



Release Notes for Cisco AS5300 Universal Access Servers for Cisco IOS Release 12.1 XM

February 25, 2002

Cisco IOS Release 12.1(5) XM8

78-12051-01 Rev. I0

These release notes for the Cisco AS5300 universal access servers describe the enhancements provided in Cisco IOS Release 12.1(5) XM8. These release notes are updated as needed.

For a list of the software caveats that apply to Release 12.1(5) XM8, see the [“Caveats” section on page 11](#) and *Caveats for Cisco IOS Release 12.1T* that accompanies these release notes. This caveats document is updated for every maintenance release and is also located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.1* on Cisco.com and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 6](#)
- [Important Notes, page 10](#)
- [MIBs, page 10](#)
- [Caveats, page 11](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation, page 23](#)
- [Obtaining Technical Assistance, page 24](#)



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

Introduction

The Cisco AS5300 is a versatile data communications platform that performs two functions in a single modular chassis, depending on the installed feature cards and IOS images:

- Remote Access Server
- Voice Gateway

The remote access server is intended for Internet service providers (ISPs), telecommunications carriers, and other service providers that offer managed Internet connections and medium to large sites that provide both digital and analog access to users on an enterprise network. By terminating both analog and digital calls on the same chassis simultaneously, the access server provides a clear, simple, and easy migration path from analog dial access services to digital dial access services.

The Cisco AS5300 Voice Gateway is a versatile data communications platform that provides the functions of an access server, router, and digital modem(s) in a single modular chassis. The Cisco AS5300 includes three feature card slots: one holds a T1/E1/PRI feature card, and the other two support modem feature cards or voice digital signal processor (DSP) feature cards. When equipped with modem cards, the Cisco AS5300 serves as a remote access concentrator for dial-up (modem or ISDN) Internet access. When equipped with voice feature cards and Voice IOS, the Cisco AS5300/Voice Gateway serves as a Voice over IP (VoIP) gateway. By using one slot for modems and the other for voice DSPs, the Cisco AS5300 can serve in both capacities. Modem, voice, or fax calls are routed to the appropriate cards/resources via Dialed Number Identification Service (DNIS).

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.1(5) XM8, see the [“New and Changed Information”](#) section on page 6 and the [“Related Documentation”](#) section on page 18.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.1(5) XM8 and includes the following sections:

- [Memory Recommendations, page 2](#)
- [Supported Hardware, page 3](#)
- [Determining the Software Version, page 4](#)
- [Upgrading to a New Software Release, page 4](#)
- [Microcode and Modem Code Software, page 4](#)
- [Feature Set Tables, page 5](#)

Memory Recommendations

Table 1 *Memory Recommendations for the Cisco AS5300*

Image Name	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
IP/Voice Plus	c5300-is-mz	16 MB	128 MB	RAM
IP Plus IPsec 56	c5300-is56i-mz	16 MB	128 MB	RAM

Table 1 Memory Recommendations for the Cisco AS5300 (continued)

Image Name	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Enterprise Voice Plus	c5300-js-mz	16 MB	128 MB	RAM
Enterprise Plus IPsec 56	c5300-js56i-mz	16 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.1(5) XM8 supports the Cisco AS5300. [Table 2](#) details the supported interfaces. For detailed descriptions of the new hardware features, see the [“New and Changed Information”](#) section on page 6.

Table 2 Supported Interfaces for the Cisco AS5300

Interface and Modem Cards	Product Description
Interface Cards	Ethernet RJ-45 (included with unit)
	Ethernet/Fast Ethernet (RJ-45) (included with unit)
	ISDN PRI
	E1-G.703/G.704
	Channelized T1 (4 ports) without serial support
	Channelized T1 (4 ports) with 4 serial ports
	Channelized T1 (8 ports) with 4 serial ports
	Channelized E1 (4 ports) without serial support
	Channelized E1 (4 ports) with 4 serial ports
	Channelized E1 (8 ports) with 4 serial ports
	HMM/48 channel
	HMM/54 channel
	HMM/60 channel
	DMM/48 channel
	DMM/96 channel
	DMM/108 channel
DMM/120 channel	
Interface Cards (continued)	48-Channel, TI C549-based VoIP feature card (Uses High Density AS53-VOXD DSP modules)
	60-Channel, TI C549-based VoIP feature card (Uses High Density AS53-VOXD DSP modules)
	24-Channel, TI C542-based VoIP feature card (First generation, uses AS53-6VOX DSP modules)
	48-Channel, TI C542-based VoIP feature card (First generation, uses AS53-6VOX DSP modules)

Table 2 Supported Interfaces for the Cisco AS5300 (continued)

Interface and Modem Cards	Product Description
Interface Cards	MICA modems
	Microcom 56K modems

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco AS5300, log in to the Cisco AS5300 and enter the **show version EXEC** command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.1 Software c5300-i-mz, Version 12.1(5) XM8, RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

http://www.cisco.com/warp/public/130/upgrade_index.shtml

Microcode and Modem Code Software

Microcode software images are bundled with the system software image with the exception of the Channel Interface Processor (CIP) microcode (all system software images). Bundling eliminates the need to store separate microcode images. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface processor boards.

You could have received a later version of modem code than the one bundled with the Cisco IOS software. The modem code in Flash memory is mapped to the modems. Unless you fully understand how Cisco IOS software uses modem code, it is important to keep the factory configuration.

To obtain the latest Cisco IOS software release compatible with Cisco MICA portware, refer to the *Cisco AS5x00 MICA 6-Port and 12-Port Modem Module Portware/Cisco IOS Software Compatibility Matrixes* at

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/sw_conf/sw_ports/compmat/mca12prt.htm.

The modem code release notes are on Cisco.com and the Documentation CD-ROM:

On Cisco.com at:

Technical Documents: Access Servers and Access Routers: Access Servers: Cisco AS5300: Configuration Documents for Cisco AS5300: Port Information

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300: Configuration Documents for Cisco AS5300: Port Information



Note

Cisco MICA portware 2.7.3.0 is compatible with Cisco IOS Release 12.1(5) XM8.

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 12.1(5) XM8 supports the same feature sets as Cisco IOS Release 12.1(5) T, but Cisco IOS Release 12.1(5) XM8 can include new features supported by the Cisco AS5300.



Caution

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

Table 3 lists the features and feature sets supported by the Cisco AS5300 in Cisco IOS Release 12.1(5) XM8 and uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced.



Note

This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 12.1(5) T by using the Feature Navigator tool at <http://www.cisco.com/go/fn>.

Table 3 Feature List by Feature Set for the Cisco AS5300

Feature	In	Software Images by Feature Sets			
		IP/ Voice Plus	IP Plus IPSec 56	Enter prise Plus	Enterprise Plus IPSec 56
Voice					
Enhancement to Fax Detection Feature for the Cisco AS5300	12.1(5) XM	Yes	Yes	Yes	Yes
Fax Detection for Cisco AS5300 Universal Access Servers	12.1(5) XM	Yes	Yes	Yes	Yes
H.323 Call Redirection Enhancements	12.1(5) XM	Yes	Yes	Yes	Yes
Media Gateway Control Protocol Basic CLASS and Operator Services	12.1(5) XM	Yes	Yes	Yes	Yes
SIP Diversion Header Implementation for Redirecting Number (CSCdr72341)	12.1(5) XM1	Yes	Yes	Yes	Yes
SIP Gateway Support for Third Party Call Control (CSCdr32290)	12.1(5) XM1	Yes	Yes	Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5300 for Cisco IOS Release 12.1(5) XM8.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM8

There are no new hardware and software features in the Cisco AS5300 for Cisco IOS Release 12.1(5) XM8.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM7

There are no new hardware and software features in the Cisco AS5300 for Cisco IOS Release 12.1(5) XM7.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM6

There are no new hardware and software features in the Cisco AS5300 for Cisco IOS Release 12.1(5) XM6.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM5

There are no new hardware and software features in the Cisco AS5300 for Cisco IOS Release 12.1(5) XM5.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM4

There are no new hardware and software features in the Cisco AS5300 for Cisco IOS Release 12.1(5) XM4.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM3

There are no new hardware and software features in the Cisco AS5300 for Cisco IOS Release 12.1(5) XM3.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM2

There are no new hardware and software features in the Cisco AS5300 for Cisco IOS Release 12.1(5) XM2.

New Hardware Features in Cisco IOS Release 12.1(5)XM1

There are no new hardware features in the Cisco AS5300 for Cisco IOS Release 12.1(5)XM1.

New Software Features in Cisco IOS Release 12.1(5)XM1

The following new software features are supported by the Cisco AS5300 for Cisco IOS Release 12.1(5)XM1.

SIP Diversion Header Implementation for Redirecting Number (CSCdr72341)

The SIP Diversion Header Implementation for Redirecting Number feature provides support for a new SIP header field; Call Control (CC)-Diversion. The CC-Diversion header field enables the SIP gateway to pass call control redirecting information during the call setup. Call control redirection is the redirection of a call based on a subscriber service such as call forwarding. Call redirection information is information is typically used for Unified Messaging and voice mail services to identify the recipient of a message. Call control redirection information can also be used to support applications such as automatic call distribution and enhanced telephony features such as Do Not Disturb and Caller ID.

For further details, please see:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121rel/sipcfs/hennigan.htm>.

SIP Gateway Support for Third Party Call Control (CSCdr32290)

This feature adds SDP changes for third party call control in SIP for click-to-dial, mid-call announcements, voice mail, and a timed conference bridge initiation.

For further details, please see *SIP Gateway Support for Third Party Call Control* at:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121rel/sipcfs/caribou.htm#xtocid33510>

New Hardware Features in Cisco IOS Release 12.1(5)XM

There are no new hardware features in the Cisco AS5300 for Cisco IOS Release 12.1(5)XM2.

New Software Features in Cisco IOS Release 12.1(5)XM

The following new software features are supported by the Cisco AS5300 for Cisco IOS Release 12.1(5)XM2.

Enhancement to Fax Detection Feature for the Cisco AS5300

Users can now route fax calls to a fax e-mail address based on the redirecting dialed number (RDNIS), the dialed number (DNIS), or on a user-specified string, in addition to previously existing choices. RDNIS is the telephone number that is dialed for a particular subscriber before a call is transferred, on busy or no answer, to a shared voice/fax mail access and deposit number (DNIS).

A new keyword in the session target `mailto:` command (`m`) specifies use of RDNIS as part of the fax e-mail address if RDNIS is present; otherwise, DNIS is used. Additionally, a string can be entered, which allows the fax e-mail to be sent to an address that is not necessarily based on a telephone number.

Fax Detection for Cisco AS5300 Universal Access Servers

On Cisco AS5300 gateways equipped with voice feature cards (VFCs), the fax detection feature lets service providers deploy unified communication applications where each subscriber has a single E.164 number for both voice mail and fax mail. When configured for fax detection, the gateway automatically listens to incoming calls to discriminate between voice and fax. The gateway then routes the calls to the appropriate application or server.



Note

For a complete description of the Fax Detection feature, see “Fax Detection for Cisco AS5300 Universal Access Servers” on the Cisco Web site at http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ft_snfax.htm.

H.323 Call Redirection Enhancements

The user-to-user information element (UUIE) of the facility message is used primarily for call redirection. The UUIE contains a field, `facilityReason`, that indicates the nature of the redirection. The H.323 Call Redirection Enhancements feature adds support for two of the reasons: `routeCallToGatekeeper` and `callForwarded`. It also provides a nonstandard method for using the facility message to effect call transfer.

Route Call to Gatekeeper

There are two situations in which the Cisco H.323 Gateway might receive or generate a facility message with a `routeCallToGatekeeper` reason.

- The gateway receives a facility message with `routeCallToGatekeeper` as a response to its H.225 SETUP message. Upon receiving the facility message, the Cisco H.323 Gateway attempts to route the call to the new gatekeeper, using the new IP address specified in the `alternativeAddress` field of the facility message.
 - If the IP address is not available, the gateway ignores the facility message and sends a release complete toward the original destination endpoint. The release complete message contains a `ReleaseCompleteReason` of `facilityCallDeflection`.
 - If the IP address is available, the gateway sends a disengage request (DRQ) message to the gatekeeper and waits for the disengage confirmation (DCF) message before it sends the SETUP message to the new destination gatekeeper.
- During the admission request (ARQ) phase of a call, a gatekeeper might determine that a call that has come through an intermediate gateway needs to be routed to another gatekeeper. The gatekeeper sends an admission rejection (ARJ) message with a `RejectReason` of `routeCallToGatekeeper` to the gateway.

Upon receiving the message, the intermediate Cisco H.323 Gateway sends a facility message to the originator of the SETUP message. This message indicates that the SETUP message should be sent to another address. (The gateway includes the `callSignalAddress` from ARJ in the `alternativeAddress` field of the facility message.)

Upon receiving the facility message, the calling gateway terminates the initial call and sends a new SETUP message to the specified gatekeeper, using the new IP address specified in the `alternativeAddress` field of the facility message. If the `callSignalAddress` is not provided, the gateway will not send the facility message and the call is terminated without any rerouting.

Call Forward

In certain cases, an H.323 endpoint might determine that a call needs to be forwarded. The endpoint then sends a facility message to the gateway with a `facilityReason` of `callForwarded`. This message includes the address of the new destination (either an `alternativeAddress` or `alternativeAliasAddress`).

Upon receiving the facility message, the Cisco H.323 Gateway sends a release complete to the original destination endpoint and initiates a new call using the new destination address supplied in the facility message. The release complete message contains a `ReleaseCompleteReason` of `facilityCallDeflection`. If the gateway is registered with a gatekeeper, the gateway sends a DRQ to the gatekeeper and waits for the DCF before sending a setup message to the destination gatekeeper.

The facility message must contain an E.164 address in the `alternativeAliasAddress` field. If no address is included, the facility message is ignored. The E164 is required because the call forwarding process initiates a new call, which may be subject to authentication processes that can handle only E.164 addresses.

If the facility message contains both an IP address (in the `alternativeAddress` field) and an E.164 address (in the `alternativeAliasAddress` field), the gateway first attempts to find a match for the new E.164 and the dial-peer. If there is no match, the gateway uses the same incoming peer to determine if there is a matching peer to reroute the call. If there is no match to the incoming peer, the message is ignored.

Call Transfer

If a facility message with a `facilityReason` of `callForwarded` is received after the call has been accepted, it is considered a call transfer. In this case, the Cisco H.323 Gateway will place the call on hold and initiate a new call using the address (`alternativeAddress` or `alternativeAliasAddress`) supplied in the facility message.

As with call forwarding, the facility message must contain an E.164 address in the `alternativeAliasAddress` field. If no address is included, the facility message is ignored. The E164 is required because the call forwarding process initiates a new call, which may be subject to authentication processes that can handle only E.164 addresses.

If the facility message contains both an IP address (in the `alternativeAddress` field) and an E.164 address (in the `alternativeAliasAddress` field), the gateway first attempts to find a match for the new E.164 and the dial-peer. If there is no match, the gateway uses the same incoming peer to determine if there is a matching peer to reroute the call. If there is no match to the incoming peer, the message is ignored.

Unlike in the call forwarding case, the facility message is accepted by both the called side and the originating side.



Note

This use of call forwarding is not defined by the ITU standard.

For further details, please see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcallrd.htm>.

Media Gateway Control Protocol Basic CLASS and Operator Services

The Media Gateway Control Protocol (MGCP) Basic CLASS and Operator Services (BCOS) are a set of calling features, sometimes called “custom calling” features, that use MGCP to transmit voice, video, and data over the IP network. These features are usually found in circuit-based networks. MGCP BCOS brings them to the Cisco IOS gateways on packet-based networks.

The MGCP BCOS software is built on the MGCP CAS PBX and AAL2 software package, and supports MGCP 0.1 and the earlier protocol versions Simple Gateway Control Protocol (SGCP) 1.1 and 1.5.

The following two features can be run as trunking gateway (TGW) features:

- 911 Calls

This feature is supported in SGCP and MGCP modes on the Cisco AS5300.

- Three-Way Calling

This feature is supported on the G.711a and G.711u codecs only.

Refer to the following documents for additional information:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcptk.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcpgr.htm>

Important Notes

Cisco IOS Release 12.1(5) XM8 is compatible with MICA portware 2.7.3.0.

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in [Table 4](#).

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined

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

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

This section contains only open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.1 and Cisco IOS Release 12.1T are also in Cisco IOS Release 12.1(5) XM8.

For information on caveats in Cisco IOS Release 12.1T, see *Caveats for Cisco IOS Release 12.1T*.

For information on caveats in Cisco IOS Release 12.1, see *Caveats for Cisco IOS Release 12.1*, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.1 and is located on Cisco.com and the Documentation CD-ROM.

Caveat numbers and brief descriptions of caveats in Cisco IOS Release 12.1(5) XM5 are listed in [Table 4](#) and [Table 5](#). For details about a particular caveat, go to Bug Toolkit at:

<http://www.cisco.com/kobayashi/bugs/bugs.html>

To access this location, you must have an account on Cisco.com. For information about how to obtain an account, go to the [“Feature Navigator” section on page 19](#).



Note

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

Open Caveats — Cisco IOS Release 12.1(5) XM8

All the caveats listed in [Table 4](#) are open in Cisco IOS Release 12.1(5) XM8. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 4 Open Caveats for Release 12.1(5) XM8

Caveat ID Number	Description
CSCdv61312	AS5300: Voice path for VoIP calls corrupted after TDM hairpin calls.
CSCdv68388	Enhancements/Fixes to Cache Error Exception Handler

Resolved Caveats — Cisco IOS Release 12.1(5) XM8

All the caveats listed in [Table 5](#) are resolved in Cisco IOS Release 12.1(5) XM8. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 5 Resolved Caveats for Release 12.1(5) XM8

Caveat ID Number	Description
CSCdt56171	Running out of DSP on terminating gateway AS5300
CSCdt67753	Need knob to disable automatic MTU adjustment added via CSCdr01713
CSCdt90813	AS5300 Crash at rtcp_construct_rr_block
CSCdu05166	FSM_BAD_EVENT: Invalid FSM Input due to E_TSP_DISCONNECT_CONF
CSCdu08652	dsp hung, dsp crash and %VTSP-3-VTSP-CALL-DISC-FAILED messages
CSCdu69834	ip mtu adjust should default to off
CSCdu86918	DSP resources do not release on hair pinned calls
CSCdv56426	CAS tdm hairpinning calls not released

Open Caveats — Cisco IOS Release 12.1(5) XM7

There are no open caveats specific to Cisco IOS Release 12.1(5) XM7 that require documentation in the release notes.

Resolved Caveats — Cisco IOS Release 12.1(5) XM7

All the caveats listed in [Table 6](#) are resolved in Cisco IOS Release 12.1(5) XM7. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 6 *Resolved Caveats for Release 12.1(5) XM7*

Caveat ID Number	Description
CSCdw65903	An error can occur with management protocol processing. Please use the following URL for further information: http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Open Caveats—Cisco IOS Release 12.1(5) XM6

There are no open caveats specific to Cisco IOS Release 12.1(5) XM6 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.1(5) XM6

All the caveats listed in [Table 7](#) are resolved in Cisco IOS Release 12.1(5) XM6. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 7 *Resolved Caveats for Release 12.1(5) XM6*

Caveat ID Number	Description
CSCdv45035	Memory leak on 5300/5800 running ThunderVoice
CSCdv83040	RADIUS attribute 242 does not support protocol 50 and 51
CSCdr08256	* is converted to 0 in the running config
CSCdu81936	Received gratuitous ARP overwrites interface MAC address in ARP tbl
CSCdv48261	Improvements to dynamic acls for ios fw

Open Caveats—Cisco IOS Release 12.1(5) XM5

There are no open caveats specific to Cisco IOS Release 12.1(5) XM5 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.1(5) XM5

All the caveats listed in [Table 8](#) are resolved in Cisco IOS Release 12.1(5) XM5. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 8 Resolved Caveats for Release 12.1(5) XM5

Caveat ID Number	Description
CSCdt09214	Spurious memory access at vp_ipfib_fixup+0x20
CSCds33599	Modem recovery doesnt kick in case of no answer
CSCdp71957	Dialer needs to turn off spoofing immdtly when async idb state is up
CSCdu50601	ISDN should release 64K call w/ cause=Bearer Cap not supported
CSCds69851	dsx1_clear_call_counter_cmd(0x601c9ac8)+0x60
CSCdt47204	SNMP LinkUp/Down traps raised on AS5300 for B channels
CSCdt42813	AS5300 hangs in hwsb_unlink

Open Caveats—Cisco IOS Release 12.1(5) XM4

All the caveats listed in [Table 9](#) are open in Cisco IOS Release 12.1(5) XM4. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 9 Open Caveats for Release 12.1(5)XM4

Caveat ID Number	Description
CSCdt61467	Need a way to change the default value of VPDN parameters
CSCdu33245	During stress test router crash
CSCdu33381	Memory allocation failures and traceback when placing calls during reload
CSCdu38669	Interoperation of ISDN and SIP messages not behaving correctly
CSCdu50611	Memory leak in process ISDN for SS7 COT transponder IVR call

Resolved Caveats—Cisco IOS Release 12.1(5) XM4

All the caveats listed in [Table 10](#) are resolved in Cisco IOS Release 12.1(5) XM4. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 10 Closed and Resolved Caveats for Release 12.1(5) XM4

Caveat ID Number	Description
CSCds14059	Support for untagged Radius tunnel attributes (attr.69 et al)
CSCds55510	Memory Leak with AAA route download
CSCds63993	H323 GW: IP calls dangling when delay TCP connection occurs
CSCds65611	All B-chan out of serv after controller no-shut then serial no-shut
CSCds66249	Disc cause code is not passed end to end
CSCds71291	Spurious Accesses in mlp_timer
CSCdt11503	IOS crashes when large OID (>256 fields) is received
CSCdt28919	No ringback on calling side, ring on called side, no audio both ways
CSCdt41888	Add dlcx functionality as hidden command

Table 10 Closed and Resolved Caveats for Release 12.1(5) XM4 (continued)

Caveat ID Number	Description
CSCdt46181	Redzone corruption in pptp_tcp_readf()
CSCdt52469	Fax-Relay feature doesn't work with modem pass through configured
CSCdt57872	Router reloads in LanguageInterpCreate
CSCdt60338	Need Anand Menon to double commit it
CSCdt63518	FIB-4-PUNTINTF msg for L2F/MP bundle member w no ip route-cache cef
CSCdt65952	MGCP sup. disconnect breaks trunking tone detection
CSCdt69055	B-channels IN_SERVICE after RESTART when L1 is DEACTIVATED
CSCdt89495	24th channel of T1 0 stays busied-out
CSCdt92919	Debug mgcp all & debug vtsp all together fail on-net to offnet fax
CSCdt96253	CRC-32 compensation vulnerability
CSCdt96945	Resource threshold information lost on GK after element failure
CSCdu04583	Large volume of disconnects, ISDN sends REL late w/no cause code
CSCdu05205	Memory corruption crash
CSCdu05236	Default disabling of parser cache should not be nvgened
CSCdu05860	c5300-jx-mz.121-5XM fails contriq on/off-net fax
CSCdu06582	MGCP was unable to detect the tone t/ro
CSCdu07504	sh voice dsp causes reload
CSCdu08214	Calltracker MIB returns NULL for userid when DNIS/ANI is not present
CSCdu14000	Traceback at rlm_link_weight_priority_insert_compare after reload
CSCdu25007	clear spe with calls running could have negative effects
CSCdu27780	AS5300 Suspend message not sent on H323 side with fax configured
CSCdu33835	Spurious memory access in COT timer expiry
CSCdu34741	Term GW doesnt disconnect call which arrives after RLM is down
CSCdu42219	Throttle 21 fails to bring up B channels after reboot w/SS7
CSCdu62721	12.1(5)XM4 candidate fails to bring up B-channels

Open Caveats—Cisco IOS Release 12.1(5) XM3

All the caveats listed in [Table 11](#) are open in Cisco IOS Release 12.1(5) XM3. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 11 Open Caveats for Release 12.1(5) XM3

Caveat ID Number	Description
CSCdt49924	ISDN: isdn map not properly populating calling party number
CSCds52536	ISDN sync call rejected/failed caller id screening/workaround>reload
CSCds70303	SHOW ISDN STAT shows hanging CCBs (CCBs without active calls)

Resolved Caveats—Cisco IOS Release 12.1(5) XM3

All the caveats listed in [Table 12](#) are resolved in Cisco IOS Release 12.1(5) XM3. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 12 *Resolved Caveats for Release 12.1(5) XM3*

Caveat ID Number	Description
CSCdr69228	Cisco AS5300 crashes at abort(0x602d9924)+0x8
CSCdt74954	Does not send correct error codes for offramp fax
CSCdr56944	Cisco AS5300 bus error at acct_search_type
CSCds13057	Cisco AS5300 ISDN callback cannot work after running a period of time
CSCdt16456	Requested circuit/channel not available even when there is one available
CSCdt27202	AAA authentication broken for T37 fax
CSCdt30184	B-Channel hangs during Dial-Out
CSCdt54401	High CPU utilization when using fas-start and during high usage
CSCdt60052	COT fails on Cisco AS5300 with VCware version 8.07 HC C549
CSCdt60517	cdapi_appl_add() corrupting memory during system init
CSCdt67802	No audio path for third call attempt after two COT failures.
CSCdt66797	Call transfer failed when alert and connect received at same time
CSCdt96526	No voice path on SETUP of retry after COT failure
CSCdt82892	After RLM shut/no shut, only primary DSL of NFAS grp reinitialized
CSCdt42813	AS5300 hangs in hwsb_unlink
CSCdt55258	MLP hangs router or causes stack overrun
CSCds52920	Syslog messages are not logged onto syslog server.
CSCdt01452	Lex interface forward bridge BPDUs coming from remote LAN extender
CSCdt09023	Cannot build the 7200 platform -p- images
CSCdt10151	H323 VSA attribute being sent for all platforms
CSCdt30629	Need to speed up RM to TACACS+ accounting processing
CSCdt38813	H323 GW leaks RTCP ports with signal only call
CSCdt78196	Cisco 3640 router crashes at L3_ProcessInternal

Open Caveats—Cisco IOS Release 12.1(5) XM2

This section documents possible unexpected behavior by Cisco IOS Release 12.1(5) XM2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCds81187
When the PPP Password Authentication Protocol (PAP)-password validation fails—that is, when the PPP PAP password is configured incorrectly—a slow memory leak occurs. There is no workaround.

- CSCdt30184

The CLI command **isdn negotiate-bchan resend-setup** does not show up when using the CLI help feature. This command allows Cisco IOS software to try a different B channel when a call setup on an initial B channel fails—for example, due to a Continuity Testing (COT) test failure. Turning on this option is recommended when using the **isdn switch-type primary ni** command in order to increase the call success rate.

Workaround: Configure the **isdn negotiate-bchan resend-setup** command, even though it is not yet documented as a command.

Resolved Caveats—Cisco IOS Release 12.1(5) XM2

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(5) XM2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCds65453

If a Class-3 switch that is connected to an ISDN PRI interface of a Cisco AS5300 initiates a call, the call uses a SIP proxy, reaches a gateway, and is terminated at another switch. Most of the calls are completed properly (that is, a tone is generated and the phone is answered), but randomly some of the calls do not complete and no error message is produced in the Cisco AS5300 log. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)XM2.

- CSCds04747

Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at <http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml>.

This caveat is resolved in Cisco IOS Release 12.1(5) XM2.

Open and Resolved Caveats—Cisco IOS Release 12.1(5) XM1

There are no open and resolved caveats specific to Cisco IOS Release 12.1(5) XM1 that require documentation in the release notes.

Open and Resolved Caveats—Cisco IOS Release 12.1(5) XM

There are no open and resolved caveats specific to Cisco IOS Release 12.1(5) XM that require documentation in the release notes.

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2. These documents consist of software installation guides, Cisco IOS configuration and command references, system error messages, and other documents.

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

Use these release notes with these documents:

- [Release-Specific Documents, page 18](#)
- [Platform-Specific Documents, page 19](#)
- [Feature Modules, page 19](#)
- [Feature Navigator, page 19](#)
- [Cisco IOS Software Documentation Set, page 20](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.1 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.1*

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.1: Release Notes: Cross-Platform Release Notes

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Release Notes: Cross-Platform Release Notes

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

Technical Documents

- The “[Caveats](#)” section on page 11

As a supplement to the caveats listed in “[Caveats](#)” in these release notes, see *Caveats for Cisco IOS Release 12.1* and *Caveats for Cisco IOS Release 12.1 T*, which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.1 and Cisco IOS Release 12.1 T.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.1: Release Notes: Caveats

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Caveats

Platform-Specific Documents

These documents are available for the Cisco AS5300 on Cisco.com and the Documentation CD-ROM:

- *Quick Start Guide Cisco AS5300 Universal Access Server Install and Configure*
- Hardware Installation Documents for Cisco AS5300
- Configuration Documents for Cisco AS5300
- *Regulatory Compliance and Safety Information*

On Cisco.com at:

Technical Documents: Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.1(5) XM8 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.1: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation

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. 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. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.1: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References

Release 12.1 Documentation Set

[Table 14](#) lists the contents of the Cisco IOS Release 12.1 software documentation set, which is available in electronic form and in printed form if ordered.

**Note**

You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management Cisco IOS User Interfaces Commands Cisco IOS File Management Commands Cisco IOS System Management Commands
<ul style="list-style-type: none"> • <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i> 	Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i> • <i>Cisco IOS Dial Services Configuration Guide: Network Services</i> • <i>Cisco IOS Dial Services Command Reference</i> 	Preparing for Dial Access Modem Configuration and Management ISDN and Signaling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Interworking Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP and IP Routing Configuration Guide</i> • <i>Cisco IOS IP and IP Routing Command Reference</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 and Novell IPX Overview Configuring AppleTalk Configuring 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, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Multiservice Applications Configuration Guide</i> • <i>Cisco IOS Multiservice Applications Command Reference</i> 	<ul style="list-style-type: none"> Multiservice Applications Overview Voice Video Broadband
<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> 	<ul style="list-style-type: none"> Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms Quality of Service Solutions
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	<ul style="list-style-type: none"> Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	<ul style="list-style-type: none"> Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding 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> 	<ul style="list-style-type: none"> Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
<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 Dial Services Quick Configuration Guide</i> • <i>Cisco IOS Software System Error Messages</i> • <i>New Features in 12.1-Based Limited Lifetime Releases</i> • <i>New Features in Release 12.1 T</i> • <i>Release Notes</i> (Release note and caveat documentation for 12.1-based releases and various platforms) 	

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/ordering/index.shtml>
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

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

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section on page 18.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0201R)

Copyright © 2000–2002, Cisco Systems, Inc.
All rights reserved.