



Release Notes for Cisco 800 and SOHO 90 Series Routers for Cisco IOS Release 12.3(4)XG2

January 19, 2005

These release notes describe new features and significant software components for the Cisco 828, 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 routers that support Cisco IOS Release 12.3 T, up to and including Release 12.3(4)XG2. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code 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\(2\)T](#) located on [Cisco.com](#) and the Documentation CD.

For a list of the software caveats that apply to Release 12.3(4)XG2, see the “[Caveats](#)” section on [page 10](#), and refer to the online [Caveats for Cisco IOS Release 12.3\(2\)T](#) document. The caveats document is updated for every 12.3 T maintenance release and is located on [Cisco.com](#).

Contents

- [System Requirements, page 2](#)
- [New and Changed Information, page 8](#)
- [Caveats, page 10](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation, page 24](#)
- [Documentation Feedback, page 25](#)
- [Obtaining Technical Assistance, page 25](#)
- [Obtaining Additional Publications and Information, page 27](#)



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(4)XG2 and includes the following sections:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 3](#)
- [Determining the Software Version, page 4](#)
- [Upgrading to a New Software Release, page 4](#)
- [Feature Set Tables, page 4](#)

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Release 12.3(4)XG2 on the Cisco 828, 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 routers.

Table 1 Recommended Memory for the Cisco 828, 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 Routers

Platform	Image Name	Feature Set	Image	Flash Memory		DRAM	
				Minimum	Recommended ¹	Minimum	Recommended
Cisco 828	Cisco 828 Series IOS IP	IP	c828-y6-mz	8 MB	8 MB	24 MB	32 MB
	Cisco 828 Series IOS IP/FW	IP/FW	c828-oy6-mz	8 MB	8 MB	24 MB	32 MB
	Cisco 828 Series IOS IP Plus	IP Plus	c828-sy6-mz	8 MB	8 MB	24 MB	32 MB
	Cisco 828 Series IOS IP/FW Plus 3DES	IP/FW Plus 3DES	c828-k9osy6-mz	8 MB	8 MB	32 MB	32 MB
Cisco 831	Cisco 831 Series IOS IP/FW2 IPsec 3DES	IP/FW2/IPsec 3DES	c831-k9o3y6-mz	8 MB	12 MB	32 MB	48 MB
	Cisco 831 Series IOS IP/FW2 Plus IPsec 3DES	IP Plus/FW2/IPsec 3DES	c831-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
Cisco 836	Cisco 836 Series IOS IP/FW2 IPsec 3DES	IP/FW2/IPsec 3DES	c836-k9o3y6-mz	8 MB	12 MB	48 MB	48 MB
	Cisco 836 Series IOS IP/FW2 Plus IPsec 3DES	IP Plus/FW2/IPsec 3DES	c836-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 836 Series IOS IP/FW2/Dial Backup Plus IPsec 3DES	IP Plus/FW2/Dial Backup IPsec 3DES	c836-k9o3s8y6-mz	12 MB	12 MB	48 MB	48 MB

Table 1 Recommended Memory for the Cisco 828, 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 Routers (continued)

Platform	Image Name	Feature Set	Image	Flash Memory		DRAM	
				Minimum	Recommended ¹	Minimum	Recommended
Cisco 837	Cisco 837 Series IOS IP/FW2 IPSec 3DES	IP/FW2/IPSec 3DES	c837-k9o3y6-mz	8 MB	12 MB	32 MB	48 MB
	Cisco 837 Series IOS IP/FW2 Plus IPSec 3DES	IP Plus/FW2/IPSec 3DES	c837-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
Cisco SOHO 91	Cisco SOHO 91 Series IOS IP/FW/3DES	IP/FW/3DES	soho91-oy1-mz	8 MB	8 MB	32 MB	32 MB
Cisco SOHO 96	Cisco SOHO 96 Series IOS IP/FW/3DES	IP/FW/3DES	soho96-k9oy1-mz	8 MB	8 MB	32 MB	32 MB
Cisco SOHO 97	Cisco SOHO 97 Series IOS IP/FW	IP/FW	soho97-oy1-mz	8 MB	8 MB	32 MB	32 MB
	Cisco SOHO 97 Series IOS IP/FW/3DES	IP/FW/3DES	soho97-k9oy1-mz	8 MB	8 MB	32 MB	32 MB

1. Recommended memory is the memory required considering future expansions.

Hardware Supported

Cisco IOS Release 12.3(4)XG2 supports the following routers:

- Cisco 828 router
- Cisco 831 router
- Cisco 836 router
- Cisco 837 router
- Cisco SOHO 91 router
- Cisco SOHO 96 router
- Cisco SOHO 97 router

For detailed descriptions of new hardware features and which features are supported on each router, see the “[New and Changed Information](#)” section on page 8. For descriptions of existing hardware features and supported modules, refer to the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 828, 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 routers, which are available on [Cisco.com](#) and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/index.htm

This URL is subject to change without notice. If it changes, point your web browser to [Cisco.com](#), and click the following path:

Technical Documentation: Routers: Fixed Config. Access Routers: <platform_name>

Determining the Software Version

To determine which version of the Cisco IOS software is currently running on your Cisco 828, 831, 836, 837, SOHO 91, SOHO96, or SOHO 97 router, log in to the router, and enter the **show version EXEC** command. The following sample output from the **show version** command indicates the version number on the second output line.

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C836 Software (C836-K9O3SY6-M), Version 12.3(4)XG2, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1) Synched to technology version 12.3(5.7)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to the *Software Installation and Upgrade Procedures* located at <http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Hardware&f=742>.

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. Release 12.3(4)XG2 supports the same feature sets as Releases 12.3 and 12.3(4)T, but Release 12.3(4)XG includes new features that are supported by the Cisco 800 series routers.



Caution

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

[Table 2](#) through [Table 8](#) list the features and feature sets that are supported in Cisco IOS Release 12.3(4)XG2.

The tables use the following conventions:

- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, “12.3(4)XG” indicates that the feature was introduced in Release 12.3(4)XG. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.
- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.



Note

These feature set tables contain only a list of selected features, which are cumulative for Release 12.3(4)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all the features in each image; additional features are listed in [Cross-Platform Release Notes for Cisco IOS Release 12.3\(4\)T](#) and in Release 12.3(4)T Cisco IOS documentation.

Table 2 Feature Set Table for the Cisco 828 Router

Feature	In	Feature Set			
		IP	IP/FW	IP Plus	IP/FW Plus 3DES
IPSec Dead Peer Detection Periodic Message Option	12.3(4)XG	No	No	No	No
SNMP Version 3 (SNMPv3)	12.3(4)XG	Yes	Yes	Yes	Yes
L2TP Client-Initiated Tunneling	12.3(4)XG	No	No	No	No
CISCO-CONFIG-COPY-MIB: FTP and RCP Support	12.3(4)XG	Yes	Yes	Yes	Yes
CISCO-CONFIG-COPY-MIB: Secure Copy Support	12.3(4)XG	Yes	Yes	Yes	Yes
Resource Reservation Protocol (RSVP)	12.3(4)XG	No	No	No	No
COPS for RSVP	12.3(4)XG	No	No	No	No
Network Time Protocol (NTP)	12.3(4)XG	No	No	Yes	Yes

Table 3 Feature Set Table for the Cisco 831 Router

Feature	In	Feature Set	
		IP/FW2 3DES	IP/FW2 Plus 3DES
IPSec Dead Peer Detection Periodic Message Option	12.3(4)XG	Yes	Yes
SNMP Version 3 (SNMPv3)	12.3(4)XG	Yes	Yes
L2TP Client-Initiated Tunneling		Yes	Yes
CISCO-CONFIG-COPY-MIB: FTP and RCP Support	12.3(4)XG	Yes	Yes
CISCO-CONFIG-COPY-MIB: Secure Copy Support	12.3(4)XG	Yes	Yes
Resource Reservation Protocol (RSVP)	12.3(4)XG	No	Yes
COPS for RSVP	12.3(4)XG	No	Yes
Network Time Protocol (NTP)		No	Yes

Table 4 Feature Set Table for the Cisco 836 Router

Feature	In	Feature Set		
		IP/FW2 3DES	IP/FW2 Plus 3DES	IP Plus/FW2/Dial Backup IPsec 3DES
IPSec Dead Peer Detection Periodic Message Option	12.3(4)XG	Yes	Yes	Yes
SNMP Version 3 (SNMPv3)	12.3(4)XG	Yes	Yes	Yes
L2TP Client-Initiated Tunneling		Yes	Yes	Yes
CISCO-CONFIG-COPY-MIB: FTP and RCP Support	12.3(4)XG	Yes	Yes	Yes
CISCO-CONFIG-COPY-MIB: Secure Copy Support	12.3(4)XG	Yes	Yes	Yes
Resource Reservation Protocol (RSVP)	12.3(4)XG	No	Yes	Yes
COPS for RSVP	12.3(4)XG	No	Yes	Yes
Network Time Protocol (NTP)	12.3(4)XG	No	Yes	Yes

Table 5 Feature Set Table for the Cisco 837 Router

Feature	In	Feature Set	
		IP/FW2 3DES	IP/FW2 Plus 3DES
IPSec Dead Peer Detection Periodic Message Option	12.3(4)XG	Yes	Yes
SNMP Version 3 (SNMPv3)	12.3(4)XG	Yes	Yes
L2TP Client-Initiated Tunneling		Yes	Yes
CISCO-CONFIG-COPY-MIB: FTP and RCP Support	12.3(4)XG	Yes	Yes
CISCO-CONFIG-COPY-MIB: Secure Copy Support	12.3(4)XG	Yes	Yes
Resource Reservation Protocol (RSVP)	12.3(4)XG	No	Yes
COPS for RSVP	12.3(4)XG	No	Yes
Network Time Protocol (NTP)	12.3(4)XG	No	Yes

Table 6 Feature Set Table for the Cisco SOHO 91 Router

Feature	In	Feature Set
		IP/FW 3DES
IPSec Dead Peer Detection Periodic Message Option	12.3(4)XG	No
SNMP Version 3 (SNMPv3)	12.3(4)XG	No
L2TP Client-Initiated Tunneling	12.3(4)XG	Yes

Table 6 Feature Set Table for the Cisco SOHO 91 Router (continued)

Feature	In	Feature Set	
		IP/FW	3DES
CISCO-CONFIG-COPY-MIB: FTP and RCP Support	12.3(4)XG	Yes	
CISCO-CONFIG-COPY-MIB: Secure Copy Support	12.3(4)XG	Yes	
Resource Reservation Protocol (RSVP)	12.3(4)XG	No	
COPS for RSVP	12.3(4)XG	No	
Network Time Protocol (NTP)	12.3(4)XG	No	

Table 7 Feature Set Table for the Cisco SOHO 96 Router

Feature	In	Feature Set	
		IP/FW	3DES
IPSec Dead Peer Detection Periodic Message Option	12.3(4)XG	No	
SNMP Version 3 (SNMPv3)	12.3(4)XG	No	
L2TP Client-Initiated Tunneling	12.3(4)XG	Yes	
CISCO-CONFIG-COPY-MIB: FTP and RCP Support	12.3(4)XG	Yes	
CISCO-CONFIG-COPY-MIB: Secure Copy Support	12.3(4)XG	Yes	
Resource Reservation Protocol (RSVP)	12.3(4)XG	No	
COPS for RSVP	12.3(4)XG	No	
Network Time Protocol (NTP)	12.3(4)XG	No	

Table 8 Feature Set Table for the Cisco SOHO 97 Router

Feature	In	Feature Set	
		IP/FW	IP/FW 3DES
IPSec Dead Peer Detection Periodic Message Option	12.3(4)XG	No	No
SNMP Version 3 (SNMPv3)	12.3(4)XG	No	No
L2TP Client-Initiated Tunneling	12.3(4)XG	Yes	Yes
CISCO-CONFIG-COPY-MIB: FTP and RCP Support	12.3(4)XG	Yes	Yes
CISCO-CONFIG-COPY-MIB: Secure Copy Support	12.3(4)XG	Yes	Yes
Resource Reservation Protocol (RSVP)	12.3(4)XG	No	No
COPS for RSVP	12.3(4)XG	No	No
Network Time Protocol (NTP)	12.3(4)XG	No	No

New and Changed Information

The following sections list the new software features supported by the Cisco 800 and SOHO 90 series routers for Release 12.3(4)XG1.

New Software Features in Release 12.3(4)XG2

The Cisco IOS Release 12.3(4)XG2 supports the same software features that are supported in the Cisco IOS Release 12.3(4)XG.

New Software Features in Release 12.3(4)XG1

The Cisco IOS Release 12.3(4)XG1 supports the same software features that are supported in the Cisco IOS Release 12.3(4)XG.

New Software Features in Release 12.3(4)XG

The following sections describe the new software features supported by the Cisco 800 and SOHO 90series routers for Release 12.3(4)XG.

IPSec Dead Peer Detection Periodic Message Option

The IPSec Dead Peer Detection Periodic Message Option feature allows you to configure your router to query the liveness of its Internet Key Exchange (IKE) peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers.

For more details, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtdpmo.htm

SNMP Version 3 (SNMPv3)

The Simple Network Management Protocol Version 3 (SNMPv3) feature is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. SNMPv3 provides the following security features:

- Message integrity—Ensuring that a packet has not been tampered with in transit
- Authentication—Determining that the message is from a valid source
- Encryption—Scrambling the contents of a packet prevents it from being seen by someone who is unauthorized to see it

For more details, refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.htm>

L2TP Client-Initiated Tunneling

The L2TP Client-Initiated Tunneling feature introduces the ability to establish client-initiated Layer 2 Tunneling Protocol (L2TP) tunnels. The client may initiate an L2TP or L2TP Version 3 (L2TPv3) tunnel to the L2TP network server (LNS) without the intermediate network access server (NAS) participating in tunnel negotiation or establishment. The benefit of this feature is that client routers now have the ability to initiate either L2TP tunnels or L2TPv3 tunnels.

For more details, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtvoltun.htm

CISCO-CONFIG-COPY-MIB: FTP and RCP Support

The CISCO-CONFIG-COPY-MIB: FTP and RCP Support feature enables use of File Transfer Protocol (FTP) and remote copy protocol (RCP) for copying configuration using SNMP.

CISCO-CONFIG-COPY-MIB: Secure Copy Support

The CISCO-CONFIG-COPY-MIB: Secure Copy Support feature enables the use of secure copy protocol (SCP) support for copying device configuration using SNMP.

Resource Reservation Protocol (RSVP)

The Resource Reservation Protocol (RSVP) is a network-control protocol that enables Internet applications to obtain special quality of service (QoS) functionalities for their data flows. RSVP is a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across the Internet will perform at the desired speed and quality.

COPS for RSVP

The Common Open Policy Service protocol (COPS) is a protocol for communicating network traffic policy information to network devices. RSVP is a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across the Internet will perform at the desired speed and quality. When combined, COPS and RSVP give network managers centralized monitoring and control of RSVP, including the abilities to.

- Refer all RSVP flow requests to an external policy server for adjudication
- Accept or reject the flow, based on the policy server decision
- Communicate to the policy servers information about flows installed on the router to policy servers to facilitate management
- Permit policy servers to remove previously installed flows in order to meet bandwidth or policy requirements

Network Time Protocol (NTP)

The Network Time Protocol (NTP) feature synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur.

For more details, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd303.htm#1001131

Cisco 836 and SOHO 96 Router Interoperability with Nokia DSLAM

The Cisco 836 and SOHO 96 router meet DSL Layer 1 requirements as documented in the *Telenor Specification Requirements for ISDN compatible ADSL modem, ATU-R*. The conformance test methods are specified in *ES 202 913 (2003-01)* and *TBR 021* January 1998.

IPv6 Support

The IP version 6 (IPv6) protocol is supported on the Cisco 830 series broadband routers from the Cisco IOS Release 12.3(4XG) forward. This IPv6 feature is supported only in the PLUS images of Cisco 830 routers.

The implementation is feature rich, with IPv6 over IP version 4 (IPv4) tunneling, dynamic IPv4 address support in 6 to 4 tunnel, native IPv6 routing, address management as well as a solid set of security features including access control list (ACL) standard and extended.

This release provides a solid platform for setting up services using the IPv6 protocol.

New Software Features in Release 12.3(4)T

For information regarding the features supported in the Cisco IOS Release 12.3(4)T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on [Cisco.com](http://www.cisco.com):

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/index.htm>

This URL is subject to change without notice. If it changes, point your web browser to [Cisco.com](http://www.cisco.com), and click the following path:

Service & Support: Technical Documents: Cisco IOS Software: Release 12.3: Release Notes: Cross-Platform Release Notes (Cisco IOS Release 12.3(4)T)

Caveats

Caveats describe unexpected behavior or defects in the 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 Cisco IOS Release 12.3(4)T are also in Release 12.3(4)XG1. For information on caveats in Cisco IOS Release 12.3(2)T, refer to the *Caveats for Cisco IOS Release 12.3(4)T* document. This document lists severity 1 and 2 caveats; the documents are located on [Cisco.com](http://www.cisco.com).



Note

If you have an account with [Cisco.com](http://www.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](http://www.cisco.com) and click **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Resolved Caveats - Release 12.3(4)XG2

This section documents possible unexpected behavior by Cisco IOS Release 12.3(4)XG2 and describes only severity 1 and 2 caveats and selected severity 3 caveats.

- CSCec59206—Bus error in NAT translating RSHELL packets.

A router may reload unexpectedly because of a bus error when it accesses a low address during the translation of TCP port 514. This is observed on a Cisco router that runs Cisco IOS Release 12.3(5) and that is configured for Network Address Translation (NAT).

Workaround

Prevent the translation of TCP port 514.

- CSCec88490—Cosmetic Display CLI Related Issues.

While giving **line-mode 2-wire ?** command in ATM mode on WIC-1SHDSL-V2, the help text displays incorrect mapping between the line number and the pins used.

Workaround

None.

- CSCed21034—atmVclTable maps all permanent virtual circuits (PVCs) to all subinterfaces.

Workaround

None.

- CSCed35253—Router crash due to corrupted data in list with Cisco IOS firewall.

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

Workaround

Disable IP Inspect and IDS.

- CSCed40563—Malicious configuration reload neighbor routers by **show cdp entry * protocol** command.

Depending upon configuration, issuing the **show cdp entry * protocol** command may cause a reload of the device.

Workaround

Disable CDP, avoid issuing the command under given circumstances, or upgrade to a fixed version of software.

- CSCed40933

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

More details can be found in the security advisory, which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.

- CSCed78149

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

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

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

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

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

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

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

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

- CSCed93836—Modifications needed to syn rst packet response.

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>.

- CSCee08584—Cisco IOS Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for Cisco’s IOS Telephony Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.

A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml>

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

This vulnerability is documented by Cisco bug ID CSCee08584.

- CSCee12666—AH SHA-1/MD5 in transport mode is broken.

On a Cisco 83X router with crypto engine accelerator enabled, the router fails to authenticate packets when AH authentication is used without any ESP in transport mode.

- CSCee39592—Cisco 831 router crashes on stress testing.
- CSCee47441—CBAC inspection causes software forced reload.

When the Cisco IOS Firewall Context-Based Access Control (CBAC) is configured, the router seems to have a software-forced reload caused by one of the inspections processed.

Workaround

None.

- CSCef46191—Unable to telnet.

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

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

Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

The Advisory is available at

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

- CSCin67568—Memory leak in CDP process with long host names.

A Cisco device experiences a memory leak in the CDP process. The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

Workaround

Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the **no cdp run** global configuration command.

- CSCdz32659—%SYS-2-MALLOCFAIL: -Process= CDP Protocol.\

Many memory allocation failure (MALLOCFAIL) messages may occur for a Cisco Discovery Protocol (CDP) process:

```
%SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
Processor, alignment 0
```

```
-Process= "CDP Protocol", ipl= 0, pid= 42
```

```
-Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C
602D0E18
```

Workaround

To prevent the symptom from occurring again, disable CDP by entering the **no cdp run** global configuration command.

- CSCin82407

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

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

This advisory will be posted to

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

Open Caveats - Release 12.3(4)XG2

There are no open caveats specific to Cisco IOS Release 12.3(4)XG2 that require documentation in the release notes.

Resolved Caveats - Release 12.3(4)XG1

This section documents possible unexpected behavior by Cisco IOS Release 12.3(4)XG1 and describes only severity 1 and 2 caveats and selected severity 3 caveats.

- CSCeb56909

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

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

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

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

- CSCec86420

When you enter the **undebug all** privileged EXEC command on a Cisco router, all traffic that passes through an encrypted generic routing encapsulation (GRE) tunnel may stop. This symptom is observed on a Cisco router that is configured with a GRE tunnel that is secured via IP Security (IPSec) and that is using Cisco Express Forwarding (CEF) switching.

Workaround

Reinitialize CEF switching by entering the **no ip cef** global configuration command followed by the **ip cef** global configuration command.

Alternate Workaround

Do not enter the **undebug all** privileged EXEC command. Rather, individually disable each **debug** command.

- CSCee06452

UTC: IPsec card: an error coming back 0x1043.

The following error message is displayed on the Cisco 831 router console:

```
%HIFN79XX-3-CMD_ERR: Hifn 79XX command returned error: (0x1043)
```

```
513624: Mar 17 15:39:43.490 UTC: %HIFN79XX-3-CMD_ERR: Hifn 79XX command returned error: (0x1043)
```

IPSECcard: an error coming back 0x1043

513625: Mar 17 15:39:43.494 UTC: IPSECcard: an error coming back 0x1043

%HIFN79XX-3-CMD_ERR: Hifn 79XX command returned error: (0x1043)

513626: Mar 17 15:39:43.494 UTC: %HIFN79XX-3-CMD_ERR: Hifn 79XX command returned error: (0x1043)

IPSECcard: an error coming back 0x1043

Workaround

None.

- CSCed34050

Cisco 837 router: Middle buffers and HIFN79xx buffer issues.

A Cisco 837 series router may encounter memory allocation failures in I/O memory.

Workaround

None.

- CSCed50556

Memory leak in crypto IKMP.

The memory that crypto Internet Key Messaging Protocol (IKMP) process is holding will increase, and if not freed, might take all the memory after some time.

- CSCed67661

Ping cannot go through right after configuring crypto map.

Workaround

None.

- CSCin71247

Software forced reload occurs in UUT when traffic is pumped.

Software forced reload occurs in Cisco 837 router unit under test (UUT) due to scheduler watch dog timeout. This happens when 64 B packets are pumped at a rate of 7217 pps.

- CSCed81346

Anti-replay fails with hardware encryption.

The Cisco 831 router with hardware encryption card fails to drop packets because of anti-replay protection.

Workaround

None.

- CSCed68575

Reload triggered in SNMP process.

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

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

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

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml>

Open Caveats - Release 12.3(4)XG1

There are no open caveats specific to Cisco IOS Release 12.3(4)XG1 that require documentation in the release notes.

Resolved Caveats - Release 12.3(4)XG

This section documents possible unexpected behavior by Cisco IOS Release 12.3(4)XG and describes only severity 1 and 2 caveats and selected severity 3 caveats.

- 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.

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

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.

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>.

Resolved Caveats - Release 12.3(4)XG

This section documents possible unexpected behavior by Cisco IOS Release 12.3(4)XG and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed01880

Not able to configure NAT TCP timeouts beyond 4194 sec.

- CSCec70367

no cns config init command causes traceback.

A traceback is seen when **no cns config initial** command is configured.

- CSCec25744

Reload when connecting spoke to spoke.

A Cisco device that functions as a spoke may reload when a spoke-to-spoke connection is terminated.

- CSCed02417

Calls to third party gateway gets rejected.

Calls made from analog phone or IP Phone to third party gateway gets rejected.

Workaround

None.

- CSCin58542

DNS support for URL filtering server command.

- CSCec51619

Static IP client spoofing address can cause local users access issues.

Static clients spoofing a server's address can cause local users to not be able to access those servers.

- CSCec41737

NAT enabled interface responding to ARP request for devices on local network.

When NAT is enabled on an interface, all the Address Resolution Protocol (ARP) requests are responded. ARP request containing a source and destination address on the same subnet (local) is not responded to by the router.

Workaround

None.

- CSCeb87091
BGP: Router will not do BGP update in PPPoE with IP CEF enabled.
Workaround
Disable IP CEF on the dialer interface by using the **no ip route-cache cef** command under the dialer interface.
- CSCed29643
Porting damage in hold timer expiration/deletion.
When a dynamic NHRP cache entry expires, the cache entry is not deleted, and can still be seen in the **show ip nhrp** command output. The cache entry remains expired, but does not disappear, causing subsequent communication with that peer to not function. Manually clearing the entry works.
- CSCed17864
Malicious static IP client can cause router-generated packets access.
Malicious static IP client can cause router-generated packets access to those address which it is spoofing.
- CSCed15931
Unidirectional TCP sequence checking.
When URL filtering feature is enabled, loading of certain sites on the web browser takes unusually long time.
Workaround
None.

Open Caveats - Release 12.3(4)XG

This section documents possible unexpected behavior by Cisco IOS Release 12.3(4)XG and describes only severity 1 and 2 caveats and selected severity 3 caveats.

- CSCed33755
IPHC:UUT fails to send RIP Update when compression is enabled.
The UUT is unable to propagate the Routing Information Protocol (RIP) updates when compression is configured on the dialer interface for PPPoE. This does not happen when Enhanced Interior Gateway Routing Protocol (EIGRP) is configured, and the routes are propagated properly.
- CSCed32369
SNMPv3: Unconfiguring does not remove from running configuration.
Even after unconfiguring the **snmp-server host** command, it is shown in the running configuration displayed using **show run** command.
- CSCed31313
Packets are not marked with PPPoE for fast and CEF switching.
The packets are marked properly with PPPoE when the service policy is attached to the WAN interface of Cisco 831 router. With fast and Cisco Express Forwarding (CEF) switching, the packets are not marked properly. When the service policy is attached to the dialer interface, the packets are marked with the process, CEF, and fast switching.

- CSCed30880
Traceback occurs for URL filtering.
- CSCec75332
Proper values not found in NHRP cache.
The **show ip nhrp** command does not show correct Next Hop Resolution Protocol (NHRP) entries after simple configuration on routers.
- CSCdy55588
Packets are not fast Switched with GRE.
When generic routing encapsulation (GRE) is enabled, fast switching of packets fails after **ip route cache** command is configured.
- CSCeb13616
The **cbQosMatchStmtStats** command output does not reflect the actual values.
- CSCin08626
TFTP fails with NAT overload when UUT listens TFTP in non-standard port.
TFTP transfer fails with Network Address Translation (NAT) overload, when router listens for TFTP protocol in a non-standard port using Port to Application Mapping (PAM) configuration.
- CSCin67341
show crypto isakmp peer command output is not proper.
- CSCin69275
The EzVPN tunnel is not brought down when IKE SAs are cleared.
On issuing **clear crypto isa** command when the Easy Virtual Private network (EzVPN) tunnel is up, the Internet Key Exchange (IKE) security associations (SAs) gets cleared but IP security (IPSec) SAs remains until the lifetime expires and the tunnel is in IPSEC_ACTIVE state.
Workaround
Use **clear crypto sa** or **clear crypto ipsec client ezvpn** commands to clear the tunnel and to renegotitate the SAs.
- CSCed70248
The Cisco 836 and Cisco SOHO 96 router does not meet the Telenor specifications.
The Cisco 836 and Cisco SOHO 96 router with firmware version 4.10.120 and Alcatel 7300 digital subscriber line access multiplexer (DSLAM) ADLT-K 12 ports line card does not meet the Telenor ADSL105 MAN specification with loop length between 3250-3500 m.
- CSCed76208
Router crashes after **write erase** and reload with configuration register 0x2102.
The router with configuration register 0x2102 crashes when reloaded after issuing the **write erase** command.
- CSCin53059
EZVPN: Router crashes while giving **show logg** command.
Unexpected router reload occurs when **show logg | include EZVPN** command is issued in the router.
- CSCed79733
Lock up and loss of line detection errors occur in Cisco 837 router.

Related Documentation

The following sections describe the documentation available for the Cisco 800 and SOHO 90 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on [Cisco.com](http://www.cisco.com) and <http://www.cisco.com/univercd/home/index.htm>.

Use these release notes with these documents:

- [Release-Specific Documents](#)
- [Platform-Specific Documents](#)
- [Cisco Feature Navigator](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on [Cisco.com](http://www.cisco.com) and <http://www.cisco.com/univercd/home/index.htm>:

- [Cross-Platform Release Notes for Cisco IOS Release 12.3\(4\)T](#)

On [Cisco.com](http://www.cisco.com) at:

Products and Solutions: Cisco IOS Software: Cisco IOS Software Releases 12.3: Instructions and Guides: Release Notes

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

Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes



Note Cross-Platform Release Notes for Cisco IOS Release 12.3 T are located on [Cisco.com](http://www.cisco.com) at or on <http://www.cisco.com/univercd/home/index.htm> at **Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cisco IOS Release 12.3 T**.

- Product bulletins, field notices, and other release-specific documents at <http://www.cisco.com/univercd/home/index.htm>
- [Caveats for Cisco IOS Release 12.3](#)

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

On [Cisco.com](http://www.cisco.com) at:

Products & Solutions: IOS Software: Cisco IOS Software Releases 12.3: Instructions and Guides: Release Notes: Release Notes for Cisco IOS Release 12.3, Part 5: Caveats

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

Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Caveats

- If you have an account on [Cisco.com](http://www.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](http://www.cisco.com) and click **Products and Solutions: Cisco IOS Software: Cisco IOS Software Releases 12.3: Troubleshooting: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

These documents are available for the Cisco 800 series routers:

On [Cisco.com](#) at:

Technical Documentation: Routers: Fixed Config. Access Routers: <platform_name>

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

Product Documentation: Routers: Fixed Config. Access Routers: <platform_name>

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To obtain updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on [Cisco.com](#). If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with [Cisco.com](#). If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on [Cisco.com](#) by following the directions found at this URL:

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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

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:

Products and Solutions: Cisco IOS Software: Cisco IOS Releases 12.3: Instructions and Guides

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

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

Cisco IOS Release 12.3 Documentation Set Contents

Table 9 lists the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form if ordered.

On [Cisco.com](http://www.cisco.com) at:

Products and Solutions: Cisco IOS Software: Cisco IOS Releases 12.3: Instructions and Guides

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

Cisco IOS Software: Cisco IOS Release 12.3

Table 9 Cisco IOS Release 12.3 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> <i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i> 	<ul style="list-style-type: none"> Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i> 	
<ul style="list-style-type: none"> <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> 	<ul style="list-style-type: none"> Transparent Bridging
<ul style="list-style-type: none"> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2: Bridging</i> 	<ul style="list-style-type: none"> SRB Token Ring Inter-Switch Link Token Ring Route Switch Module
<ul style="list-style-type: none"> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2: IBM Networking</i> 	<ul style="list-style-type: none"> 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

Table 9 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> <i>Cisco IOS Dial Technologies Configuration Guide</i> <i>Cisco IOS Dial Technologies Command Reference</i> 	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
<ul style="list-style-type: none"> <i>Cisco IOS Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS Interface and Hardware Component Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> <i>Cisco IOS IP Configuration Guide</i> <i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> <i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i> <i>Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility</i> 	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> <i>Cisco IOS Voice Configuration Library</i> <i>Cisco IOS Voice Command Reference</i> 	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Table 9 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Mobile Wireless Configuration Guide</i> • <i>Cisco IOS Mobile Wireless Command Reference</i> 	General Packet Radio Service
<ul style="list-style-type: none"> • <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i> 	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Software System Messages</i> 	

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 on the World Wide Web at this URL:

<http://www.cisco.com/cisco/web/support/index.html>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered [Cisco.com](http://www.cisco.com) users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered [Cisco.com](http://www.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 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. [Cisco.com](http://www.cisco.com) features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

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

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

Accessing all the tools on the Cisco TAC website requires a [Cisco.com](http://www.cisco.com) user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

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

- 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 online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives.

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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

Training—Cisco offers world-class networking training. Current offerings in network training are listed 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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0711R)

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

