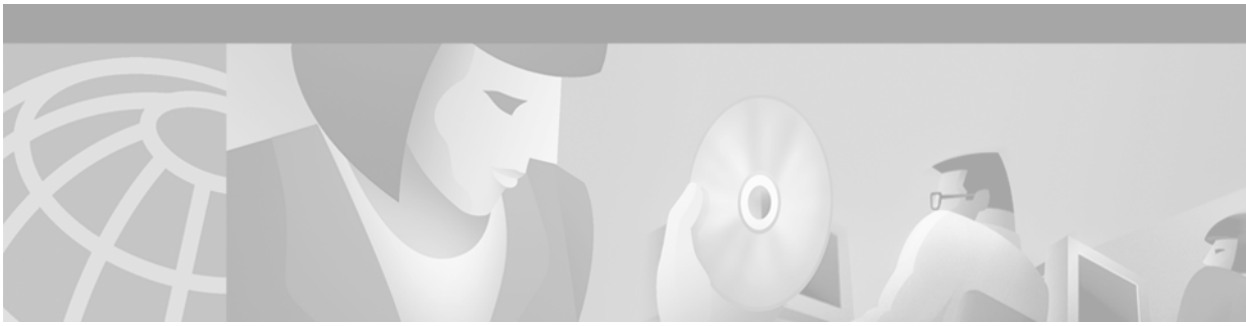

Release Notes for Cisco IAD2420 Series Integrated Access Device for Cisco IOS Release 12.2 XT

March 18, 2002

Cisco IOS Release 12.2(2) XT3

OL-1978-01 Rev. C0

Note You need to purchase a feature license to turn the Cisco Survivable Remote Site Telephony (SRS Telephony) and Cisco IOS Telephony Service Version 2.0 features on. You also need an account on Cisco.com to access the CiscoIPphone firmware versions.

These release notes for the Cisco IAD2420 series integrated access device describe the enhancements provided in Cisco IOS Release 12.2(2) XT3. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(2) XT3, see the "Caveats for Cisco IOS Release 12.2 XT" section on page 11 and *Caveats for Cisco IOS Release 12.2 T*. 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 12.2 T* located on Cisco.com and the Documentation CD-ROM.

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

Contents

These release notes describe the following topics:

Introduction

The Cisco IAD2400 Series Integrated Access Devices are fixed configuration multiservice customer premises equipment (CPE) platforms, targeted at emerging competitive local exchange carriers (CLECs), incumbent local exchange carriers (ILECs), and inter-exchange carriers (IXCs). The Cisco IAD2420 series enables service providers to cost effectively deploy next generation managed services for the growing needs of small and medium businesses (SMB) over a single high speed access link. The Cisco IAD2400 series products support both Voice over IP (VoIP) and Voice over ATM (VoAAL2), with high-density analog or digital voice interfaces.

The Cisco IAD2420 is an IP ONLY platform. It does not support other LAN protocols like IPX, Appletalk, or SNA. Additionally, the IAD2400 series only supports Simple Gateway control Protocol (SGCP) and Media Gateway Control Protocol 0.1 (MGCP). It does not support H.323 or session initiation protocol (SIP) for voice signaling.

The IAD series is a fixed configuration platform and comes with the required Flash memory and RAM for the operation of the platform. Customers do not need to acquire memory separately. Table 1 lists Cisco IAD2400 series product numbers with the corresponding WAN and telephony interfaces.

Table 1 Cisco IAD2400 Series Product Numbers

Product Number	WAN Interface	Telephony Interface
IAD2421-8FXS	T1	8 Analog FXS Ports
IAD2421-16FXS	T1	16 Analog FXS Ports
IAD2421-1T1	T1	1 T1 PBX Port
IAD2423-8FXS	ADSL	8 Analog FXS Ports
IAD2423-16FXS	ADSL	16 Analog FXS Ports

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.2(2) XT3, see the "New and Changed Information" section on page 6 and the "Related Documentation" section on page 20.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2 XT and includes the following sections:

Memory Recommendations

Table 2 lists memory recommendations for the Cisco IAD2420 series integrated access device.

Table 2 Memory Recommendations for the Cisco IAD2420 Series Integrated Access Device

Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
IP/ATM/VOIP/VOATM	c2420-a2i8sv5-mz	16MB Flash	16MB DRAM	RAM

Supported Hardware

Table 3 lists the supported interfaces for the Cisco IAD2420 series for Cisco IOS Release 12.2(2) XT3.

Each Cisco IAD2420 series router is preconfigured for one WAN port. The WAN port is either a T1 port or an asymmetric digital subscriber line (ADSL) port. Each Cisco IAD2420 is also preconfigured with either 8 or 16 foreign exchange station (FXS) analog voice ports or one T1 digital voice port for connection to a private branch exchange (PBX).

Table 3 Supported Interfaces on the Cisco IAD2420 Series

Interface, Network Module, or Data Rate		Platforms
WAN Interfaces	One T1 port (balanced, per ANSI T1.403) for connection to a WAN or carrier network	IAD2421
	One ADSL port for connection to a WAN or carrier network (DSLAM)	IAD2423
PBX Interfaces	One 8-line or 16-line analog FXS interface (loop-start or ground-start) for connection to analog phones, key systems, or PBXs.	IAD2421 and IAD2423
	One T1 port with channel-associated signaling (CAS) for connection to a digital PBX	IAD2421
Ethernet Interface	One 10BaseT LAN connection	IAD2421 and IAD2423
Serial Data Interface	One serial data interface for connections to WAN, or to user network. This interface supports HDLC, FR, or PPP encapsulations.	IAD2421 and IAD2423

Table 3 Supported Interfaces on the Cisco IAD2420 Series (continued)

Interface, Network Module, or Data Rate		Platforms
Administrative Interfaces	One EIA/TIA-32 asynchronous serial port for connection to a console	IAD2421 and IAD2423
	One EIA/TIA-32 asynchronous serial port for connection to a modem	IAD2421 and IAD2423

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco IAD2420 series integrated access device, log in to the Cisco IAD2420 series integrated access device and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 XT Software c2420-a2i8sv5-mz, Version 12.2(2) XT3, 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 the following URL:

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

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 12.2(2) XT3 supports the same feature sets as Cisco IOS Release 12.2(2) T, but Cisco IOS Release 12.2(2) XT3 can include new features supported by the Cisco IAD2420 series integrated access device.

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.

Table 4 lists the features and feature sets supported by the Cisco IAD2420 series integrated access device in Cisco IOS Release 12.2(2) XT3 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.

Table 4 Feature List by Feature Set for the Cisco IAD2420 Series Integrated Access Device

Features	In	Software Images by Feature Sets			
		IP	IP Plus	IP Plus IPSec 3DES	IP/FW/IDS Plus IPSec 3DES
Multiservice Applications - Voice					
Cisco IOS Telephony Service Version 2.0[1]	12.2(2) XT	No	Yes	Yes	Yes
Survivable Remote Site Telephony Version 2.0	12.2(2) XT	No	Yes	Yes	Yes

1. The feature name “Cisco IP Keys witch Version 2.0" has changed to “Cisco IOS Telephony Service Version 2.0" in Cisco IOS Release 12.2(2) XT. The command mode has changed from keyswitch configuration mode to telephony-service configuration mode.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco IAD2420 series integrated access device for Cisco IOS Release 12.2(2) XT3.

New Hardware and Software Features in Cisco IOS Release 12.2(2) XT3

No new hardware and software features are supported by the Cisco IAD2420 series integrated access device for Cisco IOS Release 12.2(2) XT3.

New Hardware and Software Features in Cisco IOS Release 12.2(2) XT2

No new hardware and software features are supported by the Cisco IAD2420 series integrated access device for Cisco IOS Release 12.2(2) XT2.

New Hardware and Software Features in Cisco IOS Release 12.2(2) XT1

No new hardware and software features are supported by the Cisco IAD2420 series integrated access device for Cisco IOS Release 12.2(2) XT1.

New Hardware Features in Cisco IOS Release 12.2(2) XT

No new hardware features are supported by the Cisco IAD2420 series integrated access device for Cisco IOS Release 12.2(2) XT.

New Software Features in Cisco IOS Release 12.2(2) XT

The following new software features are supported by the Cisco IAD2420 series integrated access device for Cisco IOS Release 12.2(2) XT:

Cisco IOS Telephony Service Version 2.0

Note The feature name “Cisco IP Keyswitch Version 2.0" has changed to “Cisco IOS Telephony Service Version 2.0" in Cisco IOS Release 12.2(2)XT. The command mode has changed from keyswitch configuration mode to telephony-service configuration mode.

Note You need to purchase a feature license to turn on the Cisco IOS Telephony Service feature. You also need an account on Cisco.com to access the CiscoIPphone firmware versions.

The Cisco IOS Telephony Service, under the IP Telephony services umbrella, provides basic Cisco IP phone call-handling capabilities in a LAN environment on the Cisco routers. This feature enables the Cisco multiservice routers to act as the Cisco IOS Telephony Service for the Cisco IP Phone 7960, Cisco IP Phone 7940, Cisco IP Phone 7910, and Cisco IP Conference Station 7935 and helps download phone software images, configures, and manages the Cisco IP phones in your LAN.

The Cisco IOS Telephony Service provides you with a telephony system perfect for a small office with a small number of extensions.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/ipkey2.htm

If you installed Cisco IOS Telephony Service Version 1.0 using Cisco IOS Release 12.1.5YD or 12.2.2XB, some commands have changed. You need to perform the following steps before you can upgrade your router image to 12.2(2)XT:

Step 1 Download the Cisco IOS 12.2(2)XT image to the Cisco IOS Telephony Service by entering the **copy tftp flash** command at the enabled prompt. Follow the instructions to download the image from the tftp server.

Step 2 Configure the Cisco IOS Telephony Service to boot from this new image by entering the following at the enabled prompt:

```
Router# configure terminal
Router(config)# boot system flash new image name
```

Step 3 Remove the configuration for booting from the original image, if configured, by entering the following:

```
Router(config)# no boot system flash original image name
Router(config)# end
```

Step 4 Save the configuration by entering **write memory** at the enabled prompt.

Step 5 Upload the running configuration on the Cisco IOS Telephony Service to a tftp server by entering the **copy running-config tftp** command at the enabled prompt and following the instructions.

Step 6 Edit the running configuration file on the tftp server by using a text editor to change the word “keyswitch” to “telephony-service.”

Step 7 Download the edited running configuration file to the Cisco IOS Telephony Service by entering **copy tftp startup-config** at the enabled prompt and following the instructions.

Step 8 Reload the Cisco IOS Telephony Service by entering **reload** at the enabled prompt. Enter **no** if you are prompted to save the configuration.

If the configuration register is not set to x2 or x2102, but is set to 0x0 instead, you need to boot the router from ROMMON by performing the following steps:

Step 1 Upload the running configuration on the Cisco IOS Telephony Service to a tftp server by entering **copy running-config tftp** at the enabled prompt and following the instructions.

Step 2 Edit the running configuration file on the tftp server by using a text editor to change the word "keyswitch" to "telephony-service."

Step 3 Download the edited running configuration file to the Cisco IOS Telephony Service by entering **copy tftp startup-config** at the enabled prompt and following the instructions.

Step 4 Download the Cisco IOS 12.2(2)XT image to the Cisco IOS Telephony Service by entering the **copy tftp flash:/slot0** command at the enabled prompt. Follow the instructions to download the image from the tftp server.

Step 5 Reload the Cisco IOS Telephony Service by entering **reload** at the enabled prompt. Enter **no** if you are prompted to save the configuration.

Step 6 Boot the Cisco IOS Telephony Service by entering the **boot flash:/slot0:***image-name* command at ROMMON prompt.

Survivable Remote Site Telephony Version 2.0

The Survivable Remote Site (SRS) Telephony feature, under the IP Telephony services umbrella, provides the Cisco CallManager with fallback support for the Cisco IP phones attached to the Cisco router on your local Ethernet. The SRS Telephony feature enables the routers to provide call handling support for the Cisco IP phones when the Cisco IP phones lose connection to the remote primary, secondary, or tertiary Cisco CallManager or when the WAN connection is down.

Cisco CallManager 3.0 supports Cisco IP phones at remote sites attached to Cisco branch office multiservice routers across the WAN. Prior to the SRS Telephony feature, when the WAN connection between the remote branch office router and the Cisco CallManager failed or connectivity with the Cisco CallManager was lost for some reason, the Cisco IP phones at the branch office became unusable for the duration of the failure. The SRS Telephony feature overcomes this problem and enables the basic features of the Cisco IP phones by providing call-handling support on the branch office router for its attached Cisco IP phones. The system automatically detects the failure and uses the Simple Network Auto Provisioning (SNAP) technology to autoconfigure the branch office router to provide call processing for the local Cisco IP phones. When the WAN link or connection to the primary Cisco CallManager is restored, call-handling capabilities for the Cisco IP phones switch back to the primary Cisco CallManager. During a failure when SRS Telephony feature is enabled, the Cisco IP phone displays a message to inform you that the Cisco IP phones are in the Cisco CallManager fallback mode and are able to perform limited functions.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/srs/fallbak2.htm

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 5.

Table 5 Deprecated and Replacement MIBs

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

Limitations and Restrictions

Caveat CSCdr91706 and IOS HTTP Vulnerability

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to http://router-ip/anytext?/ is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.

The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect.

This vulnerability can only be exploited if the enable password is known or not set.

You are strongly encouraged to read the complete advisory, which is available at

http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2 XT that can apply to the Cisco IAD2420 series integrated access device.

Product Number Change

Beginning with Cisco IOS Release 12.0(7)XK, Cisco changed the product numbers used to order a specific Cisco IOS software image. In short, Cisco will remove the periods separating the release train, maintenance release, and build number. The following table provides some examples.

Old Product Number	New Product Number	Release	Image Description
S364AR1K2-12.1.5=	S364AR1K2-1215=	Cisco IOS Release 12.1(5)	Cisco 3640 Series IOS Enterprise/SNA SW PLUS IPSEC 3DES
S26CP-12.1.5=	S26CP-1215=	Cisco IOS Release 12.1(5)	Cisco 2600 Series IOS IP Plus

Changes to Feature Support with Cisco IOS Release 12.2(2) XT

Cisco IOS Release 12.2(2)XT does not support the following features:

- Remote Source-Route Bridging (RSRB)
- AppleTalk
- Apollo Domain
- Banyan Virtual Integrated Network Service (VINES)
- DECnet
- Xerox Network Systems (XNS)
- LAN Emulation
- LAT
- XRemote

Caveats for Cisco IOS Release 12.2 XT

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

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

All caveats in Cisco IOS Release 12.2 and Cisco IOS Release 12.2 T are also in Cisco IOS Release 12.2(2) XT3.

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*.

For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, l**og in** to Cisco.com and click **Service and Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Open Caveats—Cisco IOS Release12.2(2) XT3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2) XT3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx04374

  If CLNS is configured on the SVI interface (Vlan), the SNPA/MAC is not learned correctly by the router in which the SVI is present. This results in the router sending packets to a non-existent destination MAC address.

  There is no workaround.

- CSCdw46537

  Symptom:

  SPAN doesn’t work after moving one port from multi span src ports. Disabling a source interface from a monitor session results in disabling the entire monitor session, not just the specified port.

  Workaround:

  If a particular source port is required to be removed form a SPAN session, stop the entire SPAN session and re-configure with only the required source ports.

- CSCdw29549

  Symptom:

  Port security failed when configuring secure MAC addresses on an irrelevant port. When Port Security is configured on two interfaces P1 & P2, and secure MAC addresses M1 & M2are configured on interfaces P1 & P2 respectively, P1 should only allow packets with source MAC address M1 and P2 should only allow M2. But if a packet with secure MAC address M1 ingresses port P1, then the switch treats it like a station movement and allows the packet to be switched.

  Workaround:

  Cisco Systems recommends that when station movement takes place, the MAC addresses associated with the port should be cleared in the switch's tables before moving them to another port.

- CSCdw14813

  Symptom:

  The command **show mac count** shows the wrong number of MAC addresses when compared to the count of addresses shown by the **show mac** command.

  There is no workaround.

- CSCdw20431

  Symptom:

  Traceback is seen on configuring the duplex and speed.

  There is no workaround.

Resolved Caveats—Cisco IOS Release12.2(2) XT3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2) XT3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv24152

  Symptom:

  A Cisco router that is running Cisco IOS Release 12.0(17)S and later 12.0 S releases may reset if Frame Relay has been incorrectly configured. If you apply the same data link control (DLC) value on an interface and on its subinterface twice in a row, the router may reset.

  There is no workaround.

- CSCdw14262

  Symptom:

  Cisco Voice over IP (VoIP) gateways that are running a Cisco IOS Release 12.2(1a) IP plus image may experience a high central processing unit (CPU) memory utilization condition at the CCH323_CT process.

  There is no workaround.

- CSCin02687

  Symptom:

  When using the Cisco 7200 series router as a Survivable Remote Site Telephony (SRST) and IOS telephony service router and making more than 30 three-party conference calls, the router crashes. The tracebacks point to the fast-ethernet interface that is being used to connect the router to the IP phones or rather the IP phone simulator.

  Workaround:

  Restrict the number of three-party conference calls.

- CSCdv62649

  Symptom:

  The command **ip tacacs source-interface** does not work properly.

  Workaround:

  If configured to use loopback interface for tacacs packets, the router may still use the interface address.

- CSCdw08182

  Symptom:

  The VWIC installed in NM-1FE2W appears in **show diag** response but not in the configuration.

  The router is recognizing that it has a VWIC-1MFT-T1 in a NM-1FE2W in the show diag. The problem is that the T1 controller doesn't appear in the configuration. The FastEthernet is present.

  There is no work-around.

- CSCdw26331

  Symptom:

  A call to a busy FXS port produces an incorrect release cause code. Calls may receive a "no route to destination" message and an incorrect clearing cause code (instead of a user busy cause code) when calls are placed to a Foreign Exchange Station (FXS) on a busy interface. Depending on the equipment that is used, the caller may receive a "number unobtainable" message or fast busy tones instead of a busy tone when this condition occurs.

  Workaround:

  Add a huntstop on the dial peer that is assigned to the FXS interface.

- CSCdw38767

  Symptom:

  Some ports on the NM-16ESW / NMD-36-ESW may not be assigned MAC addresses properly.

  Conditions:

  This occurs when the last digit of the base MAC address burnt in the NM cookie is in the range 0xF0-0xFF for NM-16ESW and range 0xDA-0xFF for NMD-36-ESW.

  Workaround:

  None.

- CSCdw46803

  Symptom:

  After a Cisco 1751 router that is running Cisco IOS Release 12.2(2)XT and that has a BRI network termination/traffic engineering (NT/TE) is reloaded, Layers 1 and 2 may become deactivated.

  Workaround:

  Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the BRI interface.

- CSCdw51152

  Symptom:

  PCI Fatal Error on DMA CH1

  When access to Flash/NVRAM occurs as a result of **write memory** or **show run** commands, and the CPU utilization is high due to heavy packet traffic, this error message can sometimes occur.

  This is due to the PCI device timing out on the PCI bus waiting for DMA access to memory.

  Workaround:

- CSCdu53333

  Symptom:

  A Cisco router that is running Cisco IOS Release 12.2(1) or 12.2(0.5g) may experience digital signal processor (DSP) reloads or fail to respond after the following DSP Timeout error messages are displayed:

  > %VTSP-3-DSP_TIMEOUT: DSP timeout on event 6: DSP ID=0x1: DSP error stats, chnl info(5, 13, 0) %VTSP-3-MSGSNDFAIL: channel:5/0:15 (54516) DSP ID:0x1 Message ID:0x47

  The problem is intermittant, and DSPs may hang indefinitely as rarely as only once every few weeks. The problem is likely to appear when T.38 fax mode is used and is likely to appear when "codec complexity medium" is configured for the voice card and there is frequent switching between the fax and voice modes.

  Workaround:

  This DSP firmware defect is fixed in DSP Release 3.6.15 / VCWare Release 9.19 and DSP Release 3.4.49 / VCWare Release 7.38, as well as newer versions of these firmware releases.

- CSCdw54986

  Symptom:

  A router with primary-ni switchtype will not be able to interoperate with switches that sends CLID/CLIP/CLIR information in FACILITY messages. The router does not accept the FACILITY and disconnects the call.

  Workaround:

  None

- CSCdw57198

  Symptom:

  SRST router with FXO ports typically has a connection plar (opx) to route an incoming call on the port to an extension in the router. With this problem, the incoming call cannot be transferred.

  There is no workaround.

- CSCdw62829

  Symptom:

  The High-Density Analog Voice/Fax Network Modules (NM-HDA) for the Cisco 2600 series and Cisco 3600 series routers support Local Voice Busyout (LVBO) features. The **busyout monitor** command can be configured under NM-HDA voice-ports to permit busyout monitoring of local interfaces or remote IP interfaces via Service Assurance Agent (SAA) probes. These features can be configured and can be saved to Non-Volatile RAM (NVRAM) successfully, but on a router reload, the boot-time parser rejects the **busyout monitor** commands.

  Any **busyout monitor** command configured under a voice-port on a NM-HDA will disappear from the running-configuration if the router is rebooted. This problem does not occur on VIC-2E/M, VIC-2FXS, and VIC-2FXO voice-ports housed on the NM-1V and NM-2V products.

  Workaround:

  Issue a **copy startup-config running-config** to re-assert the missing commands.

- CSCdw70410

  Symptom:

  A Cisco router may reload after a high-density analog voice or fax network module (NM-HDA) that is installed in a slot is replaced by another NM-HDA that has a different hardware configuration.

  Workaround:

  Use a replacement card that is the same as the original card. This condition will not occur if a card that is the same as the original is used or if a differently configured card is placed in a different slot.

- CSCdw71436

  Symptom:

  Under rare circumstances, a Cisco router may reload because of a segmentation violation (SegV) when fax calls are present.

  There is no workaround.

- CSCdw73302

  Symptom:

  When using a TCL IVR 2.0 application on a Cisco voice gateway for 2-stage calls, the configured translation rule may be applied for each received digit, instead of only for the initial digit.

  Workaround:

  None

- CSCdw73507

  Symptom:

  Ringback is not available for calls coming in from a PSTN. IP phones do not ringback on the network side. When a call comes in from a PSTN, the call should tell the PSTN end so that it can generate ringback on behalf of the IP phones by sending progress ind as 3.

  Workaround:

  None

- CSCdw75065

  Symptom:

  Alignment traceback when transfer and conference call. Tracebacks are observed during conference and at times, during regular calls. The tracebacks are on misaligned accesses to memory.

  Workaround:

  They are subsequently corrected by the hardware but prints to console are annoying and can be viewed as serious potential issues.

- CSCdw82677

  Symptom:

  Bad voice-quality during conference call. This happens when a Survivable Remote Site Telephony (SRST) ITS GW with loop-back-dns is used in conferencing with a remote GW and where a mis-match of codec types results if the GWs do not have the same codec type configured. Conferencing a-law and u-law mixes doesn't work as some legs in ITS end up with a-law and some with u-law which gives bad voice quality.

  Workaround:

  This fix is only applicable for a network that has a mixture of A-law and U-law codecs configured in the network. Configure all gateways in the network to use same codec type of either A-law or U-law.

- CSCdw84594

  Symptom:

  Show diag for Cisco 2600 series routers gives wrong values for NMs which uses TLV_IDPROM. This problem is only on Cisco 2600 series platform

  Conditions:

  While issuing **sh diag <slot>** command, HDA uses TLV_IDPROM. The hardware version, revision information, and other conditions are displayed wrongly.

  Workaround:

  None

- CSCdw85359

  Symptom:

  Caller ID is discarded when an incoming PSTN call through FXO-M1/FXS-M1 is transferred to another number. The Caller-ID displayed after the transfer is "From Private....".

  Workaround:

  None:

- CSCdx01445

  Symptom:

  The port does not go on-hook when a supervisory disconnect tone is sent from the PSTN. When call comes in through FXO port to IP Phone, the IP Phone goes into Alerting state. If the caller hangs up at this point, the PSTN sends a supervisory disconnect tone to the FXO where no action is taken which results in not freeing up the port immediately.

  Workaround:

  None

- CSCuk31298

  Symptom:

  The IP phone locks during a call to a call forward busy number. This condition occurs in a setup whereby the call forward busy feature is configured using the Cisco IOS Telephony Service (ITS) on an IP phone (phone A) to a second IP phone (phone B). When a call is made from phone A to another phone (phone C), the call can be answered normally.

  When a second call is placed from another phone to phone A via a loopback-directory number (loopback-dn), the call is forwarded to phone B. As this call is received, the original call is incorrectly cleared by the node on phone C while the call is still shown as “up” on phone A. When this condition occurs, phone A is no longer able to place or receive calls and has to be powered down to be restored to working condition.

  Workaround:

  This condition affects only the first IP phone in the internal control table on the router. The first IP phone is typically indicated as “ephone 1” when the **show ephone** EXEC command is issued.

  To prevent this condition from occurring when the router is operating in the ITS mode, add a dummy phone entry as the first IP phone or “ephone 1” in the internal control table on the router to prevent an active phone from being listed as the first IP phone in the internal control table of the router.

  Reload the router to ensure that the dummy phone occupies the first position in the control table. There is currently no workaround to this condition if the router is operating in the Survivable Remote Site Telephony (SRST) mode (call manager fall back).

- CSCuk31300

  Symptom:

  Ringing presented to caller before state of called number is known.

  When using loopback-dns for outgoing calls, the router presents a ringing tone to the IP phone caller as soon as the call has been routed and before the state of the called number is known.

  If the called number is busy, this can result in a ringing and then busy tone being played to the caller. This does not happen if loopback-dns are not used, or if they are used for incoming calls.

  Workaround.

  Do not use loopback-dns for outgoing calls.

- CSCuk31512

  Symptom:

  On a miss dialed call transfer, a new call shows previously dialed digits.

  When a Keyswitch IP phone user receives an incoming call, and they then attempt to transfer that call, but while dialling they realize they are dialling a wrong number, the transferrer has two options. If they incorrectly select "New Call", the phone displays the previous dialed digits. If the caller then dials more digits, these appear after the previous digits. The phone however only dials the digits presented after the "New Call" button was pressed, and the call is successful.

  Workaround.

  None

- CSCuk31658

  Symptom:

  On three-way calls setup by a Survivable Remote Site Telephony / Keyswitch IP phone, if the second call leg to be setup clears their call, the speech path from the IP phone where the conference was setup to the other phone is lost. The problem is observed only when the second call clears, and only if another IP phone is used in addition to the IP phone which set the conference up. Voice path is re-established if the phone that initiated the conference temporarily places the remaining caller on-hold and then immediately resumes the call.

  Workaround:

  None

- CSCdw62185

  This release integrates the DSPware 3.6.15 release. Upgrading to the DSPware 3.6.15 release to fix CSCdu53333 (dsp timeout) remedies the voice quality problem in this caveat.

Open Caveats—Cisco IOS Release12.2(2) XT2

There are no open caveats specific to Cisco IOS Release 12.2(2)XT2 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release12.2(2) XT2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XT2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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 12.2(2) XT1

There are no open caveats specific to Cisco IOS Release 12.2(2) XT that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(2) XT1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2) XT1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv48261

  The IOS Firewall Feature set, also known as Cisco Secure Integrated Software, also known as Context Based Access Control (CBAC), and introduced in IOS version 11.2P, has a vulnerability that permits traffic normally expected to be denied by the dynamic access control lists.

  This vulnerability is documented as Cisco Bug ID CSCdv48261.

  No other Cisco product is vulnerable.

  There is no workaround.

  This advisory is available at

  http://www.cisco.com/warp/public/707/IOS-cbac-dynacl-pub.shtml

- CSCdv90919

  Problem is occurring when the customer is attempting to receive dial-tone on ISDN trunks. The method that the customer uses to obtain this dial-tone is to configure the ISDN trunks for overlap-receiving, and send in a setup message with no called party number. The connected PBX then allows the calling party to hear this dial-tone, but continues to collect digits, which will be sent over the ISDN link as INFO messages. In this case, if the router has an incoming dial-peer that has an exact match to the calling party number, a PI value is not returned in the SETUP_ACK message. This causes the dial-tone from the router to not be heard.

  There is no workaround.

Open Caveats—Cisco IOS Release 12.2(2) XT

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

- CSCdw04503

  Call-forward commands not entered for E164 dial-peers.

  When dialplan pattern is configured for the local IP Phones, the existing call-forward commands under ephone-dn are not entered under the E.164 dial-peers created by the dialplan pattern command. This can cause a call not getting forwarded if you dial the entire E164 number.

  This problem happens only if you add or edit the existing dialplan pattern with call-forward commands already in place. One way to avoid this problem is to configure the right dialplan pattern before configuring the call-forward commands. Additionally, if you modify the dialplan pattern commands, configure the call forward commands again under ephone-dn. This creates the call-forward commands under the E164 dial-peers created.

- CSCdv78130

  Inconsistent music on hold (MOH) during conference.

  Music on hold works inconsistently in certain conditions. A calls B and conferences to C. B puts the conference on hold. Both A and C hear the MOH. B resumes the call and after a while puts the conference on hold again. Now only A (initiator) hears the MOH.

  There is no workaround.

- CSCdv72916

  Remote branch Analog Phone to IP Phone call disconnected during CM reconnect.

  Calls from Analog Phone to IP Phone during call-manager-fallback mode may get disconnected when the WAN link to CM comes back up. If a call is made in “normal mode” and the WAN link fails, the call stays up even though the WAN link failed. If the WAN link comes back up during the call and the call is between two IP phones or two analog phones, the call is not dropped. However, if the call is between an IP phone and an analog phone, the call is dropped.

  There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(2) XT

There are no resolved caveats specific to Cisco IOS Release 12.2(2) XT that require documentation in the release notes.

Related Documentation

The following sections describe the documentation available for the Cisco IAD2420 series integrated access device. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

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

Use these release notes with these documents:

- Release-Specific Documents, page 20
- Platform-Specific Documents, page 21
- Feature Modules, page 21
- Cisco IOS Software Documentation Set, page 22

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2: Release Notes: Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2: Release Notes**: **Cross-Platform Release Notes**

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

  Technical Documents

- Section “Caveats for Cisco IOS Release 12.2 XT” in these release notes

As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2 XT" in these release notes, see *Caveats for Cisco IOS Release 12.2*. and *Caveats for Cisco IOS Release 12.2 T*, which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2 and Cisco IOS Release 12.2 T.

On Cisco.com at:

Technical Documents: Cisco IOS Software: **Cisco IOS Release 12.2: Release Notes: Caveats**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2: Caveats**

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

Platform-Specific Documents

These documents are available for the Cisco IAD2420 series integrated access device on Cisco.com and the Documentation CD-ROM:

- Cisco IAD2420 Series Quick Start Guide
- Cisco IAD2420 Series Software Configuration Guide
- Cisco IAD2420 Series Hardware Installation Guide
- Cisco IAD2420 Series Regulatory Compliance and Safety Information

On Cisco.com, beginning under the **Service & Support** heading:

Technical Documents: Access Servers and Access Routers: Integrated Access Devices: Cisco IAD2420 Series IADs

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Integrated Access Devices: Cisco IAD2420 Series IADs

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(2) XT3 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2: New Feature Documentation**

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

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

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

Cisco IOS Release 12.2 Documentation Set Contents

Table 6 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

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

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2

Table 6 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB[1] DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server

Table 6 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Dial Technologies Configuration Guide: Dial Access* • *Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications* • *Cisco IOS Dial Technologies Command Reference, Volume 1 of 2* • *Cisco IOS Dial Technologies Command Reference, Volume 2 of 2*	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing IP Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk[1] Novell IPX
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs

Table 6 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation[1]
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT[1] NASI Telnet TN3270 XRemote[1] X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • *New Features in Release 12.2 T* • *Release Notes* (Release note and caveat documentation for 12.2-based releases and various platforms)	

1. Not supported in Cisco IOS Release 12.2(2)XT.

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

- 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 "Obtaining Documentation" section on page 25.