



# Release Notes for Cisco AS5800 Universal Access Servers for Cisco IOS Release 12.1XM

---

February 25, 2002

Cisco IOS Release 12.1(5) XM8

78-12053-01 Rev. J0

These release notes for the Cisco AS5800 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 for Cisco IOS Release 12.1 XM” section on page 17](#) 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.

## Contents

These release notes describe the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 3](#)
- [New and Changed Information, page 9](#)
- [MIBs, page 16](#)
- [Caveats for Cisco IOS Release 12.1 XM, page 17](#)
- [Related Documentation, page 26](#)
- [Obtaining Documentation, page 31](#)
- [Obtaining Technical Assistance, page 32](#)



---

**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 AS5800 access server and Cisco 5800 voice gateway are high-density, Voice, Integrated Services Digital Network (ISDN), and modem Wide Area Network (WAN) aggregation systems that provide voice and digital and analog call termination. They are intended to be used as a service provider dial point-of-presence (POP) or centralized enterprise dial gateway. The Cisco AS5800 consists of a dial shelf and one or two router shelves:

- The Cisco DS5814 (dial shelf) has 14 slots and can support 1 or 2 dial shelf controller cards and up to 12 feature cards to provide full analog modem, voice/fax, and ISDN coverage. The dial shelf supports up to 2047 simultaneous data calls or up to 1344 voice calls. Analog calls are terminated by a feature card that is loaded with integrated modems. Voice calls are terminated by feature cards that are loaded with voice DSPs.



**Note** The Cisco DS5814 supports both high-complexity and medium-complexity voice cards. You cannot mix high-complexity and medium-complexity voice cards on the same dial shelf unless the dial shelf is in split mode. If the dial shelf is in split mode, each split shelf must have voice cards of the same complexity type.

ISDN calls are terminated onboard the trunk card on High-Level Data Link Control (HDLC) controllers. The E1 trunk, T1 trunk, and the CT3 trunk cards include channel service units (CSUs) and have either 12 E1 ports, 12 T1 ports, or 28 T1 ports (within the CT3 trunk) that can operate as Primary Rate Interfaces (PRIs), inter-machine trunks (IMTs), or channelized interfaces in any combination. The specific trunk card limitations are described in [Table 2, Part 1](#).



**Note** T1 and E1 cards are not supported in the same box.

- The Cisco RS7206VXR (router shelf) contains a network processing engine, an I/O controller, and the egress interfaces, such as High-Speed Serial Interface (HSSI), Fast Ethernet (FE), Gigabit Ethernet (GE), and Asynchronous Transfer Mode (ATM), and supports either 280W AC-input or 280W DC-input redundant power. The router shelf also may contain one or two dial shelf interconnect port adapters each with a single RJ-45 receptacle, which is used to connect the router shelf to the Cisco 5814 dial shelf. The interconnect port adapter connects directly to the dial shelf controller card on the dial shelf via a Cisco-proprietary cable, customized with jack screws to secure the connection. You must use this specially designed cable that ships with your interconnect port adapter. Each router shelf can only be connected to one dial shelf controller card. If the dial shelf configured in split mode, it must be connected to two separate router shelves.



**Note** The router shelf is only supported for routing data to and from the dial shelf. The router should not be used with multiple port adapter interfaces to route LAN traffic between multiple networks.

The AC-input power shelf is an optional component of the Cisco AS5800 and is used to convert AC-input power into DC-output power for the DC-powered Cisco 5814 dial shelf. The AC-input power shelf contains two AC-input power supplies.

The AC-input to DC-output connection supplies –48V DC-output power to the dial shelf power entry modules (PEMs). The PEMs receive the –48V and transmit power to the filter module. Power flows through the filter module to the backplane, where it is distributed to the dial shelf controller card(s) and feature cards.

The AC-input power shelf includes two 2,000 W, AC-input power supplies that plug into a common power backplane in the AC-input power shelf. A single AC-input power supply is capable of powering a fully configured Cisco 5814 dial shelf. The second power supply provides full redundancy.

## Cisco AS5800 Voice Feature Cards

The Cisco AS5800 Voice Feature Cards are full-featured voice processing cards. Voice processing capabilities include Voice Activity Detection (VAD), comfort noise generation, adaptive jitter buffering, programmable 16 and 32 ms echo cancellation, programmable frame size, and Dual Tone Multiple Frequency (DTMF) detection and generation. The Cisco AS5800 Voice Feature cards offer industry-leading DSP density and a wide range of VoIP codecs.

Medium-complexity Voice Feature Cards support 336 or 192 sessions per card. The medium-complexity VFCs support only codecs that require 20-MIPS or less per session including G.711, G.729a, and G.726. Their part numbers are DS58-336-MC-VOX and DS58-192-MC-VOX, respectively.

High-complexity Voice Feature Cards support 192 or 92 sessions per card, the high-complexity VFCs support all types of codecs including G.711, G.729a, G.726, G.723.1, G.728 and G.729. Their part numbers are DS58-192VOX and DS58-96VOX, respectively.

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 9 and the [“Related Documentation”](#) section on page 26.

## System Requirements

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

- [Memory Requirements, page 3](#)
- [Supported Hardware, page 4](#)
- [Determining the Software Version, page 7](#)
- [Upgrading to a New Software Release, page 7](#)
- [Microcode and Modem Code Software, page 7](#)
- [Feature Set Tables, page 8](#)

## Memory Requirements

**Table 1** Cisco AS5800 Memory Requirements

System Components	Feature Set	Image Name	Software Image	Flash Memory Required	DRAM Memory Required
Cisco AS5800	IP Standard	IP Plus	c5800-p4-mz	16 MB	256 MB
Dial Shelf: Cisco 5814		IP Plus	dsc-c5800-mz	8 MB	64 MB <sup>1</sup>
Cisco AS5800	Service Provider Standard	Service Provider IPsec 56	c5800-p456i-mz	16 MB	256 MB

1. Cisco IOS Release 12.1(5) XM8 may be used with the older RS7206 (NPE-200 based) router shelf as long as the shelf has 128M of DRAM installed.

## Supported Hardware

Cisco IOS Release 12.1(5) XM8 supports the Cisco AS5800:

- Cisco DS5814
- Cisco RS7206
- Cisco RS7206 VXR

For detailed descriptions of the new hardware features, see the [“New and Changed Information” section on page 9](#). Table 2, parts 1 and 2, details the supported interfaces, cards, options, NPE support, and port adapters.

**Table 2, Part 1 Supported Hardware for the Cisco AS5800**

Interfaces, Cards, Options, and Support	Description
<b>Interfaces</b>	12-port T1 or E1 termination card
	1- port channelized T3 (CT3) termination card
<b>Modem Cards</b>	72-port modem card (HMM) <sup>1</sup>
	144-port modem card (DMM) <sup>2</sup>
	324-port modem card (UPC)
<b>Voice Feature Cards (VFCs)<sup>3</sup></b>	96-port voice card (96VOX)
	192-port voice card (192VOX)
	192-port medium complexity voice card (192-MC-VOX)
	336-port medium complexity voice card (336-MC-VOX)
<b>Dial Shelf</b>	DS5814 Dial Shelf
	Dial Shelf Controller (DSC) card
<b>Optional AC-input Power Shelves</b>	Two AC-input power supplies
<b>Router Shelf Support</b>	RS7206VXR (NPE-300 based) Router Shelf
	RS7206 (NPE-200 based) Router Shelf
	With any Cisco AS5800 software image, the maximum hardware configuration with an RS7206 is one CT3 or two T1/E1 trunk cards and three UPCs, five DMMs or 10 HMMs for a maximum of 28 24 T1 / 24 E1 controllers and 720 modems.  If a larger configuration is desired, a second RS7206 router shelf can be configured in split-shelf mode, or a single RS7206 VXR may be used to support up to 1344 modem sessions. Configurations above 1344 modem sessions require two RS7206VXR router shelves in split-shelf mode.  The Cisco AS5800/Voice Gateway can support 672 voice calls per RS7206VXR router shelf. 1344 voice calls require two RS7206VXR router shelves configured in split-shelf mode. RS7206 router shelves do not support voice services.

1. 72-port modem card requires 32M DRAM.

2. 144-port modem card requires 64M DRAM.

3. High-complexity voice cards (with codecs G.723.1, G.728, or G.729) require greater resources to perform complex coding and decoding that results in Voice-handling capacity reduction. Medium-complexity voice cards (with codecs G.711, G.726, or G.729a) can manage twice the number of Voice channels than high-complexity voice cards can.

Table 2, Part 2 Supported Hardware for the Cisco AS5800

Router Shelf	Port Adapter	Description
RS7206 Router Shelf	PA-100VG	Single-Port 100 VG Port Adapter
	PA-12E/2FE	Dual-Wide Ethernet-switch Port Adapter
	PA-1C-E	1-Port ESCON Channel Port Adapter
	PA-2CE1/PRI-120	2-Port Channelized E1/PRI Port Adapter, 120 ohm
	PA-2CE1/PRI-75	2-Port Channelized E1/PRI Port Adapter, 75 ohm
	PA-2CT1/PRI	2-Port Channelized T1/PRI Port Adapter
	PA-2E3	2-Port E3 Serial Port Adapter with E3 DSU
	PA-2FEISL-FX	2-Port Fast Ethernet/ISL 100BaseTx Port Adapter
	PA-2FEISL-TX	2-Port Fast Ethernet/ISL 100BaseFx Port Adapter
	PA-2H	Port Adapter, 2-Port HSSI
	PA-4B-U	4-Port BRI Port Adapter, U Interface
	PA-4E	Port Adapter, 4-Port Ethernet,10BT
	PA-4R	Port Adapter, 4-Port Token Ring (Older Hermon Based)
	PA-4R-DTR	Port Adapter, 4-Port Token Ring (Hawkeye Based)
	PA-4R-FDX	Port Adapter, 4 Port Token Ring 4/16Mbps, Full Duplex
	PA-4T+	Port Adapter, 4-Port Serial,5IN1
	PA-5EFL	Port Adapter, 5-Port Ethernet,10FL
	PA-8B-S/T	8-Port BRI Port Adapter, S/T Interface
	PA-8E	Port Adapter, 8-Port Ethernet,10BT
	PA-8T-232	Port Adapter, 8-Port Serial,232
	PA-8T-V35	Port Adapter, 8-Port Serial,V.35
	PA-8T-X21	Port Adapter, 8-Port Serial,X.21
	PA-A1-OC3MM	1-Port ATM OC3 Multi-Mode Port Adapter
	PA-A1-OC3SM	1-Port ATM OC3 Single Mode Intermediate Reach Port Adapter
	PA-A2-4E1XC-E3ATM	CES Port Adapter E3/E1 120 ohms
	PA-A2-4E1XC-OC3SM	CES OC3 Port Adapter 4E1 Ports 120 ohms
	PA-A2-4T1C-OC3SM	ATM CES Port Adapter, 4T1 CES Ports and 1 OC3 ATM SM Port
	PA-A2-4T1C-T3ATM	ATM CES Port Adapter, 4T1 CES Ports and 1 T3 ATM Port
	PA-A3-E3	1-Port ATM Enhanced E3 Port Adapter
	PA-A3-OC3MM	1-Port ATM Enhanced OC3c/STM1 Multi-Mode
	PA-A3-OC3SMI	1-Port ATM Enhanced OC3c/STM1 Single Mode
	PA-A3-OC3SML	1-Port ATM Enhanced OC3c/STM1 Single Mode
	PA-A3-T3	1-Port ATM Enhanced DS3 Port Adapter
	PA-CT3/4T1	Channelized DS3 Port Adapter with 4 T1
	PA-E3	1-Port E3 Serial Port Adapter with E3 DSU
	PA-F/FD-MM	Port Adapter,1-Port FDDI Full Duplex Multi-Mode

Table 2, Part 2 Supported Hardware for the Cisco AS5800 (continued)

Router Shelf	Port Adapter	Description
RS7206 Router Shelf (continued)	PA-F/FD-SM	Port Adapter,1-Port FDDI Full Duplex Single-Mode
	PA-FE-FX	Port Adapter,1-Port FE, 100FX
	PA-FE-TX	Port Adapter,1-Port FE,100TX
	PA-F-MM	Port Adapter,1-Port FDDI Multi-Mode
	PA-F-SM	Port Adapter,1-Port FDDI Single Mode
	PA-H	Port Adapter,1-Port HSSI
	PA-POS-OC3MM	1-Port Packet/SONET OC3c/STM1 Multi-Mode Port Adapter
	PA-POS-OC3SMI	1-Port Packet/SONET OC3c/STM1 Single Mode (IR) Port Adapter
	PA-POS-OC3SML	1-Port Packet/SONET OC3c/STM1 Single Mode (LR) Port Adapter
	PA-T3	1-Port T3 Serial Port Adapter with T3 DSUs
	PA-T3+	1-Port T3 Serial Port Adapter Enhanced
	SA-COMP/1	Service Adapter, Compression (64 VCs Stac)
	SA-COMP/4	Service Adapter, Compression (256 VCs Stac)
	RS7206VXR Router Shelf	PA-100VG
PA-12E/2FE		Dual-Wide Ethernet-Switch Port Adapter
PA-1C-E		1-Port ESCON Channel Port Adapter
PA-2E3		2-Port E3 Serial Port Adapter with E3 DSU
PA-2FEISL-FX		2-Port Fast Ethernet/ISL 100BaseTx Port Adapter
PA-2FEISL-TX		2-Port Fast Ethernet/ISL 100BaseFx Port Adapter
PA-2H		Port Adapter, 2-Port HSSI
PA-4B-U		4-Port BRI Port Adapter, U Interface
PA-4E		Port Adapter, 4-Port Ethernet,10BT
PA-4R-DTR		Port Adapter, 4-Port Token Ring (Hawkeye Based)
PA-4T+		Port Adapter, 4-Port Serial,5in1
PA-5EFL		Port Adapter, 5-Port Ethernet,10FL
PA-8B-S/T		8-Port BRI Port Adapter, S/T Interface
PA-8E		Port Adapter, 8-Port Ethernet,10BT
PA-8T-232		Port Adapter, 8-Port Serial,232
PA-8T-V35		Port Adapter, 8-Port Serial,V.35
PA-8T-X21		Port Adapter, 8-Port Serial,X.21
PA-A1-OC3MM		1-Port ATM OC3 Multi-Mode Port Adapter
PA-A1-OC3SM		1-Port ATM OC3 Single Mode Intermediate Reach Port Adapter
PA-A2-4E1XC-E3ATM		CES Port Adapter E3/E1 120 ohms
PA-A2-4E1XC-OC3SM		CES OC3 Port Adapter 4E1 Ports 120 ohms
PA-A2-4T1C-OC3SM		ATM CES Port Adapter, 4T1 CES Ports and 1 OC3 ATM SM Port
PA-A2-4T1C-T3ATM		ATM CES Port Adapter, 4T1 CES Ports and 1 T3 ATM Port

Table 2, Part 2 Supported Hardware for the Cisco AS5800 (continued)

Router Shelf	Port Adapter	Description
RS7206VXR Router Shelf (continued)	PA-A3-E3	1-Port ATM Enhanced E3 Port Adapter
	PA-A3-OC3MM	1-Port ATM Enhanced OC3c/STM1 Multi-Mode
	PA-A3-OC3SMI	1-Port ATM Enhanced OC3c/STM1 Single Mode
	PA-A3-OC3SML	1-Port ATM Enhanced OC3c/STM1 Single Mode
	PA-A3-T3	1-Port ATM Enhanced DS3 Port Adapter
	PA-E3	1-Port E3 Serial Port Adapter with E3 DSU
	PA-FE-FX	Port Adapter, 1-Port FE, 100FX
	PA-FE-TX	Port Adapter, 1-Port FE, 100TX
	PA-GE	One-Port Gigabit Ethernet PA for 7200VXR
	PA-H	Port Adapter, 1-Port HSSI
	PA-MC-8E1/120	8-Port Multichannel E1 Port Adapter
	PA-POS-OC3MM	1-Port Packet/SONET OC3c/STM1 Multi-Mode Port Adapter
	PA-POS-OC3SMI	1-Port Packet/SONET OC3c/STM1 Single Mode (IR) Port Adapter
	PA-POS-OC3SML	1-Port Packet/SONET OC3c/STM1 Single Mode (LR) Port Adapter
	PA-T3	1-Port T3 Serial Port Adapter with T3 DSUs
	PA-T3+	1-Port T3 Serial Port Adapter Enhanced

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco AS5800, log in to the Cisco AS5800 and enter the **show version EXEC** command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.1 Software (c5800-p4-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](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. 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](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 AS5800: Configuration Documents for Cisco AS5800: Port Information**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5800: Configuration Documents for Cisco AS5800: Port Information**

## Other Firmware Code

Default bundled firmware for Nextport upgraded from version 2.3.3.108 to version 2.3.5.108.

## 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 AS5800.



### Note

Features in Cisco IOS Release 12.1(5) T are listed in the *Release Notes for Cisco AS5800 Universal Access Servers for Cisco IOS Release 12.1 T*. 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>.



### Caution

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

Table 3 lists the features and feature sets supported by the Cisco AS5800 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.

**Table 3 IP Plus Image Feature List for the Cisco AS5800 for Cisco IOS Release 12.1 XM**

Features	Introduced In
<b>Dial</b>	
Call Denial for Voice Coded CPU Utilization Management	(2)XM
<b>Other</b>	
Prepaid Distributed Calling Card via Packet Telephony	(2)XM
NFAS with D Channel Backup	(2)XM
<b>Security</b>	
H.235 Accounting and Security Enhancements	(2)XM
<b>Voice</b>	
Cisco H.323 Multizone Enhancements	(2)XM
Feature Group D Support	(2)XM
H.323 Call Redirection Enhancements	(2)XM
H.323v2 Fast Connect	(2)XM
SIP Diversion Header Implementation for Redirecting Number (CSCdr72341)	(2)XM
T1 CAS for Voice over IP	(2)XM
T.38 Fax for Cisco Universal Gateways	(2)XM

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5800 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 AS5800 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 AS5800 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 AS5800 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 AS5800 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 AS5800 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 AS5800 for Cisco IOS Release 12.1(5) XM3.

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

There are no new hardware features in the Cisco AS5800 for Cisco IOS Release 12.(5)XM2.

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

The following new software features are supported by the Cisco AS5800 for Cisco IOS Release 12.(5)XM2.

### Call Denial for Voice Coded CPU Utilization Management

The Call Denial for Voice Coded CPU Utilization Management feature permits the Cisco access servers to deny incoming calls exceeding a preconfigured threshold, permitting the selection of a system CPU load level value. This feature helps ensure the quality of service of existing calls and reliability of system processes by preventing system overload caused by excessive incoming calls. It is designed to reject new digital calls (PRI, CAS, and ISDN), with as little disruption to system users as possible.

### Cisco H.323 Multizone Enhancements

This feature enables the Cisco gateway to provide information to the gatekeeper with the use of additional fields in the RAS (registration, admission, and status) messages.

For further details, please see:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5400/sw\\_conf/ios\\_121/pull0244.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pull0244.htm).

## Feature Group D Support

This feature extends support for Feature Group D signaling on Cisco platforms. Feature Group D service is a trunk side connection that enables telephone customers to choose their long distance network and use the same number of digits no matter which carrier they use. Routers interface with interexchange carriers using Feature Group D to support voice traffic in the carrier environment.

For further details, please see

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5400/sw\\_conf/ios\\_121/pulhdvfg.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pulhdvfg.htm).

## H.235 Accounting and Security Enhancements

The Cisco H.323 gateway now supports the use of CryptoH323Tokens for authentication. The CryptoH323Token is defined in H.225 Version 2 and is used in a “password-with-hashing” security scheme as described in section 10.3.3 of the H.235 specification.

For further details, please see

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5800/sw\\_conf/ios\\_122/pul0242x.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/ios_122/pul0242x.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.450.2 Call Redirection Enhancements feature adds support for two of the reasons: routeCallToGatekeeper and callForwarded. It also provides a non-standard 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 end-point. 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, which 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 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/ios121/121newft/121limit/121x/121xm/121xm\\_5/ftp56670.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ftp56670.htm).

## H.323v2 Fast Connect

The Fast Connect feature allows endpoints to establish media channels without waiting for a separate H.245 connection to be opened. This streamlines the number of messages that are exchanged and the amount of processing that must be done before endpoint connections can be established. A high-level view of the Fast Connect procedures within the H.323 protocol follows:

- The calling endpoint transmits a SETUP message containing the fastStart element that contains a sequence of encoded logical channel structures, each representing a different capability media type for both “send” and “receive” directions.
- The called endpoint selects one or more of the media types offered by the calling endpoint for the send and receive directions and returns its selections as logically encoded Q.931 messages up to and including CONNECT. At this point, the called endpoint must be prepared to receive media along any of the channels it selected.
- If H.245 procedures are needed and one or both of the endpoints do not support tunneling, then a separate H.245 connection is used.

This feature is not explicitly configurable. It is assumed that the gateway is capable of sending and receiving Fast Connect procedures unless its corresponding dial peer has been configured for RSVP (in other words, the req-qos is set to a value other than the default of best-effort). If the dial peer has been configured for RSVP, then traditional “slow” connect procedures will be followed, and the endpoint will neither attempt to initiate Fast Connect nor respond to a Fast Connect request from its peer.

A terminating endpoint can reject Fast Connect by simply omitting the fastStart element from all Q.931 messages up to and including CONNECT. In this case, normal H.245 procedures are followed and a separate H.245 TCP connection is established. So, if an endpoint does not support the Fast Connect procedures, normal H.245 procedures are followed. In addition, certain conditions can cause a Fast Connect call to fall back to normal H.245 procedures to complete the call.

Once a media connection has been opened (an audio path has been established), either endpoint has the option of switching to H.245 procedures (if they are needed) by using H.245 tunneling, whereby H.245 messages are encapsulated within the h245Control element of Q.931 messages.

The **dtmf-relay** command is the only H.245-cognizant command that can initiate H.245 tunneling procedures from a Fast Connect call. If H.245 tunneling is active on the call, switching to a separate TCP H.245 connection is not supported.

A Cisco terminating endpoint accepts a Fast Connect request only if a pair of symmetric codecs (codecs that in both directions are the equivalent or identical) can be selected from a list that has been offered. The originating endpoint is constrained only by what it can send through the codec (or voice class codec list) associated with the dial peer.

If the Cisco originating endpoint has offered multiple codecs and the terminating endpoint selects a pair of asymmetric (mismatched) codecs, then the originating endpoint initiates separate H.245 procedures to correct the asymmetric codec situation.

Fast Connect is backward compatible with H.323 Version 1 configurations.

## NFAS with D Channel Backup

The DMS100, NI2, and 4ESS switch types have been added to the existing Non-Facility Associated Signaling (NFAS) with D Channel Backup feature.

ISDN NFAS allows a single D channel to control multiple PRI interfaces. A backup D channel can be configured for use when the primary NFAS D channel fails.

Once the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all the members of the associated NFAS group.

For further details, please see

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5800/sw\\_conf/ios\\_122/ft\\_nfas.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/ios_122/ft_nfas.htm).

## Prepaid Distributed Calling Card via Packet Telephony

The Debit Card for Packet Telephony on Cisco Access Platforms is an application supported by the Cisco Interactive Voice Response (IVR) feature. The IVR voice scripts have been modified to use Tool Command Language (TCL) scripts.

The feature components consist of IVR functionality in Cisco IOS software that work in conjunction with an integrated third-party billing system. The Debit Card feature includes the ability to maintain per-user credit balance information through the use of a billing system. When these features are implemented, the billing system and IOS software functions enable a carrier to authorize voice calls and debit individual user accounts in real time at the edges of a voice-over-IP network, without requiring external service nodes. This feature uses vendor specific attributes (VSAs) to communicate with the billing system.

For further details, please see

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5400/sw\\_conf/ios\\_121/pull0134.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pull0134.htm).

## 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 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>.

## T.38 Fax for Cisco Universal Gateways

When the Cisco universal gateway is equipped with DFCs, it supports carrier-class Voice over IP (VoIP) and fax over IP services. Since the Cisco universal gateway is H.323 compliant, it supports a family of industry-standard voice codecs and provides echo cancellation and Voice Activity Detection (VAD)/silence suppression.

A universal port dial feature card (DFC) is a hardware card that processes digital service port technology for the Cisco AS5400. Ports on the universal port DFC support multiple types of services such as modem, fax, digital data, and voice. The universal port DFC provides multiple port sessions, with each session capable of originating or terminating a session over a DS-0 in PCM format. The number of sessions depends on the port density of the card. You can manage your port connections at the universal port slot level, service processing element (SPE) level, or port level using monitoring and troubleshooting commands. A port is defined as an endpoint on a DFC card through which multiservice tones, voice, and data flow. There are six ports per SPE.

The T.38 Fax Relay for Universal Gateways feature provides standards-based Fax Relay protocol support on AS5800 universal access servers. As The T.38 Fax Relay protocol is standards based, Cisco gateways and gatekeepers will now be able to interoperate with third-party T.38-enabled gateways and gatekeepers in a mixed vendor network where real time Fax Relay capabilities are required.

When a fax is sent from the originating gateway, an initial voice call is established. The terminating gateway, detects the fax tone generated by the answering fax machine. The VoIP H.323 call stack then starts a T.38 mode request using H.245 procedures. If the opposite end of the call acknowledges the T.38 mode request, the initial audio channel is closed and a T.38 Fax Relay channel is opened. When the fax transmission is completed, the call is reverted back to voice mode.

For further details, please see:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5400/sw\\_conf/ios\\_121/puldtfax.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/puldtfax.htm)

## T1 CAS for Voice over IP

This feature adds support for T1 Channel Associated Signaling (CAS) and limited support for E1 R2 signaling to the Cisco AS5800 with the Voice Feature Card (VFC).

CAS is the transmission of signaling information within the voice channel. Various types of CAS signaling are available in the T1 world. The most common forms of CAS signaling are loop-start, ground-start, and receive and transmit (E&M). The biggest disadvantage of CAS signaling is its use of user bandwidth to perform signaling functions. CAS signaling is often referred to as robbed-bit-signaling because user bandwidth is being “robbed” by the network for other purposes. In addition to receiving and placing calls, CAS signaling also processes the receipt of DNIS and ANI information, which is used to support authentication and other functions.

T1 CAS capabilities have been implemented on the Cisco AS5800 VFC to enhance and integrate T1 CAS capabilities on common central office (CO) and PBX configurations for voice calls. The service provider application for T1 CAS includes connectivity to the public network using T1 CAS from the Cisco AS5800 to the end office switch. In this configuration, the Cisco AS5800 captures the dialed-number or called-party number information and passes it along to the upper-level applications for interactive voice response (IVR) script selection, modem pooling, and other applications. Service providers also require access to calling party number, ANI, for user identification, for billing account number, and in the future, more complicated call routing.

Service providers who implement VoIP include traditional voice carriers, new voice and data carriers, and existing Internet service providers. Some of these service providers might use subscriber side lines for their VoIP connectivity to the PSTN; others will use tandem-type service provider connections.

# MIBs

## Current MIBs

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>.

The Cisco AS5800 support the following MIBs:

- AAA-SESSION-MIB
- AAA-SERVER-MIB
- ATM-MIB
- CALL-TRACKER-MIB
- CISCO-ATM2-MIB
- CISCO-ATM-IF-PHYS-MIB
- CISCO-ATM-SIG-DIAG-MIB
- CISCO-BULK-FILE-MIB
- CISCO-C8500-REDUNDANCY-MIB
- CISCO-CALL-HISTORY-MIB.my
- CISCO-CIRCUIT-INTERFACE-MIB
- CISCO-DIAL-CONTROL-MIB
- CISCO-DSP-MGMT-MIB
- CISCO-ENTITY-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENVMON-MIB.my
- CISCO-FRAME-RELAY-MIB
- CISCO-ISDN-MIB
- CISCO-MEMORY-POOL-MIB.my
- CISCO-MODEM-MGMT-MIB
- CISCO-PING-MIB
- CISCO-POP-MGMT-MIB
- CISCO-QUEUE-MIB.my
- CISCO-SMI.my
- CISCO-TC
- CISCO TOKEN RING MIB
- CISCO-SYSLOG-MIB
- CISCO-VPDN-MGMT-MIB
- DIAL-CONTROL-MIB
- ENTITY-MIB

- EXPRESSION-MIB
- FDDI-SMT73-MIB
- FSIP-MIB
- IF-MIB.mib
- OLD-CISCO-CPU-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-MEMORY-MIB
- PROCESS-MIB
- RFC-1212.mib
- RFC-1215.mib
- RFC1155-SMI.mib
- RFC1213-MIB.mib
- RFC1354-MIB.mib
- RFC1406-MIB
- RFC1407-MIB
- RFC1398-MIB
- RTT Mon MIB
- SONET-MIB

## Caveats for Cisco IOS Release 12.1 XM

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) XM7 are listed in [Table 6](#). For details about a particular caveat, go to Bug Toolkit at:

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

To access this location, you must have an account on Cisco.com. For information about how to obtain an account, go to the [“Cisco IOS Software Documentation Set”](#) section on page 27.

**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
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
CSCdu69834	<b>ip mtu adjust</b> should default to off
CSCds83208	NFAS test caused traceback: get_nfas_int
CSCdt67753	Need knob to disable automatic MTU adjustment added via CSCdr01713

## 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 open 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:  <a href="http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903">http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903</a>

## Open 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** Open Caveats for Release 12.1(5) XM6

Caveat ID Number	Description
CSCdv83040	RADIUS attribute 242 does not support protocol 50 and 51

## Resolved Caveats—Cisco IOS Release 12.1(5) XM6

All the caveats listed in [Table 8](#) 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 8** Resolved Caveats for Release 12.1(5) XM6

Caveat ID Number	Description
CSCdv16355	Missing VPN Disconnect Cause for Tunnel Setup Failures
CSCdv09157	Radius attribute 14 as string instead on integer
CSCds29417	snmp-server host ... broadcast traps to all configured hosts
CSCds36738	snmp views can be disabled, except those including/excluding iso
CSCdr08256	* is converted to 0 in the running config
CSCdu34146	%TTYDRIVER-3-NOPARTS NO particle available to set up for output
CSCdr85108	%MICA-3-NAK: NAK from modem 4 in state 0 -- payload 0x20
CSCdv08170	DS-RS go out of SYNC when analog calls are dropped
CSCdv30417	Some Mica modems stuck in DOWNLOAD SPE State, b(busiedout) PortState
CSCdv48261	Improvements to dynamic acls for ios fw
CSCdu48839	All snmp traps are displayed in running-config instead of hidden
CSCdv54898	Low CSR due to cot failures for a voice only system
CSCdv45035	Memory leak on 5300/5800 running ThunderVoice
CSCdu81936	Received gratuitous ARP overwrites interface MAC address in ARP tbl
CSCdv86243	Router shelf crashed while incoming E1-R2 call on Nextport
CSCdw01642	System restarted by bus error in l2x_ip_udp_fs, address 0xC
CSCdv75228	Unable to make outbound modem calls or use modemcap after voice call
CSCdv73152	Characters Tx is always 0
CSCdv51292	Upload big file failed after passing traffic for some time

## Open Caveats—Cisco IOS Release 12.1(5) XM5

All the caveats listed in [Table 9](#) are open in Cisco IOS Release 12.1(5) XM5. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

**Table 9** *Open Caveats for Release 12.1(5) XM5*

Caveat ID Number	Description
CSCdv30594	System reloads while attempting to reboot a DMM feature board

## Resolved Caveats—Cisco IOS Release 12.1(5) XM5

All the caveats listed in [Table 10](#) 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 10** *Resolved Caveats for Release 12.1(5) XM5*

Caveat ID Number	Description
CSCdt09214	Spurious memory access at vp_ipfib_fixup+0x20
CSCds48801	Dialer idle-timeout not working
CSCdt68534	bus error at PC 0x0, address 0x0 - serial_process_receive_packet
CSCdt46139	%ALIGN-1-FATAL: Corrupted program counter with virtual-profiles
CSCdu32284	PPP fails to start for some modem calls
CSCdu37471	RAI is not send out when signal channel is out of serv
CSCdu81278	AS5800 crashes at vpdn_add_acct_data
CSCdu59890	ISDN multilink PPP progress code error
CSCdu57960	span # of nas-port VSA populated incorrectly in egress NAS CDR
CSCdu70661	All channels except 24th channel stay busied out after configuration
CSCdu44831	Line card restarts during portware download
CSCdu48362	RS Rebooted by watchdog hard reset
CSCdu28726	ISDN layer 1 stuck at GOINGDOWN with data image
CSCds55069	V120 vty sessions are hanging
CSCdu30345	DSP stopped collection digits - phone # with 0 length
CSCdv09228	MGCP FAX failures-No Silence detection in Term GW
CSCdu63964	as5800 bus error at r4k_sig_dispatch+0xe0
CSCdt78894	Original stack is lost upon crash if there is another crash
CSCdv27964	Service messages are not generated when T1 port goes down
CSCdu86388	Constant Restart messages after reload of distant end nas
CSCdu40675	Buffer header leak on as5800
CSCdv01978	SPE recovery causes mica modems to become locked
CSCds33599	Modem recovery does not kick in case of no answer
CSCds59969	Router reloads in dialer_unlink_member

**Table 10** Resolved Caveats for Release 12.1(5) XM5 (continued)

Caveat ID Number	Description
CSCds07100	Null state after OIR of trunk card
CSCdu88651	Memory corruption crash

## Open Caveats—Cisco IOS Release 12.1(5) XM4

All the caveats listed in [Table 11](#) 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 11** Open Caveats for Release 12.1(5) XM4

Caveat ID Number	Description
CSCdt61467	Need a way to change the default value of VPDN parameters
CSCdu28545	Called phone not stop ringing for MICA only hairpinning call
CSCdu29251	Router Shelf reloaded at watchdog-timer after OIR test
CSCdu29502	Spurious Mem Access at rlm_link_weight_priority_insert_compare
CSCdu30345	DSP stopped collection digits - phone # with 0 length
CSCdu30363	Few modems enter SHUTDOWN/BAD state after 32Hrs of accepting Calls
CSCdu30864	DSIP Daemon Error found after clearing bulk calls on as5800
CSCdu32952	RS reloads with BUS EXCEPTION ERROR under high/mid load conditions
CSCdu44747	RS Reloads every couple of hours when left idle under mid-load cond
CSCdu48704	No ring back for call originated from IP phone and Netmeeting
CSCdu49767	Traceback messages when modem calls are disconnected
CSCdu53400	Incorrect count in sh call calltracker summ after digital call down
CSCdu55863	No busytone with no IVR/ no DID ISDN call
CSCdu57842	Router shelf crashes after watchdog timeout

## Resolved Caveats—Cisco IOS Release 12.1(5) XM4

All the caveats listed in [Table 12](#) 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 12** 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)
CSCds25539	Reload of DSC is not reflected in Router-Shelf
CSCds41324	Q931 Restart message allows OOS b channel to accept a call
CSCds55510	Memory Leak with AAA route download
CSCds63993	H323 GW: IP calls dangling when delay TCP connection occurs

**Table 12** Closed and Resolved Caveats for Release 12.1(5) XM4 (continued)

<b>Caveat ID Number</b>	<b>Description</b>
CSCds65611	All B-chan out of serv after controller no-shut then serial no-shut
CSCds71291	Spurious Accesses in mlp_timer
CSCds92116	5800 rtr reloads in tsp_cdapi_send_msg when doing hairpin calls
CSCdt11503	IOS crashes when large OID (>256 fields) is received
CSCdt24074	Removing primary NFAS PRI confign frm trnk cntlr causes spur mem acc
CSCdt40540	Cannot hairpin calls from isdn pri to SS7 without voice card
CSCdt41888	Add dlcx functionality as hidden command
CSCdt46181	Redzone corruption in pptp_tcp_readf()
CSCdt55611	E1 FB does not boot anymore
CSCdt63518	FIB-4-PUNTINTF msg for L2F/MP bundle member w no ip route-cache cef
CSCdt69055	B-channels IN_SERVICE after RESTART when L1 is DEACTIVATED
CSCdt72421	E1 Fb crash on m32x_drop_pkt
CSCdt82052	Need ani-dnis support in fgb
CSCdt82323	Bus error at entry_in_pw_dld_queue
CSCdt85341	TV: ISDN Bear channels are marked 1=Proposed while isdn negotiate
CSCdt89495	24th channel of T1 0 stays busied-out
CSCdt93000	Spurious memory access/Alignment errors
CSCdt96253	CRC-32 compensation vulnerability
CSCdt96945	Resource threshold information lost on GK after element failure
CSCdu00952	5850 crash in acct_periodic_update_data()
CSCdu05205	Memory corruption crash
CSCdu05236	Default disabling of parser cache should not be nvgened
CSCdu07504	<b>sh voice dsp</b> causes reload
CSCdu08214	Calltracker MIB returns NULL for userid when DNIS/ANI is not present
CSCdu12476	FB may stuck in np_bs_print_crash_info almost forever
CSCdu14000	Traceback at rlm_link_weight_priority_insert_compare after reload
CSCdu18348	UP324 Cards reboot after 20mins of stress
CSCdu20254	System returned to ROM by bus error at PC 0x60B59510
CSCdu22255	Crash at acct_periodic_update_data()
CSCdu23305	RLM flap results in Spurious mem access 0x60B6ECAC rlmc_up_state()
CSCdu25007	<b>clear spe</b> with calls running could have negative effects
CSCdu27780	AS5300 Suspend message not sent on H323 side with fax configured
CSCdu29246	ASSERTION FAILED at:./port-mgmt/pm_spe_as5800.c, line 538
CSCdu32972	E1 controller shows excessive bit errors
CSCdu34741	Term GW doesnt disconnect call which arrives after RLM is down
CSCdu35523	Disable AAA Command Accounting Periodic Timer

**Table 12** Closed and Resolved Caveats for Release 12.1(5) XM4 (continued)

Caveat ID Number	Description
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 13](#) 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 13** Open Caveats for Release 12.1(5) XM3

Caveat ID Number	Description
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 14](#) 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 14** Resolved Caveats for Release 12.1(5) XM3

Caveat ID Number	Description
CSCds66098	T1 on T3 controller broken with sf mode. Idle codes incorrect too
CSCdt20687	CSM rejects call to free timeslot
CSCds21035	Modem calls registered at 65535 speed
CSCds48164	Additional Stop record is reported for MLPPP and some PPP calls
CSCds59623	RLM/NFAS groups not on DSL 0 do not change to IN_SERVICE
CSCds72715	OIR testing deletes the d channel interface from config
CSCds81187	Memory leak in process PPP auth
CSCds90614	Modem state is not cleared if modem goes bad during active call
CSCdt06784	Reporting Address Signaling codes with ANI should be config option
CSCdt08905	CLI unusable due to voice resource not available debug
CSCdt31155	Instead of flashcard use of diskcard crashes router for clid_authen
CSCdt36362	RouterShelf crash at show_modem_all_stats() while doing <show modem>
CSCdt48613	DMM and Tetryl FBs get stuck in D state on bootup, and OIR
CSCdt54532	Cisco AS5800 crashed at LIF_dbg_getpkt_delta during stress test
CSCdt58403	RADIUS Attribute 196 shows progress code 65 instead of 60 for ISDN
CSCdt63613	Slow memory leak in PPP auth process
CSCdt65770	FB crash causes RS hang, then crash

**Table 14 Resolved Caveats for Release 12.1(5) XM3 (continued)**

Caveat ID Number	Description
CSCdt78731	DSP does not release DSO after an incomplete call for 30 seconds
CSCdt81585	Spur mem access at ct3sw_show_controllers()
CSCdt82360	Init Process take 80 percent of memory during bootup
CSCdu11970	Losing DSP resources due to INVALID counter mgmt - CAS corner case
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
CSCdt73099	Cisco AS5850: Very low CSR on CAS basic voice calls
CSCdt40308	Cisco AS5850: Some SPE hangs a when bringing up RPMS calls
CSCdt90565	Cisco AS5850: TV:SPE stuck after first modem call-out (regress CSCdt40308)
CSCdt73099	Very low CSR on CAS basic voice calls
CSCdt40308	Some SPE gets struck in a when bringing up RPMS calls
CSCdt90565	TV:SPE stuck after 1st modem call-out (regress CSCdt40308)

## 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 and 4 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.
- CSCdt16007  
Egress SS7 modem calls with Continuity Testing (COT) enabled fail to connect.  
Workaround: Disable COT on the Cisco SC2200.
- CSCdt25245  
On a Cisco 5800 with a PRI-to-PRI configuration or an SS7-to-PRI configuration with the session initiation protocol (SIP) Hairpinning feature and interactive voice response (IVR) enabled, there is no speech path and no ringback for the calls. For calls with IVR and Direct Inward Dialing (DID) disabled, there is a speech path and ringback.  
Workaround: Use the global configuration command **voice call send-alert**. This configures the alerting message to trigger ringback instead of the progress message.

- 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.

- CSCdt64373

When the **information-type fax** command is configured under a VoIP dial-peer, a fax-relay call cannot be setup.

Workaround: Do not use the **information-type fax** 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.

- 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.

- CSCdt11676

In an SS7 configuration, when modems are shut down on the calling router by issuing the command **spe 1/4 shut**, the following message shows on the console:

```
Spurious memory access made
```

There is no workaround.

This caveat is closed 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 the Cisco AS5800. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents.

Use these release notes with these documents:

- [Release-Specific Documents, page 26](#)
- [Platform-Specific Documents, page 27](#)
- [Feature Modules, page 27](#)
- [Cisco IOS Software Documentation Set, page 27](#)
- [Cisco IOS Software Documentation Set, page 27](#)

## 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 for Cisco IOS Release 12.1 XM” section on page 17](#)

As a supplement to the caveats listed in [“Caveats for Cisco IOS Release 12.1 XM”](#) in these release notes, see *Caveats for Cisco IOS Release 12.1* and *Caveats for Cisco IOS Release 12.1T*, which contains 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**

**Note**


---

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

---

## Platform-Specific Documents

These documents are available for the Cisco AS5800 on Cisco.com and the Documentation CD-ROM:

- *Read Me First—For Cisco AS5800 Universal Access Server*
- Hardware Installation Documents for the Cisco AS5800 Universal Access Server
- Configuration Documents for the Cisco AS5800 Universal Access Server
- *Cisco AS5800 Universal Access Server Regulatory Compliance and Safety Information*

On Cisco.com at:

**Technical Documents: Access Servers and Access Routers: Access Servers: Cisco AS5800**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5800**

## 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**

## 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**

## Cisco IOS Release 12.1 Documentation Set Contents

Table 15 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: Cisco IOS Software: Cisco IOS Release 12.1**

On the Documentation CD-ROM at:

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

**Table 15 Cisco IOS Release 12.1 Documentation Set**

Books	Major Topics
<ul style="list-style-type: none"> <li><i>Cisco IOS Configuration Fundamentals Configuration Guide</i></li> <li><i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management
<ul style="list-style-type: none"> <li><i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li><i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i></li> <li><i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i></li> </ul>	Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking

**Table 15 Cisco IOS Release 12.1 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i></li> <li>• <i>Cisco IOS Dial Services Configuration Guide: Network Services</i></li> <li>• <i>Cisco IOS Dial Services Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP and IP Routing Configuration Guide</i></li> <li>• <i>Cisco IOS IP and IP Routing Command Reference</i></li> </ul>	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i></li> </ul>	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i></li> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i></li> </ul>	Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Multiservice Applications Configuration Guide</i></li> <li>• <i>Cisco IOS Multiservice Applications Command Reference</i></li> </ul>	Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms Quality of Service Solutions

**Table 15 Cisco IOS Release 12.1 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide</i></li> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Security Overview</li> <li>Authentication, Authorization, and Accounting (AAA)</li> <li>Security Server Protocols</li> <li>Traffic Filtering and Firewalls</li> <li>IP Security and Encryption</li> <li>Other Security Features</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Cisco IOS Switching Services Overview</li> <li>Cisco IOS Switching Paths</li> <li>Cisco Express Forwarding</li> <li>NetFlow Switching</li> <li>MPLS Switching</li> <li>Multilayer Switching</li> <li>Multicast Distributed Switching</li> <li>Virtual LANs</li> <li>LAN Emulation</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Wide-Area Networking Overview</li> <li>Configuring ATM</li> <li>Configuring Frame Relay</li> <li>Configuring Frame Relay-ATM Interworking</li> <li>Configuring SMDS</li> <li>Configuring X.25 and LAPB</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Guide Master Index</i></li> <li>• <i>Cisco IOS Command Reference Master Index</i></li> <li>• <i>New Features in 12.1-Based Limited Lifetime Releases</i></li> <li>• <i>New Features in Release 12.1 T</i></li> <li>• <i>Cisco IOS Debug Command Reference</i></li> <li>• <i>Cisco IOS Dial Services Quick Configuration Guide</i></li> <li>• Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms)</li> </ul>	

# 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/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco 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](mailto: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 26.

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, Stratum, 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 © 2001–2002  
Cisco Systems, Inc.  
All rights reserved.