



Release Notes for Cisco IOS Release 12.3(7)XR4 on the Cisco ICS 7750

January 25, 2007

These release notes describe features and functionality of Cisco IOS Release 12.3(7)XR4 on the Cisco Integrated Communications System (ICS) 7750.



Note

When upgrading to the Cisco IOS Release 12.3(7)XR4 on the Cisco ICS 7750, you must upgrade both flash and DRAM memory. For more information, refer to [“Memory Requirements” section on page 2](#).

These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode changes, related document changes, and any other important changes. Use these release notes with the [Cross-Platform Release Notes for Cisco IOS Release 12.3](#) located on Cisco.com.

Contents

These release notes discuss the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 11](#)
- [Important Notes, page 11](#)
- [Caveats, page 11](#)
- [Open Caveats - Release 12.3\(7\)XR, page 16](#)
- [Obtaining Documentation, page 22](#)
- [Documentation Feedback, page 23](#)
- [Cisco Product Security Overview, page 23](#)
- [Obtaining Technical Assistance, page 24](#)
- [Obtaining Additional Publications and Information, page 26](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Release 12.3(7)XR4 on the Cisco ICS 7750. It includes the following sections:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 3](#)
- [Determining Your Software Release, page 9](#)
- [Feature Set Tables, page 10](#)

Memory Requirements

[Table 1](#) describes the new memory requirements as of Cisco IOS Release 12.3(7)XR4 for the Cisco IOS feature sets on analog station interface cards (ASIs) and multiservice route processor cards (MRPs) in a Cisco ICS 7750.


Note

If you intend to use Survivable Remote Site Telephony (SRST) and if you expect the amount of voice traffic to reach two full T1s (48 channels) on an MRP300, the amount of DRAM that is required on the MRP300 increases to 128 MB. Refer to [Installing Memory, PVD, and VPN Modules in ASI Cards, MRP Cards, and SPE Cards in the Cisco ICS 7750](#) for memory upgrade instructions.

Table 1 Available Software Images and Memory Requirements for ASIs and MRPs

Platform	Image Name	Image	Required Flash Memory for the MRP300, MRP3-8FXS ¹ , MRP3-16FXS	Required Flash Memory for the MRP200, ASI81, ASI160 ²	Required DRAM Memory ³	Runs From
Cisco ICS 7750	IP/Voice Plus	ics7700-sv3y-mz	64MB	Not applicable	128MB	RAM
	IP/FW/Voice Plus IPSec 56	ics7700-k8o3sv3y-mz	64MB	Not applicable	128MB	RAM
	IP/FW/Voice Plus IPSec 3DES	ics7700-k9o3sv3y-mz	64MB	Not applicable	128MB	RAM
	IP/IPX/AT/ IBM/ Voice, Plus	ics7700-bnr2sv3y-mz	64MB	Not applicable	128MB	RAM
	IP/IPX/AT/IBM/FW/ Voice, Plus IPSec 56	ics7700-bk8no3r2sv3y-mz	64MB	Not applicable	128MB	RAM
	IP/IPX/AT/IBM/FW/ Voice, Plus IPSec 3DES	ics7700-bk9no3r2sv3y-mz	64MB	Not applicable	128 MB	RAM

Table 1 Available Software Images and Memory Requirements for ASIs and MRPs (continued)

Platform	Image Name	Image	Required Flash Memory for the MRP300, MRP3-8FXS ¹ , MRP3-16FXS	Required Flash Memory for the MRP200, ASI81, ASI160 ²	Required DRAM Memory ³	Runs From
	Reduced-IP/ Analog Voice Plus ⁴	ics7700-sv12y10-mz	64MB	Not applicable	128 MB	RAM
	Reduced-IP/ Voice Plus ⁴	ics7700-sv3y10-mz	64MB	Not applicable	128 MB	RAM

1. FXS = Foreign Exchange Station.
2. Flash memory is not used for the Cisco IOS image on ASIs and MRP200s. Since onboard flash is not available on ASIs and MRP200s, a Cisco IOS compressed image resides on the system processing engine (SPE) and is downloaded to the RAM of each ASI or MRP200 before image decompression.
3. You can upgrade ASI or MRP card memory to 80 MB, 96 MB, or 128MB by installing a dual in-line memory module (DIMM) in the card DIMM slot. For memory upgrade instructions, refer to *Installing Memory, PVDM, and VPN Modules in ASI Cards, MRP Cards, and SPE Cards in the Cisco ICS 7750*.
4. This image comprises one of the voice-only packages, and does not include data networking support.

Hardware Supported

Cisco IOS Release 12.3(7)XR4 supports ASIs and MRPs in a Cisco ICS 7750. See [Table 2](#) for a description of the processor cards which are supported in the Cisco ICS 7750.

Processor Cards

[Table 2](#) lists the processor cards that can be used in the Cisco ICS 7750.

Table 2 Cisco ICS 7750 Processor Cards

Card	Card Description	Port Description
SPE	A single-board computer that runs system software applications such as ICS System Manager and Cisco CallManager.	<ul style="list-style-type: none"> • SPE200¹: No front-panel ports. • SPE310: Front-panel ports for video, keyboard, and universal serial bus (USB).
MRP200 MRP300	A voice-and-data-capable router that can carry voice traffic over an IP network and can link remote Ethernet LANs to central offices over WAN links. The multiservice route processor has two slots that support combinations of WAN interface cards (WICs), voice WAN interface cards (VWICs), and Voice interface cards (VICs). It also has two slots to support Packet Voice Data modules (PVDMs). Five versions of PVDMs are available. The MRP 300 has onboard flash memory.	Supports the data and voice interface port types listed in Table 5 .

Table 2 Cisco ICS 7750 Processor Cards (continued)

Card	Card Description	Port Description
ASI 81 MRP3-8FXS	A voice-and-data-capable router that can carry voice traffic over an IP network and can link small-to- medium-size remote Ethernet LANs to central offices over WAN links (depending on the type of card installed in its WIC/VIC/VWIC slot) and can support connections to analog telephones, fax machines, and polycoms. It also has two PVDM slots. The MRP3-8FXS has onboard flash memory.	<ul style="list-style-type: none"> • Eight FXS ports • One slot that supports the data and voice interface port types listed in Table 5
MRP3-8FXOM1	A voice-and-data-capable router that can carry voice traffic over an IP network and can link small-to- medium-size remote Ethernet LANs to central offices over WAN links (depending on the type of card installed in its WIC/VIC/VWIC slot) and can support connections to analog trunks between a Central Office (CO) and an IP telephony system. It also has two PVDM slots and onboard flash memory. See the “ Open Caveats - Release 12.3(7)XR ” section on page 16 for more information about connections to the central office.	<ul style="list-style-type: none"> • Eight FXO² ports • One slot that supports the data and voice interface port types listed in Table 5
ASI 160 MRP3-16FXS	An analog gateway that supports connections to telephones, fax machines, and polycoms. It also has two PVDM slots. The MRP3-16FXS has onboard flash memory.	Sixteen FXS ports
System alarm processor (SAP)	A module that monitors the status of the chassis, power supply modules, and fans, and feeds real-time data to the system processing engines. The SAP card delivers its data to the SPE running System Manager.	<ul style="list-style-type: none"> • Two COM ports • One console port
System switch processor (SSP)	An Ethernet switch that passes data between all system cards and to any other Ethernet switches connected to the system.	Two Ethernet 10/100 ports

1. System software release 2.1.0 or later is supported only on SPE 310s.

2. FXO = Foreign Exchange Office.

[Table 3](#) lists the number of processor cards supported by a Cisco ICS 7750.

Table 3 Number of Cards Supported in a Cisco ICS 7750 Chassis

Card	Minimum Required	Maximum Allowed
SAP	1	1
SSP	1	1
MRP	0	5
ASI	0	5
SPE310	1	5
200W power supply module	1	2

MRP and ASI Card Upgrades

You can upgrade MRP and ASI cards as follows:

- Flash Memory. MRP cards ship with 16 MB of flash memory. You can upgrade MRP card memory to 80 MB maximum by installing a flash single in-line memory module (SIMM) in the card SIMM slot.
- Memory. MRP and ASI cards ship with 64 MB of dynamic RAM (DRAM). You can upgrade MRP and ASI card memory to 128 MB maximum by installing a dual in-line memory module (DIMM) in the card DIMM slot.
- Voice and data processing power. VICs, VWICs, and FXS modules installed in MRP or ASI cards might require additional digital signal processors (DSPs) for processing heavier volumes of voice traffic. You can install Packet Voice/Data Modules (PVDMs) in one or both of the card PVDM slots to give MRP and ASI cards more processing power.

Refer to [Installing Memory, PVDM, and VPN Modules in ASI Cards, MRP Cards, and SPE Cards in the Cisco ICS 7750](#) for instructions on how to upgrade ASI and MRP cards.

Table 4 lists the part numbers to use for the required flash and DRAM memory upgrades.

Table 4 Cisco ASI and MRP Card Replacement DIMMs and PVDMs

Description	Cisco Part Number
64-MB FLASH SIMM	MEM1700-64MFS=
64-MB SDRAM DIMM	MEM1700-64D=
20-channel packet voice/fax data DSP module	PVDM-256K-20HD=

Wide Area Network Interface Cards, Voice Interface Cards, and Voice WAN Interface Cards

Table 5 lists the WICs, VICs, and VWICs that you can order in Cisco ICS 7750 MRP and ASI 81 cards. Refer to the [Cisco ICS 7750 Installation and Configuration Guide](#) and the ICS System Manager online help for configuration instructions.

Table 5 Supported WICs, VICs and VWICs

Card Description	Abbreviated Name	Support in MGCP ¹ Mode
2-port FXS voice/fax interface card	VIC-2FXS	Yes
2-port FXO voice/fax interface card	VIC-2FXO	Yes
4-port FXO voice/fax interface card with battery reversal detection and caller ID support (for the United States, Europe, and Australia) [Replaces the VIC-4FXO-M1, VIC-2FXO-M1, VIC-2FXO-M2, and VIC-2FXO-M3]	VIC2-4FXO	No MGCP support if Caller ID or battery reversal detection enabled
4-port FXO voice/fax interface card with battery reversal detection and caller ID support (for the United States)	VIC-4FXO-M1	No MGCP support if Caller ID or battery reversal detection enabled
2-port FXO voice/fax interface card with battery reversal detection and caller ID support (for the United States)	VIC-2FXO-M1	No MGCP support if Caller ID or battery reversal detection enabled
2-port FXO voice/fax interface card with battery reversal detection and caller ID support (for Europe)	VIC-2FXO-M2	No MGCP support if Caller ID or battery reversal detection enabled
2-port FXO voice/fax interface card with battery reversal detection (for Australia)	VIC-2FXO-M3	No MGCP support if Caller ID or battery reversal detection enabled

Table 5 Supported WICs, VICs and VWICs (continued)

Card Description	Abbreviated Name	Support in MGCP ¹ Mode
2-port E&M ² voice/fax interface card	VIC2-2E/M	No
2-port E&M voice/fax interface card	VIC-2E/M	No
2-port analog DID ³ voice/fax interface card	VIC-2DID	FXS mode only
4-port analog FXS/DID voice/fax interface card	VIC-4FXS/DID	FXS mode only
2-port ISDN BRI voice/fax interface card (network and terminal side) [Replaces the VIC-2BRI-NT/TE]	VIC2-2BRI-NT/TE	Yes
2-port ISDN BRI voice/fax interface card (network and terminal side)	VIC-2BRI-NT/TE	Yes
1-port T1/fractional T1 multiflex trunk with CSU/DSU	VWIC-1MFT-T1	Yes
2-port T1/fractional T1 multiflex trunk with CSU/DSU	VWIC-2MFT-T1	Yes
1-port E1/fractional E1 multiflex trunk with CSU/DSU	VWIC-1MFT-E1	Yes
2-port E1/fractional E1 multiflex trunk with CSU/DSU	VWIC-2MFT-E1	Yes
1-port serial, asynchronous and synchronous (T1/E1)	WIC-1T	Not applicable
2-port serial, asynchronous and synchronous (T1/E1)	WIC-2T	Not applicable
2-port serial, low speed (up to 128 kbps), asynchronous and synchronous	WIC-2A/S	Not applicable
1-port ISDN ⁴ BRI ⁵ (S/T interface)	WIC-1B-ST	Not applicable
1-port ISDN BRI with integrated NT1 (U interface)	WIC-1B-U	Not applicable
1-port, four-wire 56-kbps CSU/DSU ⁶	WIC-1DSU-56K4	Not applicable
1-port, T1/fractional T1 CSU/DSU	WIC-1DSU-T1	Not applicable

1. MGCP = Media Gateway Control Protocol
2. E&M = Ear and Mouth
3. DID = Direct Inward Dial
4. ISDN = Integrated Services Digital Network
5. BRI = Basic Rate Interface
6. CSU/DSU = channel services unit/data services unit

Table 6 lists the combinations of WICs, VICs, and VWICs that are supported on MRP300s, MRP3-8FXOM1s, and MRP3-8FXSs, where the left column of the table shows that a T1, E1, 8-port FXO-M1, or 8-port FXS module is installed in Slot 0, and where the remaining columns of the table show the types of modules that could be installed in Slot 1 of a given type of MRP.

Table 6 Supported Combinations of WICS, VICs, and VWICs on MRP300s, MRP3-8FXOM1s, and MRP3-8FXSs

Slot 0	MRP300 (Voice Only) ¹	MRP300 (Data Only)	MRP300 (Voice and Data)	MRP3-8FXOM1	MRP3-8FXS
	Slot 1				
VWIC-1MFT-E1 (voice)	VIC-2BRI-NT/TE, VIC2-2BRI-NT/TE, VIC-2DID, VIC2-2E/M, VIC-2E/M, VIC-2FXO, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-4FXO-M1, VIC2-4FXO, VIC-2FXS, VIC-4FXS/DID	Not applicable	VWIC-1MFT-E1 (data), WIC-1T, WIC-2T, WIC-2A/S, WIC-1B-ST, WIC-1B-U, WIC-1DSU-56K4, WIC-1DSU-T1	Not applicable	Not applicable
VWIC-1MFT-T1 (voice)	VWIC-1MFT-T1 (voice), VIC-2BRI-NT/TE, VIC2-2BRI-NT/TE, VIC-2DID, VIC2-2E/M, VIC-2E/M, VIC-2FXO, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-4FXO-M1, VIC2-4FXO, VIC-2FXS, VIC-4FXS/DID	Not applicable	VWIC-1MFT-T1 (data), WIC-1T, WIC-2T, WIC-2A/S, WIC-1B-ST, WIC-1B-U, WIC-1DSU-56K4, WIC-1DSU-T1	Not applicable	Not applicable
VWIC-1MFT-T1 (data) or VWIC-1MFT-E1 (data)	Not applicable	WIC-1T, WIC-2T, WIC-2A/S, WIC-1B-ST, WIC-1B-U, WIC-1DSU-56K4, WIC-1DSU-T1	VWIC-1MFT-T1 (voice), VWIC-1MFT-E1 (voice)	Not applicable	Not applicable
VWIC-2MFT-T1 (data) or VWIC-2MFT-E1 (data)	Not applicable	Empty slot	Empty slot	Not applicable	Not applicable

Table 6 Supported Combinations of WICS, VICs, and VWICs on MRP300s, MRP3-8FXOM1s, and MRP3-8FXSs

	MRP300 (Voice Only) ¹	MRP300 (Data Only)	MRP300 (Voice and Data)	MRP3-8FXOM1	MRP3-8FXS
Slot 0	Slot 1				
VWIC-2MFT-T1 (voice) or VWIC-2MFT-E1 (voice)	Empty slot	Not applicable	Empty slot	Not applicable	Not applicable
8-port FXO-M1 module	Not applicable	Not applicable	Not applicable	VIC-2DID, VIC2-2E/M, VIC-2E/M, VIC-2-2E/M, VIC-2FXO, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-4FXO-M1, VIC2-4FXO, VIC-2FXS, VIC-4FXS/DID, VWIC-1MFT-T1 (voice), VWIC-1MFT-E1 (voice), VWIC-2MFT-T1 (1 voice, 1 data), VWIC-2MFT-E1 (1 voice, 1 data) WIC-1T, WIC-2T, WIC-2A/S, WIC-1B-ST, WIC-1B-U, WIC-1DSU-56K4, WIC-1DSU-T1	Not applicable

Table 6 Supported Combinations of WICS, VICs, and VWICs on MRP300s, MRP3-8FXOM1s, and MRP3-8FXSs

Slot 0	MRP300 (Voice Only) ¹	MRP300 (Data Only)	MRP300 (Voice and Data)	MRP3-8FXOM1	MRP3-8FXS
8-port FXS module	Not applicable	Not applicable	Not applicable	Not applicable	VIC-2DID, VIC2-2E/M, VIC-2E/M, VIC-2FXO, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-4FXO-M1, VIC2-4FXO, VIC-2FXS, VIC-4FXS/DID, VWIC-1MFT-T1 (voice), VWIC-1MFT-E1 (voice), VWIC-2MFT-T1 (1 voice, 1 data), VWIC-2MFT-E1 (1 voice, 1 data) WIC-1T, WIC-2T, WIC-2A/S, WIC-1B-ST, WIC-1B-U, WIC-1DSU-56K4, WIC-1DSU-T1

1. Up to 48 voice channels are now supported on the same MRP300, in certain configurations.

Determining Your Software Release

Complete the following steps to determine the Cisco IOS software version running on Cisco ICS 7750 ASI, MRP, or SSP cards:

-
- Step 1** On a PC, choose **Start > Run**.
- Step 2** Enter the following command to open a Telnet session, where *IP address* is the IP address of the card that you wish to verify:
- ```
telnet IP address
```
- Step 3** Enter your login password.

**Step 4** Enter the **show version** command:

```
card> show version
```

The following is some of the output that is displayed after entering the command **show version** on an ASI or MRP card:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) ICS7700 Software (ICS7700-SV3Y-M), Version 12.3(7)XR3, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
```

Additional output lines from the **show version** command include information such as the processor revision numbers, amount of available memory, hardware IDs, and partition information.

## 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 12.3(7)XR supports the same feature sets as Releases 12.2 and 12.2T, but Release 12.3(7)XR can include new features supported by the Cisco ICS 7750 platform. [Table 7](#) lists the feature sets supported by the Cisco ICS 7750.

**Table 7** Feature Sets Supported by the Cisco ICS 7750

| Image Name                                                        | Feature Set Matrix Terms                | Software Image          |
|-------------------------------------------------------------------|-----------------------------------------|-------------------------|
| Cisco ICS 7750 IOS IP, Voice, Plus                                | IP/Voice Plus                           | ics7700-sv3y-mz         |
| Cisco ICS 7750 IOS IP, FW, Voice, Plus, IPSec 56                  | IP/FW/Voice Plus IPSec 56               | ics7700-k8o3sv3y-mz     |
| Cisco ICS 7750 IOS IP, FW, Voice, Plus, IPSec, 3DES               | IP/FW/Voice Plus IPSec 3DES             | ics7700-k9o3sv3y-mz     |
| Cisco ICS 7750 IOS IP, IPX, AT, IBM, Voice, Plus                  | IP/IPX/AT/IBM/Voice Plus                | ics7700-bnr2sv3y-mz     |
| Cisco ICS 7750 IOS IP, IPX, AT, IBM, FW, Voice, Plus, IPSec 56    | IP/IPX/AT/IBM/FW/ Voice Plus IPSec 56   | ics7700-bk8no3r2sv3y-mz |
| Cisco ICS 7750 IOS IP, IPX, AT, IBM, FW, Voice, Plus, IPSec, 3DES | IP/IPX/AT/IBM/FW/ Voice Plus IPSec 3DES | ics7700-bk9no3r2sv3y-mz |
| Cisco ICS 7750 IOS Reduced IP, Analog Voice, Plus <sup>1</sup>    | Reduced-IP/Analog Voice Plus            | ics7700-sv12y10-mz      |
| Cisco ICS 7750 IOS Reduced IP, Voice, Plus <sup>1</sup>           | Reduced-IP/Voice Plus                   | ics7700-sv3y10-mz       |

1. This image comprises one of the new voice-only packages, and does not include data networking support.



### Note

For additional information about feature support for this Cisco IOS release, use the Feature Navigator. See the [“Feature Navigator”](#) section on [page 19](#) for additional information.

## New and Changed Information

There are no new hardware or software features for the Cisco ICS 7750 on Cisco IOS Release 12.3(7)XR4.

## Important Notes

The following sections contain important notes about Cisco IOS-related issues that can apply to the Cisco ICS 7750.

## Software Images on MRP and ASI Cards

All of the MRPs and ASIs in a Cisco ICS 7750 must run the same Cisco IOS image.

## Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Release 12.2 T are also in Release 12.3(7)XR. For information on caveats in Cisco IOS Release 12.2 T, refer to the *Caveats for Cisco IOS Release 12.2 T* document. For information on caveats in Cisco IOS Release 12.2, refer to the *Caveats for Cisco IOS Release 12.2* document. These documents list severity 1 and 2 caveats, and are located on Cisco.com.



**Note**

If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Technical Support: Tools & Utilities: Software Bug Toolkit**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

## Resolved Caveats - Release 12.3(7)XR4

This section documents possible unexpected behavior by Cisco IOS Release 12.3(7)XR4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg44078—A Cisco836 router may report a huge delay transmitting traffic on the two Ethernet interfaces (Ethernet 0 or 2). The problem has been observed with 12.3(7)XR3 with DMZ.  
Workaround: Administratively shut down both the Ethernet0 and Ethernet2 interfaces and then administratively bring up both these interfaces one after the other.
- CSCeg89937—Ethernet interface does not send ping replies after reload.
- CSCed03333—CBAC FTP-data sessions remain in SIS\_CLOSING state.

Workaround: Lowering the inspect FTP timeout and disabling CEF will reduce exposure. Bump certain out-of-order packets to process path for catch-up and then drop packets if unsuccessful.

- CSCee47441—CBAC inspection causes software-forced reload.

When the Cisco IOS Firewall CBAC is configured, the router may have a software-forced reload caused by one of the inspections processed. This symptom is observed when the router is part of a DMVPN hub-spoke with a Cisco VoIP phone solution deployed on it, and the router is connected to the central office over the Internet. The Cisco VoIP phone runs the SKINNY protocol.

Workaround: None.

- CSCee67450—BGP error msg trackback.

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

Cisco has made free software available to address this problem. Please see the advisory available at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>.

- CSCef81501—Crash occurs while scaling L2TPv3 Xconnect commands on subinterfaces.

When L2TPv3 tunnels are scaled and the IP Path MTU Discovery feature is enabled, a memory leak and crash may occur. This symptom is observed when multiple Xconnect statements are applied in conjunction with the IP Path MTU Discovery feature in the pseudowire class.

Workaround: Do not enable the IP Path MTU Discovery feature in an L2TPv3 configuration.

- CSCeg01740—Crash when L2TPv3 manual session delete.

A router crashes when you delete a manual static Xconnect service with L2TPv3 encapsulation.

Workaround: Do not delete a manual static Xconnect service with L2TPv3 encapsulation.

- CSCef43691—L2TPv3 and UTI sessions doing PMTUD vulnerable to spoofed ICMP paks.

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

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

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

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

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

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

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

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef44225—IPSec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets.  
See note for CSCef43691 above.
- CSCef60659—More stringent checks required for ICMP unreachable.  
See note for CSCef43691 above.
- CSCsa59600—IPSec PMTUD not working [after CSCef44225].  
See note for CSCef43691 above.
- CSCef44699—GRE and IPinIP doing PMTUD vulnerable to spoofed ICMP packets.  
See note for CSCef43691 above.
- CSCef61610—Incorrect handling of ICMPv6 messages can cause TCP performance problems.  
See note for CSCef43691 above.
- CSCef67682

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

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

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

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

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

We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml> contain fixes for this issue.

- CSCef68324  
Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

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

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

- CSCsa52807—L2TP doing PMTUD vulnerable to spoofed ICMP paks.  
See note for CSCef43691 above.
- CSCsa61864—Enhancements to L2TPv3 PMTUD may not work [Follow-up to CSCef43691]  
See note for CSCef43691 above.

## Open Caveats - Release 12.3(7)XR4

This section documents possible unexpected behavior by Cisco IOS Release 12.3(7)XR4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeh89139—IPSEC real time DNS : unable to resolve peer hostname.  
With the IPSEC realtime DNS feature, when resolving the hostname, the router tries to do a ISAKMP SA negotiation and both fail (negotiation and name resolving).

## Caveats - Release 12.3(7)XR3

There are no caveats specific to Cisco IOS Release 12.3(7)XR3 that require documentation in the release notes.

## Caveats - Release 12.3(7)XR2

There are no caveats specific to Cisco IOS Release 12.3(7)XR2 that require documentation in the release notes.

## Caveats - Release 12.3(7)XR1

There are no caveats specific to Cisco IOS Release 12.3(7)XR1 that require documentation in the release notes.

## Resolved Caveats - Release 12.3(7)XR

This section describes resolved caveats in Release 12.3(7)XR.

- CSCdu53656  
A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.  
Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.
- CSCea28131

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

- CSCec64185

When a Cisco ICS 7750 uses E1 R2 signaling with country = Argentina, problems occur with call connections.

- CSCec88384

MGCP BRI has one-way voice only. This problem does not occur with BRI under H.323.

- CSCed22834

A Cisco ICS 7750 that runs Cisco IOS Release 12.3(2)XE when E1 R2 signaling is configured might not recognize that a Telco switch is in the “blocking” state. The ICS 7750 attempts to place calls on time slots that are busied out by the Telco switch which results in a low call success rate.

- CSCed27956—TCP checks should verify ACK sequence number.

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.

- CSCed38527—TCP checks should verify SYN sequence number.

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.

- CSCed78149—Internet Control Message Protocol (ICMP) might perform Denial of Service (DoS) attacks against TCP.

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

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

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

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

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

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

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

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCsa54608

The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

Only devices running certain versions of Cisco IOS are affected.

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

This advisory will be posted at

[http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth\\_proxy.shtml](http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml).

- CSCin82407

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

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

This advisory will be posted to

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

## Open Caveats - Release 12.3(7)XR

There are no open caveats specific to Cisco IOS Release 12.3(7)XR that require documentation in the release notes.

## Related Documentation

The following sections describe the documentation available for the Cisco ICS 7750. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

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

Use these release notes with the documents listed in the following sections:

- [Release-Specific Documents, page 17](#)
- [Cisco ICS 7750 Documents, page 18](#)
- [Feature Navigator, page 19](#)
- [Cisco IOS Software Documentation Set, page 19](#)

## Release-Specific Documents



### Note

---

Defects or problems related to the Cisco ICS 7750 platform are no longer addressed or corrected in maintenance releases for IOS releases 12.2, 12.2T, and 12.3.

---

The following documents are specific to Release 12.3 and Release 12.2, and apply to Release 12.3(7)XR. They are located on Cisco.com:

- [Release Notes for Cisco IOS Release 12.3\(7\)XR](#)

To reach the *Release Notes for Cisco IOS Release 12.3(7)XR on the Cisco ICS 7750* from Cisco.com, click this path:

**Products & Services: IOS Software: Cisco IOS Software Releases 12.3: Cisco IOS Software Release 12.3(7)XR: Technical Documentation: Release Notes: Cisco ICS 7750 - Cisco IOS Release 12.3(7)XR**

- [Release Notes for Cisco IOS Release 12.3T](#)

To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.3T* from Cisco.com, click this path:

**Products & Services: IOS Software: Cisco IOS Software Releases 12.3: Cisco IOS Software Releases 12.3T: Technical Documentation: Release Notes: Cisco IOS Software Releases 12.3 T**

- [Release Notes for Cisco IOS Release 12.3](#)

To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.3* from Cisco.com, click this path:

**Products & Services: IOS Software: Cisco IOS Software Releases 12.3: Cisco IOS Software Releases 12.3: Technical Documentation: Release Notes: Cisco IOS Software Releases 12.3**

- [Release Notes for Cisco IOS Release 12.2 T](#)

To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* from Cisco.com, click this path:

**Products & Services: IOS Software: Cisco IOS Software Releases 12.2: Cisco IOS Software Releases 12.2 T: Technical Documentation: Release Notes: Cisco IOS Software Releases 12.2 T**

- [Caveats for Cisco IOS Release 12.3](#)

The *Caveats for Cisco IOS Release 12.3* and the *Caveats for Cisco IOS Release 12.3 T* documents contain caveats applicable to all platforms for all maintenance releases of Release 12.3.

To reach the caveats document from Cisco.com, click this path:

**Products & Services: IOS Software: Cisco IOS Software Releases 12.3: Cisco IOS Software Releases 12.3T: Technical Documentation: Release Notes: Cisco IOS Software Releases 12.3T**

- [Caveats for Cisco IOS Release 12.2 and 12.2 T](#)

The *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T* documents contain caveats applicable to all platforms for all maintenance releases of Release 12.2.

To reach the caveats document from Cisco.com, click this path:

**Products & Services: IOS Software: Cisco IOS Software Releases 12.2: Cisco IOS Software Releases 12.2 T: Technical Documentation: Release Notes: Cisco IOS Software Releases 12.2 T**



**Note**

If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Technical Support: Tools & Utilities: Software Bug Toolkit**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

## Cisco ICS 7750 Documents

The documents described in this section are available at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/voice/ics/index.htm>

You can click this path to reach the documents on Cisco.com.

**Products & Services: Voice Application Systems: Cisco ICS 7700 Series Integrated Communications Systems: Technical Documentation**

## Documentation Set

Printed versions of many of the platform-specific documents can be ordered as a boxed set (order number DOCS-7750=).

## Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Feature Navigator is available 24 hours a day, 7 days a week.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at [cdbadmin@cisco.com](mailto:cdbadmin@cisco.com). If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to set up an account.

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

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

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

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are available on Cisco.com—unless you specifically ordered 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. To reach the Cisco IOS software documentation set on Cisco.com, click this path:

**Products & Services: IOS Software: Cisco IOS Software Releases 12.2 Mainline: Technical Documentation: Master Indices**

### Release 12.3 Documentation Set

Table 8 describes the contents of the Cisco IOS Release 12.3 software documentation set, which is available in both electronic and printed form.



#### 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.



#### Note

Some aspects of the complete Cisco IOS Release 12.3 software documentation set might not apply to the Cisco ICS 7750.

**Table 8 Cisco IOS Release 12.3 Documentation Set**

| Books                                                                                                                                                                                                                                                                                                                                              | Major Topics                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Cisco IOS Configuration Fundamentals Configuration Guide</li> <li>Cisco IOS Configuration Fundamentals Command Reference</li> </ul>                                                                                                                                                                         | Cisco IOS User Interfaces<br>File Management<br>System Management                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <ul style="list-style-type: none"> <li>Cisco IOS Bridging and IBM Networking Configuration Guide</li> <li>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2</li> <li>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2</li> </ul>                                                                        | Transparent Bridging<br>SRB<br>Token Ring Inter-Switch Link<br>Token Ring Route Switch Module<br>RSRB<br>DLSW+<br>Serial Tunnel and Block Serial Tunnel<br>LLC2 and SDLC<br>IBM Network Media Translation<br>SNA Frame Relay Access<br>NCIA Client/Server<br>Airline Product Set<br>DSPU and SNA Service Point<br>SNA Switching Services<br>Cisco Transaction Connection<br>Cisco Mainframe Channel Connection<br>CLAW and TCP/IP Offload<br>CSNA, CMPC, and CMPC+<br>TN3270 Server |
| <ul style="list-style-type: none"> <li>Cisco IOS Dial Technologies Configuration Guide: Dial Access</li> <li>Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications</li> <li>Cisco IOS Dial Technologies Command Reference, Volume 1 of 2</li> <li>Cisco IOS Dial Technologies Command Reference, Volume 2 of 2</li> </ul> | Dial Access<br>Modem and Dial Shelf Configuration and Management<br>ISDN Configuration<br>Signaling Configuration<br>Point-to-Point Protocols<br>Dial-on-Demand Routing<br>Dial Backup<br>Dial Related Addressing Service<br>Network Access Solutions<br>Large-Scale Dial Solutions<br>Cost-Control Solutions<br>Internetworking Dial Access Scenarios                                                                                                                              |
| <ul style="list-style-type: none"> <li>Cisco IOS Interface Configuration Guide</li> <li>Cisco IOS Interface Command Reference</li> </ul>                                                                                                                                                                                                           | LAN Interfaces<br>Serial Interfaces<br>Logical Interfaces                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <ul style="list-style-type: none"> <li>Cisco IOS IP Configuration Guide</li> <li>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</li> <li>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</li> <li>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</li> </ul>                                     | IP Addressing<br>IP Services<br>IP Routing Protocols<br>IP Multicast                                                                                                                                                                                                                                                                                                                                                                                                                |
| <ul style="list-style-type: none"> <li>Cisco IOS AppleTalk and Novell IPX Configuration Guide</li> <li>Cisco IOS AppleTalk and Novell IPX Command Reference</li> </ul>                                                                                                                                                                             | AppleTalk<br>Novell IPX                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Table 8** Cisco IOS Release 12.3 Documentation Set (continued)

| Books                                                                                                                                                                                                                                  | Major Topics                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</li> <li>• Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</li> </ul> | Apollo Domain<br>Banyan VINES<br>DECnet<br>ISO CLNS<br>XNS                                                                                                                                                                     |
| <ul style="list-style-type: none"> <li>• Cisco IOS Voice, Video, and Fax Configuration Guide</li> <li>• Cisco IOS Voice, Video, and Fax Command Reference</li> </ul>                                                                   | Voice over IP<br>Call Control Signaling<br>Voice over Frame Relay<br>Voice over ATM<br>Telephony Applications<br>Trunk Management<br>Fax, Video, and Modem Support                                                             |
| <ul style="list-style-type: none"> <li>• Cisco IOS Quality of Service Solutions Configuration Guide</li> <li>• Cisco IOS Quality of Service Solutions Command Reference</li> </ul>                                                     | Packet Classification<br>Congestion Management<br>Congestion Avoidance<br>Policing and Shaping<br>Signaling<br>Link Efficiency Mechanisms                                                                                      |
| <ul style="list-style-type: none"> <li>• Cisco IOS Security Configuration Guide</li> <li>• Cisco IOS Security Command Reference</li> </ul>                                                                                             | AAA Security Services<br>Security Server Protocols<br>Traffic Filtering and Firewalls<br>IP Security and Encryption<br>Passwords and Privileges<br>Neighbor Router Authentication<br>IP Security Options<br>Supported AV Pairs |
| <ul style="list-style-type: none"> <li>• Cisco IOS Switching Services Configuration Guide</li> <li>• Cisco IOS Switching Services Command Reference</li> </ul>                                                                         | Cisco IOS Switching Paths<br>NetFlow Switching<br>Multiprotocol Label Switching<br>Multilayer Switching<br>Multicast Distributed Switching<br>Virtual LANs<br>LAN Emulation                                                    |
| <ul style="list-style-type: none"> <li>• Cisco IOS Wide-Area Networking Configuration Guide</li> <li>• Cisco IOS Wide-Area Networking Command Reference</li> </ul>                                                                     | ATM<br>Frame Relay<br>SMDS<br>X.25 and LAPB                                                                                                                                                                                    |
| <ul style="list-style-type: none"> <li>• Cisco IOS Mobile Wireless Configuration Guide</li> <li>• Cisco IOS Mobile Wireless Command Reference</li> </ul>                                                                               | General Packet Radio Service                                                                                                                                                                                                   |

**Table 8** Cisco IOS Release 12.3 Documentation Set (continued)

| Books                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Major Topics                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Cisco IOS Terminal Services Configuration Guide</li> <li>Cisco IOS Terminal Services Command Reference</li> </ul>                                                                                                                                                                                                                                                                                                                    | ARA<br>LAT<br>NASI<br>Telnet<br>TN3270<br>XRemote<br>X.28 PAD<br>Protocol Translation |
| <ul style="list-style-type: none"> <li><i>Cisco IOS Configuration Guide Master Index</i></li> <li><i>Cisco IOS Command Reference Master Index</i></li> <li>Cisco IOS Debug Command Reference</li> <li>Cisco IOS Software System Error Messages</li> <li>New Features in 12.2-Based Limited Lifetime Releases</li> <li>New Features in Release 12.2T</li> <li>Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)</li> </ul> |                                                                                       |

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

### Cisco Technical Support Website

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

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

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

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