking up host names that are longer than 92 bytes.

- CSCdv63941

  A Cisco 7200VXR router with a Network Services Engine (NSE-1) may display incorrect NetFlow statistics after NetFlow is enabled.

  Workaround: Disable Parallel Express Forwarding (PXF) using the **no ip pxf** global configuration command.

- CSCdv71453

  A Cisco router that is using IP with the Cisco Appliance Server Architecture (CASA) enabled may reload when a client sends a large frame to the forwarding agent (FA). This large frame is then fragmented outbound to the Local Director (LD) as the IP CASA header causes the frame to be larger than the interface maximum transmission unit (MTU) between the FA and the LD. In return, the LD sends a bad IP CASA frame back to the FA, which can cause the router to reload. The following error message is displayed when this condition occurs:

  ```
  System returned to ROM by bus error at PC 0x0, address 0x0
  ```
  A Local Director caveat has been created to track this issue (CSCdv70142). The Local Director code was version 3.2.2.

  Workaround: Configure the client to send smaller packets.

- CSCdv76946

  Pings can be sent across Fast Ethernet interfaces that have 802.1q (dot1q) encapsulation configured. However, if the encapsulation on the subinterfaces are changed to Inter-Switch Link (ISL) on both of the routers, the routers may reload.

  There are no known workarounds.

- CSCdv83402

  A PPPoE/PPPoA aggregation router may unexpectedly reload when many PPP events happen in a short amount of time. The router will display a STACKLOW message before reloading.

  There are no known workarounds.

- CSCdw00924

  On a PPP multilink bundle that has multiple links, if one of the links departs from the bundle while data is enqueued for output at the bundle interface, the output mechanism on the bundle may stall, halting any further output from that bundle. The output queue on the bundle becomes full, causing packets that are forwarded to that bundle to be dropped and the affected bundle to stop transmitting packets.

  There are no known workarounds.

- CSCdw10106

  After the router has created a large number of translations, doing a **clear ip nat trans *** causes a crash.

  There are no known workarounds.

- CSCdw22714

  A Cisco router may reload if the last network statement for an area is removed from the configuration of an Open Shortest Path First (OSPF) router.

  There are no known workarounds.

- CSCdw26306

  If the **write memory** EXEC command is issued simultaneously with the **show config** privileged EXEC command or the **show running-config** EXEC command via two individual Telnet sessions by two different users, output similar to the following may be displayed:

  ```
  bGc nx
  ^@^@^@^A^A^A^@^@^A^@^@^E^@^@^@^@^@^@^@^@^@^^@^@^@^@^@^@^A^@^@^@^@^@^@^@^
  @^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
  ```

  This symptom is observed on a Cisco 7500 router that is running Cisco IOS Release 12.1(10)E.

  There are no known workarounds.

- CSCdw45491

  When Radius user profiles contain an “ip:route” VSA which itself contains VRF information, the route is parsed incorrectly. This leads to an error when the route is applied, and causes the call to go down.

  There are no known workarounds.

- CSCdw52890

  On a Cisco 7500 router that has a Versatile Interface Processor (VIP) and that is running Cisco IOS Release 12.0(19.6)S, the “VIP will crash with a %SYS-2-WATCHDOG: Process aborted on watchdog timeout Process = TurboACL” error message may be displayed when compiled access lists with noncontiguous masks are used. This behavior does not affect compiled access lists that do not have noncontiguous masks.

  Workaround: Turn off compiled access lists using the no access-list compiled global configuration command.

  Alternate workaround: Avoid using entries that have noncontiguous masks or replace such entries with single or multiple entries with contiguous masks.

- CSCdw54872

  Accounting Attribute Acct-Authentic[45] is missing in the Alive record for interim accounting. Attribute 45 is correctly included in the Stop record but not in the Alive record.

  There are no known workarounds.

- CSCdw65799

  An ATM permanent virtual connection (PVC) may remain in the "INAC" state after it is configured.

  This symptom is observed on a Cisco router that is running the c7200-p-mz.122-7.4.S image of Cisco IOS Release 12.2(7.4)S.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface to restore the PVC.

- CSCdw70202

  A watchdog-forced reload may occur if binary vendor-specific attributes (VSAs) are treated as tagged when they are actually untagged and if the **debug radius** EXEC command is enabled.

  There are no known workarounds.

- CSCdw93992

  A Cisco Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) may fail to send accounting records for a PPP over ATM (PPPoA) call after the call has been forwarded via L2TP to an L2TP network server (LNS). The LNS drops the call by sending a Call Disconnect Notification (CDN) message to the LAC.

  Workaround: Clear the virtual access interface for the call on the LAC.

- CSCdx08399

  Lightweight Directory Access Protocol (LDAP) packets may be corrupted.

  This symptom is observed on a Cisco router when Network Address Translation (NAT) is configured.

  There are no known workarounds.

- CSCdx24485

  Since CSCdx05675 and CSCdw46830, IOS no longer enforces strict matching of the MRU advertised by the LAC with the MTU of the relevant virtual template interface on the LNS. This is because the effective maximum receive unit size for a virtual access interface is not necessarily limited to the MTU size.

  For customers who want the strict behavior (e.g. to trigger LCP renegotiation on mismatch in the above described circumstances) a config knob is being added with this DDTS. The command is: **ppp mru match**.

- CSCdx24523

  When doing dialup ppp, the Framed-IP-Netmask[9] attribute is not installed correctly.

  There are no known workarounds.

- CSCdx34233

  A 7400 is used as LNS. When connected with a local user and with the command

  interface Virtual-Template1ppp timeout idle 1200, the user always ping. The idle timeout is never reset and the user was disconnect after the absolute timeout.

  In the "sh vi", the input packet increase, and not the output.

  With "no ip pxf", the problem does not appear.

  With "12.2.4b2", the problem does not appear also for the local user which doesn't use radius, there is a workaround: ppp timeout idle 1200 either for the "radius" users, the radius parameter is preferred and so is equivalent to ppp timeout idle 1200 which only work as outbound which is not a realistic workaround

- CSCdx35300

  A Gigabit Ethernet input queue may become wedged.

  This symptom is observed on a Cisco 7400 router.

  There are no known workarounds.

- CSCdx37849

  A device that is running Cisco IOS software may reload when a command is issued to display a file that contains certain character patterns.

  This symptom occurs if the file in question has a very large line. This line may have a very large continuous set of characters without any new line characters and is most likely corrupted.

  There are no known workarounds.

- CSCdx42856

  The aaa route download is not working on reload.

  This problem has been seen on a c6400 - NRP1 running 12.2(4)B3 and it has been reproduced with 12.2(4)T3.

  Workaround: To trigger the download do

  ```
  no aaa route download <time>
  aaa route download <time>
  ```
  or wait until <time> has elapsed.

- CSCdx52693

  After upgrading the IOS on a C7206VXR (NPE300) to 12.2.4B3 the router reloaded itself after 3 hours with the error message “System returned to ROM by error - a Software forced crash, PC 0x606596A4 at 09:54:11 MET Wed Apr 24 2002”

  System restarted at 09:56:05 MET Wed Apr 24 2002

  System image file is “disk1:c7200-js-mz.122-4.B3.bin”

  There are no known workarounds.

- CSCdx59130

  7200 router upgraded from 12.2(4)B2 to 12.2(4)B3, after that the router does not use the next-hop-adress specified in the config.

  Instead 12.2(4)B3 uses the next-hop-router adress for that route. Clearing the service “clear ssg service xxx” or reboot does not seem to help.

  However removing the SSG configuration completely and put it in again seems a work-around.Then everything works fine. (After every reboot this workaround should be done)

- CSCdx61867

  Symptoms are Virtual Interfaces stop being reused after being reused a few times. Problem shows up with high volume, short duration calls.

  Normal use causes this to happen.

  There are no known workarounds.

- CSCdx69995

  If Border Gateway Protocol (BGP) has more than a few hundred Virtual Private Network version 4 (VPNv4) prefixes to advertise, you may see the following message:

  ```
  %BGP-3-INSUFCHUNKS: Insufficient chunk pools for message, requested size 4204 BGP may
  not be able to advertise the VPNv4 routes.
  ```

  The conditions under which this symptom occurs are not known at this time.

  There are no known workarounds.

- CSCdx88866

  Multihop traffic is dropped rather than forwarded.

  On a 7200 NSE-1 or a 7400 with PXF enabled, multihop traffic is dropped by PXF. Multihop is not currently a support feature in the PXF path. But this traffic should be punted to the RP rather than dropped.

  Workaround: Do not enable “ip PXF”.

- CSCin12283

  SSG throws out garbled data on the console. In some cases, it might hang the router console.

  This may happen when a user logs onto a service and clicks on the service-name on SESM (it does not happen always). In the attachment (email for issue#1), the problem occurs when a user logs-on/logs-off a few number of times.

  There are no known workarounds.

- CSCin02516

  When “no ip address” on an interface, the associated adjacency entries are not removed. If the previous interface’s ip address is re-assigned in its subinterface, the adjacency entry is still pointing to the previous main interface.

  There are no known workarounds.

- CSCin10403

  The router reloads while displaying ssg tcp-redirect mappings for the command “show ssg tcp-redirect mappings”.

  This problem occurs when there are a large number of tcp-redirect mappings and the show command is entered.

  Workaround: The command “show ssg tcp-redirect mapping” should not be used when there are many users being redirected.

- CSCuk27669

  Entering the **show ip cef** EXEC command may cause a Cisco router to reload if load-shared paths change while the command executes.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(4)B4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)B4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(4)B4.

Resolved Caveats—Cisco IOS Release 12.2(4)B4

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)B4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdr00817

  During PXF switching with dynamic NAT, certain dynamically created NAT entries may get aged out even there is active flow. During PXF switching on NSE-1

  Work around: None- the result is new NAT entry gets rebuild with subsequent packets.

- CSCdu14530

  If the IP address is removed from a the PPP interface of a 7500, running 12.1E IOS, and then the IP address is added, this change is not reflected immediately in CEF. This results in 50% packet loss until the background CEF process updates the adjacency.

  Workaround: shut / no shut the PPP interface.

  Alternative workaround: Disable CEF (not an option as the 7500 is a PE router).

- CSCdu33067

  A Gigabit Ethernet interface may reset when a large number of subinterfaces are added to it using a vendor-specific virtual private network (VPN) configuration product or a script.

  Workaround: Add fewer subinterfaces at each attempt.

- CSCdu77971

  A Cisco router or access server running Cisco IOS (release 12.2T) could experience excessive CPU utilization by L2TP Daemon process when running L2TP tunneling protocol.

  There are no known workarounds.

- CSCdv46135

  With Cisco Express Forwarding (CEF) enabled, the system will experience a memory leak if an interface's primary IP address is removed.

  There are no known workarounds.

- CSCdv46891

  A system accounting record is not sent when a radius server is added or deleted, even though the cli “radius-server accounting system host-config” is turned on. This is found in 12.2(3.6)B1.

  There are no known workarounds.

- CSCdv50649

  “encapsulation aal5autoppp ...” is missing in the PVC Range and PVC in Range configuration modes. Explicit PPPoX protocol has to be configured with “protocol pppoe” or “protocol ppp virtual-template ...” to accept incoming sessions.

  There are no known workarounds.

- CSCdv62649

  The command “ip tacacs source-interface” doesn't work properly. If configured to use loopback interface for tacacs packets, router may still use interface address.

  There are no known workarounds.

- CSCdv62742

  LNS running IOS 12.2(5.7)T with “vpdn aaa attribute nas-port vpdn-nas” configured reports the wrong value for attribute 61.

  LNS reports value 1 = Sync when the LAC reports the correct physical port value 2 = ISDN

  There are no known workarounds.

- CSCdv79009

  When there is an access-class configured on VTY lines, and telnet comes into VRF interface - connection is rejected regardless to permit statements in ACL used by 'access-class'.

  There are no known workarounds.

- CSCdv88009

  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x60858850 reading 0x4 error messages may result from walking SNMP variables related to BGP4. There is no observable impact on router operation.

  There are no known workarounds.

- CSCdv90477

  Traceback and/or crash may occur when generating AAA accounting start record.

  There are no known workarounds.

- CSCdv91266

  In a Multiprotocol Label Switching (MPLS) over routed bridge encapsulation (RBE) environment, tagged packets are sent out as routed packets instead of bridged packets. MPLS support is needed for RBE interfaces.

  There are no known workarounds.

- CSCdw09685

  The following trace back is seen while doing service logon from raider, without providing host ip address whenever the router uses SSG feature:

```
12:03:11: %SYS-5-CONFIG_I: Configured from console by console
12:03:13: %SYS-2-GETBUF: Bad getbuffer, bytes= 1664592064
-Process= "IP Input", ipl= 0, pid= 44
-Traceback= 605CAE88 611FB5D0 611F8FB4 611E1B5C 611E2678 606F83F8 607222D0 607200D0
607201F0
6072036C 60616BAC 60616B98
Decoded Trace:
-------------
0x605CAE88:getbuffer(0x605cae08)+0x80
0x611FB5D0:SendCmdCode__16SSGRadiusHandlerP8paktype_UlUsP7hostkeyiiPciT7T7ii(0x611fb48
8)+0x148
0x611F8FB4:HandlePacket__16SSGRadiusHandlerP8paktype_UlUlUsUs(0x611f8da4)+0x210
0x611E1B5C:UDPInput__19SSGPacketDispatcherP8paktype_P8udptype_(0x611e1ac4)+0x98
0x611E2678:ssg_ip_udp_input(0x611e2644)+0x34
0x606F83F8:udp_process(0x606f8270)+0x188
0x607222D0:ip_enqueue(0x60722128)+0x1a8
Enter hex value: 607200D0
0x607200D0:ip_process_pak(0x6071edac)+0x1324
Enter hex value: 607201F0 6072036C 60616BAC 60616B98
0x607201F0:ip_process_input(0x60720190)+0x60
```

```
0x6072036C:ip_input(0x607202b8)+0xb4
0x60616BAC:r4k_process_dispatch(0x60616b98)+0x14
0x60616B98:r4k_process_dispatch(0x60616b98)+0x0
```

There are no known workarounds.

- CSCdw35046

  A Cisco router may reload when proxied RADIUS is used for authentication and accounting.

  There are no known workarounds.

- CSCdw40164

  When a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) (for dial-in) or an L2TP network server (LNS) (for dial-out) attempts to set up an alternate peer, the attempt may fail after the start control connect request (SCCRQ) is sent.

  There are no known workarounds.

- CSCdw42091

  router may crash if we unconfigure protocol pppoe from a VC when “test pppoe x x” command is sending PADIs. Workaround is not to unconfigure protocol pppoe when “test pppoe x x” command is active.

  There are no known workarounds.

- CSCdw52832

  A Cisco router boots the boot image in bootflash instead of booting the full Cisco IOS image from the disk if all of the following conditions are met:

  – The configuration register is set to autoboot.

  – There is no configuration in the NVRAM.

  – The **boot system** command is not in the configuration.

  – There is a complete and bootable Cisco IOS image on the disk, and there is a boot image in bootflash.

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

- CSCdw76955

  Any i82543 based PA or I/O Controller card would experience spuriours resets when higher layer protocols add/remove hw mac addresses, add/remove interfaces/sub-interfaces or change an interfaces characteristics (ipaddresses, etc.). These spurious resets may cause link flaps and protocol flaps (HSRP, OSPF, EIGRP, etc.).

  There are no known workarounds.

- CSCdx09654

  Network Address Translation (NAT) is not reset if Parallel Express Forwarding (PXF) is enabled.

  This symptom is observed on a Cisco 7200 router when NAT is used while PXF is enabled. An NAT entry is created when the data flow starts. The NAT entry is then switched by PXF with active data that is going through the translation. The data flow does not reset the timeout timer and sessions may be dropped as a result.

  When the configured timeout value is reached, the packets are punted back to the CPU for a new NAT entry. The new entry has different translation information and may cause the session to assume that the session is new causing the old session to be terminated.

  Workaround: Extend the timeout values.

- CSCdx16143

  If protocol pppoe is unconfigured when “test pppoe x x” is still sending PADIs, router may crash at crash at atm_match_vc_group.

  There are no known workarounds.

- CSCdx24528

  In 12.2T and 12.2T-base image, too much output come up when debug ppp events is turned on.

  There are no known workarounds.

- CSCdx33179

  A new instance of CSCdm05357 found in 12.2

  There are no known workarounds.

- CSCdx38190

  All users able to access SSG services.

  Workaround: Do “ssg enable” followed by “no ssg enable”.

- CSCdx56527

  A 7400 running 12.2(4)B2 or B3 doesn't release all the memory it use. There is a memory leak of around 20M/Day with 125000 session establishment over a week then it crash.

  The memory leak is triggered by AAA attempting to enable TCP (VJ) Header Compression twice within the same user session. The workaround is to disable TCP Header Compression in any Radius/AAA database.

  There are no known workarounds.

- CSCdx57829

  If you have multiple nat outside interfaces and you are pxf accelerating the nat feature. If you type the command “no ip nat outside” on a nat outside enabled interface it may disable pxf nat and go to the software path even though other nat outside enabled interfaces still exist.

  Workaround: Remove ip nat outside from all interfaces and then add back ip nat outside to re-enable pxf nat.

- CSCin03065

  When an attempt is made to create an additional session that has similar tunnel parameters that are defined by a RADIUS profile (for the same domain, the same user, or a different user), instead of creating a session under the existing tunnel, a new tunnel and a session are created. This condition is observed in Cisco IOS Release 12.2(7.4)T and occurs if the tunnel parameters are defined by RADIUS without either of the following definitions:

  Cisco-Avpair vpdn:tunnel-id = “xyz”

  or

  Tunnel-Client-Auth-ID = “xyz”

  Workaround: Define one of the following definitions under a RADIUS profile when tunnel parameters are defined:

  Cisco-Avpair vpdn:tunnel-id = “xyz”

  or

  Tunnel-Client-Auth-ID = “xyz”

- CSCin04547

  An NSE-1 or 7400 may crash with substantial churn in load balancing information.

  There are no known workarounds.

- CSCin07972

  SSG connection counters were not updated on 7400 with PXF. The downlink i/f of the host was BVI.

  Workaround: Disable pxf using the **no ip pxf** command

  Alternative workaround 1: Bind SSG to the physical ethernet i/f

  Alternative workaround 2: Give “no ip route-cache cef” on the physical ethernet i/f.

- CSCin08083

  Quota used not updated on prepaid billing server at end of session. When user is directly connected and SSG sends his MAC address in accounting records.

  There are no known workarounds.

- CSCin09724

  User will not be able to reach tunnel service. This happens only with high tunnel activation rate.

  Workaround: Clear the tunnel connection and then logon again.

- CSCin10233

  Unexpected system reset occurs when SSG processing radius proxy logonrequests at high activation rate.

  This will happen when SSG gets the duplicate radius proxy logon requests for the same msisdn. This is not a problem when SSG gets the retransmits and also this problem doesn't happen always.

  There are no known workarounds.

- CSCin10258

  Unexpected system reset may happen if traffic is there on a ssg tunnel connection when it's going down.

  This may happen when the downstream traffic is going on a ssg tunnel connection when it's getting terminated. This doesn't happen always, happens some times.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(4)B3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)B3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(4)B3.

Resolved Caveats—Cisco IOS Release 12.2(4)B3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)B3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu63623

  A Cisco 7200 series router running NAT with large numbers of NAT translations active will encounter the following high cpu at interrupt level:

  ```
  router#show proc cpu | incl util
  CPU utilization for five seconds: 100%/95%; one minute: 88%; five minutes: 88%
  ```

  The cpu at interrupt level can be reduced by issuing the following:

  ```
  router#clear ip nat translation *
  ```

  The cpu at interrupt level can also be reduced by configuring much shorter timeout intervals (than the default) for the NAT translations:

  ```
  router(config)#ip nat translation ?
    dns-timeout     Specify timeout for NAT DNS flows
    finrst-timeout  Specify timeout for NAT TCP flows after a FIN or RST
    icmp-timeout    Specify timeout for NAT ICMP flows
    max-entries     Specify maximum number of NAT entries
    port-timeout    Specify timeout for NAT TCP/UDP port specific flows
    pptp-timeout    Specify timeout for NAT PPTP flows
    syn-timeout     Specify timeout for NAT TCP flows after a SYN and no further
                    data
    tcp-timeout     Specify timeout for NAT TCP flows
    timeout         Specify timeout for dynamic NAT translations
    udp-timeout     Specify timeout for NAT UDP flows
  ```

  There are no known workarounds.

- CSCdu66646

  On a Cisco 7200 series router, issuing the **show ip nat translations tcp verbose** command with over 20,000 TCP translations active on a router may cause a software watchdog to timeout and terminate the process, causing the router to reload.

  There are no known workarounds.

- CSCdu81007

  The Cisco Express Forwarding (CEF) table is not updated properly when the IP address of an interface changes. The new IP address is added to the CEF table but the old one is not removed. If subinterfaces are used, the old ones remain in the CEF table even after the subinterfaces are removed.

  Workaround: When you issue the **shut** command on the subinterface before changing the address, the IP address is correctly deleted from the CEF tables.

- CSCdu81936

  On a Cisco router, an ARP packet received by the router that has the router's own interface address, but with a different MAC address, can overwrite the router's own MAC address in the ARP table, causing that interface to stop sending and receiving traffic. This attack is successful only against interfaces on the Ethernet segment that is local to the attacking host.

  Workaround: Hard-code the interface's ARP table entry by using the **arp** *ip-address hardware-address type [alias]* command. This entry will remain in the ARP table until the **clear arp** command is issued.

- CSCdv02925

  A Cisco router may have a memory leak whenever a SNMP walk is performed in the csCugInterlockCodeTable of the CISCO-ATM-SWITCH-CUG-MIB.

  There are no known workarounds.

- CSCdv22980

  A Cisco routers running NAT may crash while attempting to access the low address. This problem is triggered by an attempt to allocate memory at the interrupt path.

  There are no known workarounds.

- CSCdv25288

  On a Cisco router, a memory alignment error may occur on an ISDN PRI when a forced disconnection is performed on an ISDN call.

  There are no known workarounds.

- CSCdv30101

  A Cisco 7206VXR router running Cisco IOS Release 12.2(5) may experience a software-forced reload in the “IP NAT Ager” process and a watchdog timeout.

  There are no known workarounds.

- CSCdv37414

  A Cisco 7200 router running Cisco IOS Release 12.2(3) may experience packet loss if Cisco Express Forwarding (CEF) is configured over an Inter-Switch Link (ISL) trunk configured that is configured on a PA-2FE-FX Two-Port Fast Ethernet port adaptor.

  There are no known workarounds.

- CSCdv38563

  On a Cisco router, the Network access server (NAS) may fail to include attributes 90 and 91 when a router hostname is used as the tunnel ID and when the tunnel ID is not included in the user profile.

  There are no known workarounds.

- CSCdv55144

  A Cisco router with Memory Pool Mib may encounter the following problems:

  1. Improper ordering of CiscoMemoryPoolTypes

  2. GET request are handled as GET-NEXT requests

  There are no known workarounds.

- CSCdv57565

  A Cisco 7200 series router may contain vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages. The vulnerabilities can be repeatedly exploited to produce a denial of service. In most cases, workarounds are available that may mitigate the impact. These vulnerabilities are identified by various groups as VU#617947, VU#107186, OUSPG #0100, CAN-2002-0012, and CAN-2002-0013.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-non-ios-pub.shtm

- CSCdv64668

  On a Cisco router, the first PAP authentication after a PPP renegotiation triggered by a CONFREQ from the client will fail even though the RADIUS/TACACS+ server returns a success.

  There are no known workarounds.

- CSCdv89039

  A Cisco router that is running Cisco IOS Release 12.2(5) may reload because of a bus error at the ipnat_unlock_parent_entry process.

  There are no known workarounds.

- CSCdv90584

  A Cisco router running Cisco IOS Release 12.2(6.2)T on the LNS may have Radius Tunnel accounting attributes 66, 67, 81, 82, 90, 91 prefixed with Tag 00

  There are no known workarounds.

- CSCdw00722

  On a Cisco router, if the parent entry time out is less than the child entry timeout, the parent entry may not time out. This may result in the address not being freed and available for others.

  There are no known workarounds.

- CSCdw02017

  On a Cisco router, an EVENT-MIB set action may not work correctly.

  There are no known workarounds.

- CSCdw04802

  On a Cisco router, the virtual-access output counters and the RADIUS accounting data is double the real value.

  Workaround: Use xEthernet as the ingress interface.

- CSCdw19522

  When using the unnumbered DHCP relay feature on a Cisco 7200 series router, the router may unexpectedly reload after forwarding the DHCPACK from the dhcp server to the client, when using the IOS versions with the fix for CSCds73113. This crash will occur in unusual sequence if the DHCP client gets a DHCPACK from the server after approximately 5 minutes of sending initial DHCP discover, which may coincide with the binding timer expiry in the DHCP relay.

  There are no known workarounds.

- CSCdw20648

  On a Cisco 7200 series router, when rate-limit is configured on the virtual-template, all packets are punted from PXF to the RP.

  Workaround: A policymap having police must be configured instead to allow PXF acceleration.

- CSCdw27563

  On a Cisco router, the nas_ip_address is not able to report the nsp address even when configured to do so. This is only affecting 6400 platform.

  There are no known workarounds.

- CSCdw57301

  A Cisco router may experience intermittent tacacs plus authentication failures and have the following message show up in the debug tacacs:

  ```
  TPLUS(xxxx): Select Error Invalid argument
  ```

  Workaround: Reboot the router.

- CSCdw59858

  A Cisco router with PPP capabilities may reload unexpectedly after 100 days regardless of configuration. The only means of avoiding an unexpected reload is to perform periodic reloads.

  There are no workarounds.

- CSCdw61367

  On a Cisco 7200 series router, L2TP Async dialout has failed since the commit of CSCdw11765.

  There are no known workarounds.

- CSCdw61510

  For some combinations or input and output features on a Cisco 7400 series router, it is possible to create a state that causes PXF to punt all traffic.

  Workaround: Use the **no ip pxf** command.

- CSCdw62647

  A Cisco 7400 series router may have the Acct-Terminate-Cause sent out in a accounting request is NAS-Error in the 12-2.4B release image when a PPPOE user terminates its session normally in the 12-2.4B release image.

  There are no known workarounds.

- CSCdw62692

  On a Cisco 7400 series router, when the **vpdn aaa attribute nas-port vpdn-nas** global configuration command is configured, the NAS-IP-address (attribute 4) sent in accounting start and stop requests does not match. The start accounting request that is sent by the Layer 2 Tunneling Protocol (L2TP) network server (LNS) uses an IP address that corresponds to the physical interface of the L2TP access concentrator (LAC). The stop accounting request, however, sends the IP address of the interface that is specified in the **ip radius source-interface** global configuration command in the LNS or the physical interface on the LNS.

  There are no known workarounds.

- CSCdw69187

  On a Cisco 7400 series router, a c7400 or NSE-1 with the L3 cache bypass feature enabled, IOS does not recognize PA insertion or removal.

  Workaround: The L3 cache bypass feature cannot be used on a c7400 or NSE-1 when the router is subject to reconfiguration by PA insertion or removal.

- CSCdw72786

  When a Cisco 7401 or 7200 NSE-1 router is used as a L2TP Access Concentrator (LAC) or as an L2TP Network Server (LNS) for tunneling of PPPoE sessions, a ping from a Client PC to the LNS may fail if the packet size is in a critical range near an MTU size and Parallel Express Forwarding (PXF) is enabled.

  Workaround: The only available workaround is to disable PXF globally in the router by using the **no ip pxf** global configuration command.

- CSCdw78219

  On a Cisco 7200 series router, different session ID in Service Accounting Start and Service Accounting Stop/Interim records Log on to the same service twice without logging off.

  Workaround: Do not log on to the service without logging off the previous session. This problem has been fixed in the latest version of SESM for auto-services.

- CSCdw87320

  On a Cisco router, Peruser-acls that are longer than 600 bytes may attempt to be free twice. When this happens, an unexpected reload on a Cisco IOS box running flo_t may occur.

  There are no known workarounds.

- CSCdw87704

  A Cisco router used for PPPoA aggregation may fail authentication for PPP sessions even when the AAA server responded with success.

  Workaround: Clear the virtual access interface of the user.

- CSCdw89981

  A Cisco router may have a memory leak in process “PPP IPCP” when using AAA per user attributes.

  There are no known workarounds.

- CSCdw90521

  A Cisco 7200 series router running c7200-g4js-mz.122-4.B1 may unexpectedly reload with the following cause code when running SSG.

  ```
  System was restarted by error - a Software forced crash, PC 0x60658624
  ```

  There are no known workarounds.

- CSCdx04161

  A Cisco 7200 series router with a 12.2(04)B image may have the Acct-Authentic (Radius attribute 45) sent out as Remote in Radius accounting records when performing a local VPDN authorization on L2TP LAC. The correct value should be Local.

  There are no known workarounds.

- CSCin02189

  A Cisco 7400 series router may have Traceback messages appear with address 0x3c. This happens with the SSG tcp-redirect feature when redirecting an unauthenticated SSG user to a server that is on an SSG uplink interface, is not part of the SSG default-network and port-map host-key has been enabled.

  Workaround: If the interface on which the redirected server is not an uplink or if it is a part of the SSG default network or port-bundle host-key feature is not enabled, then this traceback will not occur.

- CSCin04907

  A Cisco 7200 series router may have process switched internet service packets dropped in carbon_04 image.

  Work Around: Add a network specific route either in the service profile or in the global routing table using the **ip route** command.

- CSCin05032

  In PPPoEoA setup on a Cisco 7200 series router, spurious memory access messages appear on PPPoE client while unconfiguring and reconfiguring protocol pppoe on a PVC with some sessions up.

  There are no known workarounds.

- CSCin05105

  Symptom:

  On a Cisco 7200 series router, SSG crashes while executing show running confing command.

  Workaround: Do not configure the interface as downlink, which is used for route 0.0.0.0/0

- CSCin05326

  On a Cisco 7400 series router, downstream Accounting of packets does not happen because Dot1Q encapsulation is configured on the uplink ethernet interface.

  Workaround: Avoid Dot1Q encapsulation.

- CSCin05660

  On a Cisco 7200 series router, Attribute Framed-IP-Address is not sent in the access request even when the **radius-server attribute 8 include-in-access-req** command is configured and the router is configured to an assign ip address to the peer from a local pool.

  There are no known workarounds.

- CSCuk31098

  On a Cisco router, the Acct-Authentic attribute is not included in the accounting records sent from the LAC.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(4)B2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)B2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(4)B2.

Resolved Caveats—Cisco IOS Release 12.2(4)B2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)B2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw65903

  An error can occur with management protocol processing. Please use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Open Caveats—Cisco IOS Release 12.2(4)B1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)B1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu34891

  A Cisco 7200 series router using Class-Based Weighted Fair Queueing (CBWFQ) on Parallel eXpress Forwarding (PXF), classifying by precedence in the Access Control Lists (ACLs), may have some streams repeatedly misclassified.

  There are no known workarounds.

- CSCdu44023

  On a Cisco 7200 series router, subinterface network options are only sometimes visible. When the options are not visible, the subinterface network gives an unrecognized command.

  There are no known workarounds.

- CSCdu63338

  A Cisco 7200 series router using only one AC power supply might show erroneous information about a DC power supply.

  There are no known workarounds.

- CSCdu88327

  A Cisco router may have no LINEPROTO-5-UPDOWN message printed even though the session is up.

  There are no known workarounds.

- CSCdv08146

  A Cisco 7400 series router with MultihopVirtual Private Dialup Network (VPDN) enabled may not have the input counters on its gigabit interface increment packets that were switched through the multihop interface.

- CSCdv25305

  A 7206VXR router with a NSE-1 running Cisco IOS Release 12.1(8)E2 or earlier release will not give exact netflow output when the **show ip cache flow** command is entered.

  Workaround: Disable Parallel eXpress Forwarding (PXF) using the “no ip pxf” main configuration mode.

- CSCdv37075

  A Cisco 7200 series router with a Network Services Engine (NSE-1) and Parallel eXpress Forwarding (PXF) enabled will not perform the Class-Based Weighted Fair Queueing (CBWFQ) **priority** command when the bandwidth is specified as a percentage of the interface bandwidth.

  Workaround: Configure the **priority** bandwidth explicitly.

- CSCdv53408

  A Cisco 7400 series router with an Asynchronous Transfer Mode (ATM) interface may experience Cyclic Redundancy Check (CRC) errors on input packets.

  There are no known workarounds.

- CSCdv70007

  On a Cisco 7200 series router, the two command-line interface (CLI), “sh isdn active” and “sh isdn status” do not match the active calls.

  There are no known workarounds.

- CSCdv75160

  A Cisco 7400 series router running Cisco IOS Release 12.2(02)DD may reload unexpectedly due to a bus error.

  There are no known workarounds.

- CSCdv86601

  On a Cisco 7200 series router, when a Network Address Translator (NAT) service is unbound from an uplink interface, the NAT entries for active connections to that service are not deleted.

  Workaround: The NAT translations can be cleared manually using the **clear ip nat translations *** command. This command will clear all NAT translations on the router and must be used when there are no active Service Selection Gateway (SSG) NAT connections.

- CSCdv89182

  On a Cisco router, the following error message is seen with the 12.2PB nightly build image: RADIUS: Fail to get the acct best addr on both LNS and LAC.

  This error message is not there in 12.2(04)B throttle image.

  There are no known workarounds.

- CSCdw01472

  The Gigabit Ethernet (GE) interface on a Cisco 7401 router may not count all input drops or throttles.

  When the input queue fills up on the GE interface, new input packets are dropped. These dropped packets may not be reflected in the interface input drop or throttle counts.

  There are no known workarounds.

- CSCdw01593

  On a Cisco 7200 series router, when all Network Address Translator (NAT) entries are cleared on the router using “clear ip nat translations *”, NAT entries created by Service Selection Gateway (SSG) for proxy and Layer 2 Tunnel Protocol (L2TP) tunnel service connections also get cleared. Once this happens, user traffic on NAT connections will not be address translated.

  This problem exists with all SSG images running with SSG enabled.

  Workaround: Clear individual NAT entries instead of using “clear ip nat translations *” when there are SSG NAT connections with real IP a address assigned by services.

- CSCdw04802

  On a Cisco router, the virtual-access output counters and the RADIUS accounting data is double the real value.

  Workaround: Use xEthernet as the ingress interface.

- CSCdw05784

  A Cisco 7401ASR (NSE) router running Cisco IOS software image c7400-is-mz.122-2.DD may reload unexpectedly.

  There are no known workarounds.

- CSCdw09799

  On a Cisco 7200 series router, Virtual Private Network (VPN) may download service profile twice during user login. This does not create any problems since only the service profile is downloaded twice.

  There are no known workarounds.

- CSCdw11263

  A Cisco 7200 router configured as a L2TP Network Server (LNS) might crash at dec21140_rx_interrupt, when reloaded with bidirectional traffic ON.

  Workaround: Reload the router with LOW/NO traffic.

- CSCdw12504

  A Cisco 7401ASR router running Cisco IOS release 12.2(2)DD may reload due to a bus error.

  There are no known workarounds.

- CSCdw16275

  A Cisco 7400 series router forwarding to terminal services under the Telnet banner will not a receive response.

  There are no known workarounds.

- CSCdw20470

  A Cisco 7206VXR router running Cisco IOS release 12.2(2)DD may reload due to a bus error.

  There are no known workarounds.

- CSCdw22547

  On a Cisco 7200 series router with the PA-MC-8TE1+ High Density ISDN Aggregation Port Adaptor, a serial interface created via a channel-group under a T1/E1 controller will not perform Real-Time Transport Protocol (RTP) header-compression (cRTP) when fast-switching is configured on the same interface. If fast-switching is disabled, then cRTP is active.

  Workaround: Using the **no ip route-cache** command to disable fast-switching on the interface where cRTP is configured.

- CSCdw23718

  On a Cisco 7400 series router, L2TP Network Server (LNS) will reload with a bus error when receiving a Tunnel Setup request from a L2TP Access Concentrator (LAC), when the LAC hostname is made up of 64 characters.

  Workaround: Use a short LAC hostname.

- CSCdw24835

  A Cisco 7200 series router running Cisco IOS software image c7200-p-mz.122-5.bin may reload unexpectedly due to a bus error at PC 0x6066AD8C, address 0x6120.

  There are no known workarounds.

- CSCdw46830

  In a VPDN environment, a Cisco router acting as an LNS may reject incoming calls when the ip mtu adjust feature is active and when the LAC does not advertise an MRU to the client during LCP negotiation.

  Workaround: Do not configure ip mtu adjust on the LNS

  Alternative workaround: Configure the LNS to perform LCP renegotiation

- CSCin00405

  On a Cisco router, a no radius accounting start or stop record is sent by the Network Access Solutions (NAS) when the **ppp multilink** and **aaa accounting delay-start** commands are configured.

  Workaround: Remove one of these two commands.

Resolved Caveats—Cisco IOS Release 12.2(4)B1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)B1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdt15266

  A Cisco 7100 router that is running c7100-jk2o3s-mz.121-5a.E image of Cisco IOS Release 12.1(5a)E may experience spurious memory access when an Ethernet interface is enabled.

  There are no known workarounds.

- CSCdu69834

  A Cisco router with networks where Path MTU Detection does not work properly may see TCP transactions broken when connected via an access interface that utilizes L2F or L2TP protocols. Any access servers with VPDN or MMP enabled may see this problem. The temporary workaround is to configure “mtu 1501” on the virtual-template interface.

  The default setting of the automatic MTU adjustment feature for VPDN Group is “no ip mtu adjust”.

- CSCdv06104

  A Cisco router may reload when the PPP Multilink protocol is used with Cisco Express Forwarding (CEF).

  Workaround: Disable CEF.

- CSCdv43856

  This is seen in 12.2(4.2)PI. This is just a problem in debug and will not affect any other functionality.

  There are no known workarounds.

- CSCdw52218

  On a Cisco 7400 series router with 12.2(04)B image, the **ip radius source-interface** command does not work. Even if the ip radius source-interface xyz 0 is configure, the router still sends the address of the phsical interface connected to the radius server, rather than the interface configured in the command (xyz 0).

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(4)B

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)B and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu34891

  A Cisco 7200 series router using Class-Based Weighted Fair Queueing (CBWFQ) on Parallel eXpress Forwarding (PXF), classifying by precedence in the Access Control Lists (ACLs), may have some streams repeatedly misclassified.

  There are no known workarounds.

- CSCdu44023

  On a Cisco 7200 series router, subinterface network options are only sometimes visible. When the options are not visible, the subinterface network gives an unrecognized command.

  There are no known workarounds.

- CSCdu63338

  A Cisco 7200 series router using only one AC power supply might show erroneous information about a DC power supply.

  There are no known workarounds.

- CSCdu88327

  A Cisco router may have no LINEPROTO-5-UPDOWN message printed even though the session is up.

  There are no known workarounds.

- CSCdv08146

  A Cisco 7400 series router with MultihopVirtual Private Dialup Network (VPDN) enabled may not have the input counters on its gigabit interface increment packets that were switched through the multihop interface.

- CSCdv25305

  A 7206VXR router with a NSE-1 running Cisco IOS Release 12.1(8)E2 or earlier release will not give exact netflow output when the **show ip cache flow** command is entered.

  Workaround: Disable Parallel eXpress Forwarding (PXF) using the “no ip pxf” main configuration mode.

- CSCdv37075

  A Cisco 7200 series router with a Network Services Engine (NSE-1) and Parallel eXpress Forwarding (PXF) enabled will not perform the Class-Based Weighted Fair Queueing (CBWFQ) **priority** command when the bandwidth is specified as a percentage of the interface bandwidth.

  Workaround: Configure the **priority** bandwidth explicitly.

- CSCdv53408

  A Cisco 7400 series router with an Asynchronous Transfer Mode (ATM) interface may experience Cyclic Redundancy Check (CRC) errors on input packets.

  There are no known workarounds.

- CSCdv70007

  On a Cisco 7200 series router, the two command-line interface (CLI), “sh isdn active” and “sh isdn status” do not match the active calls.

  There are no known workarounds.

- CSCdv75160

  A Cisco 7400 series router running Cisco IOS Release 12.2(02)DD may reload unexpectedly due to a bus error.

  There are no known workarounds.

- CSCdv86601

  On a Cisco 7200 series router, when a Network Address Translator (NAT) service is unbound from an uplink interface, the NAT entries for active connections to that service are not deleted.

  Workaround: The NAT translations can be cleared manually using the **clear ip nat translations *** command. This command will clear all NAT translations on the router and must be used when there are no active Service Selection Gateway (SSG) NAT connections.

- CSCdv89182

  On a Cisco router, the following error message is seen with the 12.2PB nightly build image: RADIUS: Fail to get the acct best addr on both LNS and LAC.

  This error message is not there in 12.2(04)B throttle image.

  There are no known workarounds.

- CSCdw01472

  The Gigabit Ethernet (GE) interface on a Cisco 7401 router may not count all input drops or throttles.

  When the input queue fills up on the GE interface, new input packets are dropped. These dropped packets may not be reflected in the interface input drop or throttle counts.

  There are no known workarounds.

- CSCdw01593

  On a Cisco 7200 series router, when all Network Address Translator (NAT) entries are cleared on the router using “clear ip nat translations *”, NAT entries created by Service Selection Gateway (SSG) for proxy and Layer 2 Tunnel Protocol (L2TP) tunnel service connections also get cleared. Once this happens, user traffic on NAT connections will not be address translated.

  This problem exists with all SSG images running with SSG enabled.

  Workaround: Clear individual NAT entries instead of using “clear ip nat translations *” when there are SSG NAT connections with real IP a address assigned by services.

- CSCdw04802

  On a Cisco router, the virtual-access output counters and the RADIUS accounting data is double the real value.

  Workaround: Use xEthernet as the ingress interface.

- CSCdw05784

  A Cisco 7401ASR (NSE) router running Cisco IOS software image c7400-is-mz.122-2.DD may reload unexpectedly.

  There are no known workarounds.

- CSCdw09799

  On a Cisco 7200 series router, Virtual Private Network (VPN) may download service profile twice during user login. This does not create any problems since only the service profile is downloaded twice.

  There are no known workarounds.

- CSCdw11263

  A Cisco 7200 router configured as a L2TP Network Server (LNS) might crash at dec21140_rx_interrupt, when reloaded with bidirectional traffic ON.

  Workaround: Reload the router with LOW/NO traffic.

- CSCdw12504

  A Cisco 7401ASR router running Cisco IOS release 12.2(2)DD may reload due to a bus error.

  There are no known workarounds.

- CSCdw16275

  A Cisco 7400 series router forwarding to terminal services under the Telnet banner will not a receive response.

  There are no known workarounds.

- CSCdw20470

  A Cisco 7206VXR router running Cisco IOS release 12.2(2)DD may reload due to a bus error.

  There are no known workarounds.

- CSCdw22547

  On a Cisco 7200 series router with the PA-MC-8TE1+ High Density ISDN Aggregation Port Adaptor, a serial interface created via a channel-group under a T1/E1 controller will not perform Real-Time Transport Protocol (RTP) header-compression (cRTP) when fast-switching is configured on the same interface. If fast-switching is disabled, then cRTP is active.

  Workaround: Using the **no ip route-cache** command to disable fast-switching on the interface where cRTP is configured.

- CSCdw23718

  On a Cisco 7400 series router, L2TP Network Server (LNS) will reload with a bus error when receiving a Tunnel Setup request from a L2TP Access Concentrator (LAC), when the LAC hostname is made up of 64 characters.

  Workaround: Use a short LAC hostname.

- CSCdw24835

  A Cisco 7200 series router running Cisco IOS software image c7200-p-mz.122-5.bin may reload unexpectedly due to a bus error at PC 0x6066AD8C, address 0x6120.

  There are no known workarounds.

- CSCin00405

  On a Cisco router, a no radius accounting start or stop record is sent by the Network Access Solutions (NAS) when the **ppp multilink** and **aaa accounting delay-start** commands are configured.

  Workaround: Remove one of these two commands.

Resolved Caveats—Cisco IOS Release 12.2(4)B

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)B. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv00283

  On a Cisco 7500 series router, ATM Switched Virtual Circuits (SVC) may take much longer to delete than the configured idle-timeout. If “i” is the configured idle-duration, then deletion takes more than 2*i seconds.

  There are no known workarounds.

- CSCdv78557

  On a Cisco 7200 series router, there can be tracebacks at pppatm_cleanup_newvc() in certain scenarios for PPP over Asynchronous Transfer Mode (PPPoA) testing.

  There are no known workarounds.

- CSCdv86531

  On a Cisco 7200 series router, when Service Selection Gateway (SSG) is scaled beyond a certain limit, the router may reload unexpectedly.

  To avoid this problem, keep the number of host objects less than equal to 27k (the speed at which the box is found to be stable).

  There are no known workarounds.

- CSCdw28811

  When the Class-Based Weighted Fair Queueing (CBWFQ) feature in Parallel eXpress Forwarding (PXF) on an Network Service Engine-1 (NSE-1) or a Cisco 7400 series router is used for ATM Permanent Virtual Circuits (PVCs), it wrongly apportions the bandwidths. It behaves as though the entire bandwidth for the interface is available on each PVC.

  This will not matter if either:

  1. All classes with configured bandwidths have those bandwidths configured as percentages.
  2. Both a default class is configured, and each class has a configured bandwidth as a specific value.

  There are no known workarounds.

- CSCdw29624

  A Cisco 7200 series router with an ATM subinterface will encounter the following error message if the ATM subinterface is in the shutdown state:

  ```
  %ATMFAILMODIFYVC
  ```
  There are no known workarounds.

- CSCin00170

  A Cisco 7200 NSE-1 and a Cisco 7400 series router may experience Layer 2 Tunneling Protocol (L2TP) packet loss on L2TP Network Server (LNS) with Parallel eXpress Forwarding (PXF) enabled.

  Workaround: Upgrade to a Cisco IOS Release 12.2(4)B or later image.

- CSCin00381

  On a Cisco 7200 series router, using the **no dial pool-member** command causes the router to hang.

  There are no known workarounds.

Related Documentation

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

Documentation is available as printed manuals or electronic documents.

Use these release notes with these documents:

Release-Specific Documents

For Use in T Train and Special Train Release Notes

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2**

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

  Technical Documents

- *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2 B" in these release notes, see *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2 and Cisco IOS Release 12.2 T.

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2**: **Release Notes: Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **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 12.2(15)B 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 12.2**: **New Feature Documentation**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **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 12.2**: **Configuration Guides and Command References**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**

Cisco IOS Release 12.2 Documentation Set Contents

Table 26 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

Note You can find the most current Cisco IOS documentation on Cisco.com 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 12.2**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**

Table 26 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference*, Volume 1 of 2 • *Cisco IOS Bridging and IBM Networking Command Reference*, Volume 2 of 2	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide: Dial Access* • *Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications* • *Cisco IOS Dial Technologies Command Reference*, Volume 1 of 2 • *Cisco IOS Dial Technologies Command Reference*, Volume 2 of 2	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference*, Volume 1 of 3: Addressing and Services • *Cisco IOS IP Command Reference*, Volume 2 of 3: Routing Protocols • *Cisco IOS IP Command Reference*, Volume 3 of 3: Multicast	IP Addressing IP Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX

Table 26 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service

Table 26 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • New Features in Release 12.2 T • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)	

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 156.