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

January 24, 2007

Cisco IOS Release 12.2(13)ZD4

OL-3833-35

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(13)ZD4. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(13)ZD4, see the "Caveats for Cisco IOS Release 12.2 ZD" section on page 11 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.

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

Contents

These release notes describe the following topics:

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(13)ZD4

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
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7200-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	20 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7200-jk9s-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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	20 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	32 MB	128 MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7400-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	32 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7400-jk9s-mz	20 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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	20 MB	128 MB	RAM

Table 2 Images and Memory Recommendations for Cisco IOS Release 12.2(13)ZD3

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
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7200-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	20 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7200-jk9s-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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	20 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	32 MB	128 MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7400-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	32 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7400-jk9s-mz	20 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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	20 MB	128 MB	RAM

Table 3 Images and Memory Recommendations for Cisco IOS Release 12.2(13)ZD2

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
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7200-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	20 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7200-jk9s-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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	20 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	32 MB	128 MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7400-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	32 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7400-jk9s-mz	20 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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	20 MB	128 MB	RAM

Table 4 Images and Memory Recommendations for Cisco IOS Release 12.2(13)ZD1

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
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7200-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	20 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7200-jk9s-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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	20 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	32 MB	128 MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7400-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	32 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7400-jk9s-mz	20 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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	20 MB	128 MB	RAM

Table 5 Images and Memory Recommendations for Cisco IOS Release 12.2(13)ZD

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
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7200-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	20 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7200-jk9s-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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7200-g4js-mz	20 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	32 MB	128 MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7400-ik9o3s-mz	20 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	32 MB	128 MB	RAM
		Enterprise IPSec 3DES	c7400-jk9s-mz	20 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
	Enterprise SSG Standard Feature Set	Enterprise SSG	c7400-g4js-mz	20 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(13)ZD4 supports the following Cisco 7000 family platforms:

- Cisco 7200 series routers
- Cisco 7400 series routers

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 8.

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(13)ZD4:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 ZD Software (c7200-is-mz), Version 12.2(13)ZD4, 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

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 ZD.

New Hardware Features in Cisco IOS Release 12.2(13)ZD4

There are no new hardware features supported in Cisco IOS Release 12.2(13)ZD4.

New Software Features in Cisco IOS Release 12.2(13)ZD4

There are no new software features supported in Cisco IOS Release 12.2(13)ZD4.

New Hardware Features in Cisco IOS Release 12.2(13)ZD3

There are no new hardware features supported in Cisco IOS Release 12.2(13)ZD3.

New Software Features in Cisco IOS Release 12.2(13)ZD3

There are no new software features supported in Cisco IOS Release 12.2(13)ZD3.

New Hardware Features in Cisco IOS Release 12.2(13)ZD2

There are no new hardware features supported in Cisco IOS Release 12.2(13)ZD2.

New Software Features in Cisco IOS Release 12.2(13)ZD2

There are no new software features supported in Cisco IOS Release 12.2(13)ZD2.

New Hardware Features in Cisco IOS Release 12.2(13)ZD1

There are no new hardware features supported in Cisco IOS Release 12.2(13)ZD1.

New Software Features in Cisco IOS Release 12.2(13)ZD1

There are no new software features supported in Cisco IOS Release 12.2(13)ZD1.

New Hardware Features in Cisco IOS Release 12.2(13)ZD

The following new hardware feature is supported in Cisco IOS Release 12.2(13)ZD:

PA-FC-1G

Platforms: Cisco 7200 series routers and Cisco 7401 routers.

The PA-FC-1G is a single-width, Peripheral Component Interconnect (PCI) port adapter designed to tunnel fibre channel frames through TCP connections, guaranteeing reliable transport of SAN traffic over IP-based WANs.

The PA-FC-1G provides a single one gigabit fibre channel interface to the external networks and a single PCI interface into 7200 VXR and 7401ASR routers. It offers an alternative technology to carry SAN traffic over long distances without requiring a dedicated fibre channel network and delivers aggregate throughput of up to 800 Mbps.

New Software Features in Cisco IOS Release 12.2(13)ZD

There are no new software features supported in Cisco IOS Release 12.2(13)ZD:

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Deprecated and Replacement MIBs

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

Table 6 Deprecated and Replacement MIBs

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

Caveats for Cisco IOS Release 12.2 ZD

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(13)ZD4.

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 7 Caveats Reference for Cisco IOS Release 12.2 ZD

DDTS Number	Open in Release	Resolved in Release
CSCdx40184		12.2(13)ZD1
CSCdy61597		12.2(13)ZD1
CSCdz19249	12.2(13)ZD	
CSCdz39220	12.2(13)ZD	
CSCdz44675	12.2(13)ZD	
CSCea13954	12.2(13)ZD	
CSCea13987		12.2(13)ZD
CSCea19885		12.2(13)ZD1
CSCea27536		12.2(13)ZD1
CSCea28450		12.2(13)ZD1
CSCea32240		12.2(13)ZD1
CSCea33065		12.2(13)ZD1

Table 7 Caveats Reference for Cisco IOS Release 12.2 ZD

CSCea36231		12.2(13)ZD1
CSCea46342		12.2(13)ZD1
CSCea51030		12.2(13)ZD1
CSCea51076		12.2(13)ZD1
CSCea54851		12.2(13)ZD1
CSCeb78836		12.2(13)ZD1
CSCed21717		12.2(13)ZD1
CSCed27956		12.2(13)ZD1
CSCed38527		12.2(13)ZD1
CSCef67682		12.2(13)ZD
CSCei61732		12.2(13)ZD4
CSCei76358		12.2(13)ZD4
CSCin56408		12.2(13)ZD1
CSCsa81379		12.2(13)ZD2
CSCef68324		12.2(13)ZD3

Open Caveats—Cisco IOS Release 12.2(13)ZD4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(13)ZD4 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(13)ZD4.

Resolved Caveats—Cisco IOS Release 12.2(13)ZD4

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(13)ZD4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei61732

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

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

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

- CSCei76358

  Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability.

Open Caveats—Cisco IOS Release 12.2(13)ZD3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(13)ZD3 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(13)ZD3.

Resolved Caveats—Cisco IOS Release 12.2(13)ZD3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(13)ZD3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef68324

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

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

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

Open Caveats—Cisco IOS Release 12.2(13)ZD2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(13)ZD2 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(13)ZD2.

Resolved Caveats—Cisco IOS Release 12.2(13)ZD2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(13)ZD2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsa81379

  NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
```

```
cnfFeatureTable              1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry              1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType               1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot               1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive             1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches           1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches           1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges      1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

Open Caveats—Cisco IOS Release 12.2(13)ZD1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(13)ZD1 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(13)ZD1.

Resolved Caveats—Cisco IOS Release 12.2(13)ZD1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(13)ZD1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx40184

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCdy61597

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea19885

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea27536

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea28450

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCeb78836

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCed21717

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCed27956

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

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

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

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

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

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

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

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCin56408

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Open Caveats—Cisco IOS Release 12.2(13)ZD

This section documents possible unexpected behavior by Cisco IOS Release 12.2(13)ZD and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz19249

  When routing config is removed and added again the passive-interface fcpa6/0 command is removed from the config. This needs to be added again to disallow all routing on this interface.

  On boot up the router automatically disables routing on the fcpa interface by changing the corresponding flag in software. If the user removes the router config he reverts this flag and hence needs to add it back by with the command mentioned above in order to disable routing on the fcpa interface.

  Workaround: Execute the **passive-interface fcpa6/0** command under router config.

- CSCdz39220

  PA-FC-1G supports only 1Gig speed; when connected to 2Gig FC Switch ports, may not function properly - a lot of Line Protocol toggles may be experienced before the B-port comes UP.

  Auto-speed sensing has not been implemented.

  Workaround: Configure the FC switch port speed as 1Gig.

- CSCdz44675

  When switch port is disabled on the local E-port<->B-port link OR when “no ins” or “shut” or other such events happen to cause the TCP tunnel to be brought DOWN, no light will be seen by the remote Switch E-port.

  As part of bringing the FC link offline, the current implementation shuts the light off from the B-port SFP. This is because of the E-port toggling between Faulty Retry mode, No Light & In Sync states, when inter-operating with Brocade switches. When the B-port of PA-FC-1G attempts to go out of offline state (FC Link Init process) when the Brocade switch port is in Faulty Retry mode, the FC link between the B-port and E-port takes a long time to come UP.

  Workaround: This side-effect of our implementation, wherein, we shut the light off when going to offline, is harmless.

- CSCea13954

  B-port is not coming up as the “SM state” in “show fc-tunnel” is stuck in SM_FC_INIT_PENDING_ST.

  Class-F frames are suppressed on the Switch. Due to this all FC control frames are sent as Class-2 frames by, e.g., Brocade switches. These frames are not punted to the 7200 CPU for FC link (B-port) to be brought UP.

  Workaround: Switches connected to GGPA shall not be configured to suppress Class-F frames.

Resolved Caveats—Cisco IOS Release 12.2(13)ZD

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(13)ZD. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea13987

  Fabric is unstable as B-port goes up & down continuously.

  E_D_TOV = 1sec & R_A_TOV = 2sec are too small for the FCIP, as network delays could be larger than 1sec over IP cloud.

  Workarounds: When the Switch E-port is connected to GGPA FC port (B-port), please use higher values for these TOVs. Suggested default values are E_D_TOV=10sec & R_A_TOV=20sec, however, please use your own discretion depending on your network requirements, such that the Fabric remains stable and network requirements are still met.

- CSCef67682

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

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

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

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

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

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

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 ZD" 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 7401 ASR Installation and Configuration Guide*
- *Cisco 7401 ASR 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(13)ZD1 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 8 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 8 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 8 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 8 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 21.