Release Notes for Cisco IAD2430 Series Integrated Access Devices for Cisco IOS Release 12.2(15)ZJ5

April 26, 2004

Cisco IOS Release 12.2(15)ZJ5

OL-4333-01 Rev G0

These release notes for the Cisco IAD2430 Series Integrated Access Devices (IAD) describe the product-related enhancements provided in Cisco IOS Release 12.2(15)ZJ5. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(15)ZJ5, see Caveats for Cisco IOS Release 12.2(15)ZJ, page 22. See also *Caveats for Cisco IOS Release 12.2 T*, which is updated for every maintenance release and is 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.

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html.

Note Cisco IOS Release 12.2(15)ZJ5 is the last scheduled maintenance release for Cisco IOS Release 12.2(15)ZJ. TAC support will continue to be available. These release notes will be the last release notes published for Cisco IOS Release 12.2(15)ZJ.

Contents

These release notes describe the following topics:

Cisco Systems

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

Inheritance Information

Cisco IOS Release 12.2(15)ZJ5, an early deployment release, is based on Cisco IOS Release 12.2(15)T, which in turn is based on Cisco IOS Release 12.2. Cisco IOS Release 12.2(15)T is the sixth early deployment maintenance release of Cisco IOS Release 12.2 T and is based on the mainline Cisco IOS Release 12.2.

All features in Cisco IOS Release 12.2(15)T are in Cisco IOS Release 12.2(15)ZJ5.

Table 1 References for the Cross-Platform Release Notes for Cisco IOS Release 12.2 T and Cisco IOS Release 12.2(15)T

Topic	Location
• Determining the Software Version • Upgrading to a New Software Release	To view information about the topics in the left-hand column, click **Cross-Platform System Requirements** at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122treqs.htm
• New and Changed Information (Feature Descriptions) • MIBs • Important Notes	To view information about the topics in the left-hand column. For Cisco IOS Release 12.2 T, go to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122tnewf.htm Scroll down and click **New Software Features in Cisco IOS Release 12.2(15)T**, or **MIBs**, or **Important Notes**.
• Related Documentation • Obtaining Documentation • Obtaining Technical Assistance	To view information about the topics in the left-hand column, go to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122tdocs.htm

Introduction

For information on new features supported by Cisco IOS Release 12.2(15)ZJ5, see "New and Changed Information" section on page 10.

Cisco IOS Release 12.2(15)ZJ5 supports the Cisco IAD2430 Series Integrated Access Devices.

The Cisco IAD2430 is the next generation integrated voice and data services platform for Service Providers, building on the industry leading Cisco IAD2420 series IAD. The Cisco IAD2430 series offers a major leap forward in price performance and enhanced SW functionality such as MGCP SRST used to accelerate the migration from TDM to VoIP cost efficiently. The Cisco IAD2430 series harnesses the maturity of the Cisco IAD2420 series software and enhances functionality by providing more capabilities such as denser interfaces (up to 24 FXS or up to 2 voice and 2 data T1s), encryption, and DC power back up while maintaining it's 1RU form factor for space saving Service Provider Managed Services deployment.

Cisco 2430 Series Integrated Access Device

The Cisco IAD2430 Series Integrated Access Device consists of the following five models:

- Cisco 2430-24FXS IAD
- Cisco 2431-8FXS IAD
- Cisco 2431-16FXS IAD
- Cisco 2431-1T1E1 IAD
- Cisco 2432-24FXS IAD

The supported WAN interface cards (WICs) and Voice Interface Cards (VICs) are:

- WIC-2T
- WIC-1DSU-T1
- VIC2-4FXO

See Table 4 on page 6 for information on supported voice interfaces, WAN interfaces, and ports for the Cisco IAD2430 Series Integrated Access Devices.

Note Unlike the Cisco IAD2420 Series IAD, the Cisco IAD2430 series IAD does not include serial or DSL ports. Serial connectivity is available through WIC-2T. See Unsupported Features, page 20 for a list of all unsupported features in Cisco IOS Release 12.2(15)ZJ.

Port Numbering

Port numbering conventions for the Cisco IAD2430 Series Integrated Access Device differs from the Cisco IAD2420 Series Integrated Access Device:

- An external compact flash card is numbered slot 0.
- 10/100Base-T Fast Ethernet ports are numbered Fast Ethernet 0/0 and Fast Ethernet 0/1 from right to left.
- T1/E1 ports are numbered T1 or E1 1/0 and T1 or E1 1/1 from right to left.
- The slot for WICs and VICs is numbered slot 0. WIC and VIC interfaces are numbered by interface face with this slot number and an interface number, beginning with 0 and running from right to left.

- FXS voice port numbering begins at 2/0 and extends to 2/7, 2/15, or 2/23, depending on the number of voice ports.

MGCP Endpoint Naming Convention

The Media Gateway Control Protocol (MGCP) endpoint naming convention for Cisco IAD2430 Series IAD differs from the Cisco IAD2420 Series IAD. The MGCP naming convention for the Cisco IAD2430 Series IAD is the following:

Cisco IAD2431-1T1E1

S1/DS1-0/1@iad2430-digital
S1/DS1-0/2@iad2430-digital
. . .
S1/DS1-0/24@iad2430-digital

S1/DS1-1/1@iad2430-digital
S1/DS1-1/2@iad2430-digital
. . .
S1/DS1-1/24@iad2430-digital

Cisco IAD2430-24FXS, IAD2431-8FXS, IAD2431-16FXS, IAD2432-24FXS

AALN/S2/0@iad2430-analog
AALN/S2/1@iad2430-analog
. . .
AALN/S2/23@iad2430-analog

Voice Analog Ports

AALN/S0/0@iad2430-analog
AALN/S0/1@iad2430-analog
AALN/S0/2@iad2430-analog
AALN/S0/3@iad2430-analog

Early Deployment Releases

These release notes describe Cisco IOS Release 12.2(15)ZJ5 for the Cisco IAD2430 Series Integrated Access Devices. Cisco IOS Release 12.2(15)ZJ5 is an early deployment (ED) release based on Release 12.2(15)T, which in turn is based on Cisco IOS Release 12.2. Early deployment releases contain fixes to software caveats as well as support for new Cisco hardware and software features. Feature support is cumulative from release to release, unless otherwise noted.

Table 2 lists features supported by the Cisco IAD2430 Series Integrated Access Devices in Cisco IOS Release 12.2(15)ZJ5. See *Platform-Specific Documents, page 37* for a list of the documentation specific to the Cisco IAD2430 Series Integrated Access Device.

Table 2 Early Deployment (ED) Releases for the Cisco IAD2430 Series Integrated Access Devices

ED Release	Additional Software Features[1] and MIBs[2]	Additional Hardware Features	Hardware Availability
Cisco IOS Release 12.2(15)ZJ3	• Cisco CallManager Express 3.0	None	NA
Cisco IOS Release 12.2(15)ZJ2	None	None	NA

Table 2 Early Deployment (ED) Releases for the Cisco IAD2430 Series Integrated Access Devices (continued)

ED Release	Additional Software Features[1] and MIBs[2]	Additional Hardware Features	Hardware Availability
Cisco IOS Release 12.2(15)ZJ1	None	None	NA
Cisco IOS Release 12.2(15)ZJ	• Cisco CallManager Express (CME) Version 3.0 • Cisco SIP Survivable Remote Site Telephony (SRST) • Cisco Survivable Remote Site Telephony (SRST) Version 3.0 • **tftpdnld -r** ROM monitor command • **fpga-pref** ROM monitor command (new) • **network-clock-participate** command	• Cisco 2430-24FXS IAD • Cisco 2431-8FXS IAD • Cisco 2431-16FXS IAD • Cisco 2431-1T1E1 IAD • Cisco 2432-24FXS IAD	Now

1. Only major features are listed.
2. MIB = Management Information Base

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(15)ZJ and includes the following sections:

- Memory Recommendations, page 5
- Supported Hardware, page 6
- Determining Your Software Release, page 8
- Upgrading to a New Software Release, page 8
- Feature Support, page 8

Memory Recommendations

Table 3 displays the memory recommendations of the Cisco IOS feature sets for the Cisco IAD2430 Series Integrated Access Devices for Cisco IOS Release 12.2(15)ZJ.

Cisco IAD2430 Series Integrated Access Devices are available with a 32-MB or 64-MB Flash memory card.

Table 3 Memory Recommendations for the Cisco IAD2430 Series Integrated Access Devices for Cisco Release 12.2(15)ZJ

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Cisco IAD2430 Series IOS IP subset/Voice	c2430-i6s-mz	32 MB	64 MB	RAM
Cisco IAD2430 Series IOS IP subset/IPSEC 64bit/FW/Voice	c2430-i6k9o3s-mz	32 MB	64 MB	RAM

Table 3 Memory Recommendations for the Cisco IAD2430 Series Integrated Access Devices for Cisco Release 12.2(15)ZJ (continued)

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Cisco IAD2430 Series IOS IP PLUS	c2430-is-mz	64 MB	128 MB	RAM
Cisco IAD2430 Series IOS IP PLUS/IPSEC 64bit/FW/Voice	c2430-ik9o3s-mz	64 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(15)ZJ supports the following Cisco IAD2430 Series Integrated Access Devices:

- Cisco 2430-24FXS IAD
- Cisco 2431-8FXS IAD
- Cisco 2431-16FXS IAD
- Cisco 2431-1T1E1 IAD
- Cisco 2432-24FXS IAD

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 10.

Each Cisco IAD2430 Series router is preconfigured for one wide-area network (WAN) port. The WAN port is either two T1 ports or an IDSU port. Cisco IAD2430 is also preconfigured with up to 24 foreign exchange station (FXS) analog voice ports and/or twoT1 digital voice ports for connection to a private branch exchange (PBX).

Table 4 lists the supported interfaces for the Cisco IAD2430 Series IAD for Cisco IOS Release 12.2(15)ZJ5.

For additional information about supported hardware for this platform and release, refer to the Hardware/Software Compatibility Matrix in the Cisco Software Advisor at the following location:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Table 4 Supported Interfaces on the Cisco IAD2430 Series Integrated Access Device

Interface and Port	Product Description	Supported IAD2430 Models
Interfaces Common to All Models		
10/100BASE-T Fast Ethernet Port	All Cisco IAD2430 Series models have two 10/100BASE-T Fast Ethernet ports except for Cisco2431-8FXS IAD, which has one.	All
Console and auxiliary ports	One EIA/TIA-32 asynchronous serial port for connection to a console. One EIA/TIA-32 asynchronous serial port for connection to a modem.	All

Table 4 Supported Interfaces on the Cisco IAD2430 Series Integrated Access Device (continued)

Interface and Port	Product Description	Supported IAD2430 Models
Voice Interfaces		
Analog FXS[1] Voice Ports over RJ-21 Connector	One 8-line or 16-line analog or 24-line FXS interface (loop-start or ground-start) for connection to analog phones, key systems, or PBXs.	• IAD2430-24FXS: 24 ports • IAD2431-8FXS: 8 ports • IAD2431-16FXS: 16 ports • IAD2432-24FXS: 24 ports
VIC2-4FXO	All models support one VIC[2] slot, except for Cisco IAD2430-24FXS IAD, which supports none.	• IAD2431-8FXS • IAD2431-16FXS • IAD2431-1T1E1 • IAD2432-24FXS
T1/E1 Port	Two or one T1 ports with channel-associated signaling (CAS) for connection to a digital PBX, except for Cisco IAD2430-24FXS IAD, which supports none. E1 ports are currently not supported.	• IAD2431-8FXS: 1 port • IAD2431-16FXS: 1 port • IAD2431-1T1E1: 2 ports • IAD2432-24FXS: 2 ports
WAN Interfaces		
WIC-2T	All models support one WIC[3] slot, except for Cisco IAD2430-24FXS IAD, which supports none. The supported WICs are WIC-2T and WIC-1DSU-T1. One 2T port (balanced, per ANSI T1.403) for connection to a WAN or carrier network or for a serial connection	• IAD2431-8FXS • IAD2431-16FXS • IAD2431-1T1E1 • IAD2432-24FXS
WIC-1DSU-T1	One DSU port for connection to a WAN or carrier network.	• IAD2431-8FXS • IAD2431-16FXS • IAD2431-1T1E1 • IAD2432-24FXS
Compact Flash Card		
Internal Compact Flash Card	A built-in compact flash card is supported on all models except on the Cisco IAD2430-24FXS IAD	• IAD2431-8FXS • IAD2431-16FXS • IAD2431-1T1E1 • IAD2432-24FXS
External Compact Flash Card	An external compact flash card is supported on all models.	All

[1] Foreign Exchange Station

[2] Voice Interface Card

[3] WAN Interface Card

Note For a list of unsupported features in Cisco IOS Release 12.2(15)ZJ, see Unsupported Features, page 20 in the Limitations and Restrictions section.

Determining Your Software Release

To determine the version of Cisco IOS software running on the Cisco IAD2430 Series Integrated Access Devicesr, log in to the router and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 2400 Software (2430-is-mz), Version 12.2(15)ZJ, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, please refer to *How to Choose a Cisco IOS Software Release* at:

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

For information about upgrading to a new software release, refer to *Cisco 3700 Series Multiservice Access Routers* at:

http://www.cisco.com/en/US/products/hw/routers/ps282/products_tech_note09186a0080204548.shtml

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.

To improve the usability of the release notes documentation, Cisco IOS Release 12.2(15)ZJ release notes no longer contains the feature set tables. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

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

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

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

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

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

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.2(15)ZJ5 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

Step 1 From the Cisco Feature Navigator home page, click Feature.

Step 2 To find a feature, use either "Search by full or partial feature name" or "Browse features in alphabetical order." Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the text box on the left side of the web page.

Step 3 Select a feature from the left text box, and click the Add button to add a feature to the Selected Features text box on the right side of the web page.

Note To learn more about a feature in the list, click the Description button below the left box.

Repeat this step to add additional features. A maximum of 20 features can be chosen for a single search.

Step 4 Click Continue when you are finished selecting features.

Step 5 From the Major Release drop-down menu, choose 12.2T.

Step 6 From the Release drop-down menu, choose the appropriate maintenance release.

Step 7 From the Platform Family drop-down menu, select the appropriate hardware platform. The "Your selections are supported by the following:" table will list all the software images (feature sets) that support the feature(s) that you selected.

Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.2(15)ZJ5, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

Step 1 From the Cisco Feature Navigator home page, click Compare/Release.

Step 2 In the "Find the features in a specific Cisco IOS release, using one of the following methods:" box, choose 12.2 T from the Cisco IOS Major Release drop-down menu.

Step 3 Click Continue.

Step 4 From the Release drop-down menu, choose the appropriate maintenance release.

Step 5 From the Platform Family drop-down menu, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down menu, choose the appropriate feature set. The "Your selections are supported by the following:" table will list all the features that are supported by the feature set (software image) that you selected.

New and Changed Information

The following sections list the new hardware products and software features supported by the Cisco IAD2430 Series Integrated Access Devices for Cisco IOS Release 12.2(15)ZJ5.

For more information about these features, refer to the documents listed in the "Related Documentation" section on page 37.

New Hardware in Cisco IOS Release 12.2(15)ZJ4 and Cisco IOS Release 12.2(15)ZJ5

No new hardware products are supported by the IAD2430 Series Integrated Access Devices for Cisco IOS Release 12.2(15)ZJ5. Cisco IOS Release 12.2(15)ZJ4 is not distributed for widespread availability.

New Software Features in Release 12.2(15)ZJ4 and Cisco IOS Release 12.2(15)ZJ5

No new software features are supported by the IAD2430 Series Integrated Access Devices for Cisco IOS Release 12.2(15)ZJ5. Cisco IOS Release 12.2(15)ZJ4 is not distributed for widespread availability.

New Hardware in Cisco IOS Release 12.2(15)ZJ3

No new hardware products are supported by the IAD2430 Series Integrated Access Devices for Cisco IOS Release 12.2(15)ZJ3.

New Software Features in Release 12.2(15)ZJ3

Cisco CallManager Express 3.0

Cisco CallManager Express (Cisco CME) is the new name for the product previously known as Cisco IOS Telephony Services (Cisco ITS). In addition to the features introduced in Cisco IOS Release 12.2(15)ZJ, the current release adds support for the Cisco Wireless IP Phone 7920 when it registers with Cisco CME as a Cisco IP Phone 7960. In this release, there are a set of features that are not supported on the Cisco Wireless IP Phone 7920 (intercom and paging to the phones are the two most prominent). These features and others will be added in future releases.

For additional information, refer to the *Cisco CallManager Express 3.0 System Administrator Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/itsv30/index.htm

A new command reference document collects all the Cisco CallManager Express 3.0 commands in a single location. See the *Cisco CallManager Express 3.0 Command Reference* at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/cme30cr/index.htm

New Hardware and Software Features in Cisco IOS Release 12.2(15)ZJ1 and Release 12.2(15)ZJ2

No new hardware and software features are supported by the IAD2430 Series Integrated Access Devices for Cisco IOS Release 12.2(15)ZJ1 and Release 12.2(15)ZJ2.

New Hardware in Release 12.2(15)ZJ

The following new hardware models are supported in Cisco IOS Release 12.2(15)ZJ.

Cisco IAD2430 Series Integrated Access Device

The Cisco IAD2430 Series Integrated Access Devices consists of five models. All models include one or two 10/100BASE-T Fast Ethernet ports and console and auxiliary ports. The following is a description of the five models:

- The Cisco 2430-24FXS IAD includes an RJ-21 interface for 24 analog FXS voice ports, two 10/100BASE-T Fast Ethernet ports, and an external compact flash card slot.
- The Cisco 2431-8FXS IAD includes an RJ-21 interface for 8 analog FXS voice ports, one T1/E1 port, one 10/100BASE-T Fast Ethernet port, and a slot for a WAN interface card (WIC) or voice interface card (VIC).
- The Cisco 2431-16FXS IAD includes an RJ-21 interface for 16 analog FXS voice ports, one T1/E1 port, two 10/100BASE-T Fast Ethernet ports, and a slot for a WIC or VIC.
- The Cisco 2431-1T1E1 IAD includes two T1/E1 ports, two 10/100BASE-T Fast Ethernet ports, and a slot for a WIC or VIC.
- The Cisco 2432-24FXS IAD includes two T1/E1 ports, two 10/100BASE-T Fast Ethernet ports, and a slot for a WIC or VIC.

Note See Table 4 on page 6 for a list of the supported voice interfaces, WAN interfaces, and ports for the Cisco IAD2430 Series Integrated Access Devices.

New Software Features in Release 12.2(15)ZJ

The following new software features are supported by the Cisco IAD2430 Series Integrated Access Devices in Cisco IOS Release 12.2(15)ZJ.

Cisco CallManager Express Version 3.0

Cisco CallManager Express (CME) Version 3.0 delivers the next-generation CME feature set.

Cisco CME Version 3.0 supports the following enhancements:

- CME setup tool for quick installation

  The CME setup tool provides a question-and-answer interface that allows you to set up an entire Cisco CME system at automatically.

- Automatic assignment of free extension numbers to new IP phones

  The **auto assign** command specifies a range of extension numbers to which newly discovered IP phones are automatically assigned. This method is useful when you have a phone setup in which each phone is assigned a separate, unique extension number.

- Call pickup and call-pickup groups

  Call pickup allows phone users to retrieve calls from other extension numbers by using the **PickUp** soft key and dialing the ringing number. When extensions are assigned to pickup groups, other members of the group can retrieve incoming calls using fewer keystrokes.

- Night service

  When night service is active, incoming calls to designated night-service extension numbers will also ring on other phones that are designated as night-service phones. Phone users at the other phones can use call pickup to retrieve the incoming calls.

- Call-blocking (toll bar) based on time of day, day of week, or date

  Call blocking to prevent the unauthorized use of phones is implemented by matching calls to a specified digit pattern during a specified time period. Up to 32 patterns of digits can be specified. Individual phones can be exempted from call blocking, and individual user logins can override call blocking if they are configured.

- Hunt groups

  Ephone hunt groups provide the ability to direct incoming calls for a specific number (the ephone hunt group pilot number) to a defined group of extensions. Incoming calls are redirected on busy or no answer from extension to extension in the list until they are answered or they reach the number that was defined as the final number.

- Secondary dial tone

  Secondary dial tone is generated when a phone user dials a predefined digit. The tone terminates when additional digits are dialed. For example, you can configure a secondary dial tone to be heard after the number 9 is dialed to reach an external line.

- Cisco IP Phone 7902G Support

  The Cisco IP Phone 7902G, is a cost-effective, entry-level IP phone addressing the voice communications needs of a lobby, laboratory, manufacturing floor, or hallway—or other areas where only basic calling capability is required. For further information, go to Cisco.com and click **Products & Service**, **IP Phone**, **Cisco 7900 Series IP Phones**, **Product Literature**, and **Data Sheets** or go to the following URL:
  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7902/index.htm

- Cisco IP Phone 7912G Support

  The Cisco IP Phone 7912G provides core business features and addresses the communication needs of a cubicle worker who conducts low to medium telephone traffic. The Cisco IP Phone 7912G offers four dynamic soft keys that guide a user through call features and functions. For further information, go to Cisco.com and click **Products & Service**, **IP Phone**, **Cisco 7900 Series IP Phones**, **Product Literature**, and **Data Sheets**.

- Speed Dial

  Three types of speed dial are available:

  - On multi-button phones, the buttons that are not used for extensions can be programmed as speed-dial buttons.
  - Local speed-dial numbers are common to all phone users in a CME system. Phone users access the list of local speed-dial numbers from the Directories button.
  - Personal speed-dial numbers are specific to individual phones. Phone users access their list of personal speed-dial numbers from the Directories button.

- Account code entry

  Cisco IP Phone 7940 and Cisco IP Phone 7960 users can enter account codes during call setup or while connected to an active call, using the **Acct** soft key. Account codes are inserted into call detail records (CDRs) on the CME router for later interpretation by billing software.

- Callback Busy Subscriber

  This feature allows callers who dial a busy extension number to request a callback from the system when a called number that was busy is free. Callers can also request callbacks for extensions that do not answer and the system will notify them after the called phone is next used.

  This feature is available only on Cisco IP Phone 7940 and Cisco IP Phone 7960.

- Do Not Disturb

  Do not disturb (DND) service is enabled using a soft key on a Cisco IP Phone 7940 or a Cisco IP Phone 7960. When DND is enabled, incoming calls do not ring on the phone, but do provide visual alerting and call information and can be answered if desired. A display message indicates that DND is in effect. Call forwarding on busy and no answer operates the same as without DND.

- Several international languages and call-progress tone sets are newly supported, as well as international date and time formats. The set of supported languages varies by phone type.

- Call-forward-all soft key on Cisco IP phones

- Flash soft key for hookflash functionality for the PSTN

  Certain PSTN services, such as three-way calling and call waiting, require hookflash intervention from a phone user. A new soft key, labeled Flash, has been introduced to provide this functionality for Cisco IP Phone 7940 and Cisco IP Phone 7960 users on FXO lines attached to the CME system. The Flash soft key is enabled using the **fxo hook-flash** command.

- Dual-line mode

  Dual-line extensions are available to handle call-waiting, call transfer, or conferencing using a single button.

- Extension overlays for better call handling and distribution

  An extension (ephone-dn) overlay allows more than one ephone-dn to use the same physical line button on an IP phone. Overlaid ephone-dns can be used to receive incoming calls and place outgoing calls.

- CME GUI enhancements

  The Cisco CME Graphical User Interface (GUI) provides a web-based interface to manage most CME systemwide and phone-based features. In particular, the GUI facilitates the routine adds and changes associated with employee turnover, allowing these changes to be performed by non-technical staff.

  The CME GUI provides three levels of access to support the following user classes:

  - System administrator—Able to configure all systemwide and phone-based features. This person is familiar with Cisco IOS software and VoIP network configuration.
  - Customer administrator—Able to perform routine phone adds and changes without having access to systemwide features. This person does not have to be trained in Cisco IOS software.
  - Phone user—Able to program a small set of features on his or her own phone and search the CME directory.

- Label support

  The label support feature allows you to enter a meaningful text string to view in the display adjacent to an extension button on an IP phone rather than the extension number that is associated with that button.

- Busy lamp monitor and direct station select

  For multi-button phones and expansion modules, the buttons for extensions that are shared with other phones can be designated as monitor buttons, which show the status of those extensions on the other phones. When not in use, a monitor line can be used with the **Transfer** soft key to quickly transfer a call.

- Phone directory entry

  The Cisco CME system automatically creates a local phone directory based on the telephone numbers that are assigned during the configuration of extensions and phones. Additional entries to the local CME directory can be made using the **directory entry** command.

- Silent and feature ring options

  The silent ring feature allows you to designate phone buttons that do not emit an audible ring when they receive incoming calls. Although this feature is supported by all phone types, it is most useful on phone buttons that are used to display the activity of shared lines, which are typically found on the Cisco IP Phone 7960 and Cisco IP Phone Expansion Module 7914.

- New and modified commands

  Approximately 35 new and modified commands are described in the Command Reference at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/itsv30/its30cmd.htm

For further information, refer to the *Cisco CallManager Express System Administrator Guide Version 3.0* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/itsv30/index.htm

Cisco SIP Survivable Remote Site Telephony (SRST)

SRST Features

The SIP Survivable Remote Site Telephony (SRST) feature describes SRST functionality for Session Initiation Protocol (SIP) networks. SIP-SRST provides backup to an external SIP proxy server by providing basic registrar and redirect services. These services are used by a SIP IP phone in the event of a WAN connection outage and the SIP phone is unable to communicate with its primary SIP proxy. The SIP-SRST device also provides PSTN gateway access for placing and receiving PSTN calls.

SIP-SRST provides four new features:

- SIP registrar

  A local SIP gateway that becomes the SIP registrar acts as a backup SIP proxy or redirector, and accepts SIP Register messages from SIP phones. It becomes a location database of local SIP IP phones that are set up for dual-registration. Dual-registration allows SIP IP phones to simultaneously register with both their primary and fallback registrar devices. That is, when a SIP IP phone registers with a SIP-SRST gateway, it simultaneously registers with the main proxy and SIP redirect server for coverage in case of WAN failure. A registrar accepts SIP Register requests and dynamically builds VoIP dial peers allowing the Cisco IOS Voice Gateway software to route calls to SIP phones.

- Backup registrar service to SIP IP phones

  Backup registrar service to SIP IP Phones can be provided by configuring a voice register pool on SIP gateways. The voice register pool configuration provides registration permission control and can also be used to configure some dial peer attributes that are applied to the dynamically created VoIP dial peers when SIP Phone registrations match the pool.

- Call Redirect Enhancement to Support Calls Between SIP IP Phones Through the IOS Voice Gateway

  The call redirect enhancement supports calls from a local SIP phone to another local SIP phone through the Cisco IOS Voice Gateway. Prior to this enhancement, an attempt by a SIP phone to contact another local SIP phone using the Cisco IOS Voice Gateway as if it were a SIP proxy or redirect server would fail. However, now the Cisco IOS Voice Gateway can act as a SIP redirect server. The voice gateway responds to the originator with a SIP Redirect message, allowing the SIP phone that originated the call to establish a call to its destination.

- Sending 300 Multiple Choice Messages

  Prior to Cisco IOS Release 12.2(15)ZJ, when a call was redirected, the SIP gateway would send a "302 Moved Temporarily" message. The first longest match route on a gateway (dial-peer destination pattern) was used in the Contact header of the 302 message. With release 12.2(15)ZJ, if multiple routes to a destination exist for a redirected number (multiple dial peers are matched), the SIP gateway sends a "300 Multiple Choice" message and the multiple routes in the Contact header are listed.

SIP Gateway Enhancements

SIP Gateway enhancements were also introduced in Cisco IOS Release 12.2(15)ZJ to support the SRST feature for SIP networks. They are:

- NOTIFY-Based Out-of-Band DTMF Relay

  Skinny Client Control Protocol (SCCP) IP phones do not support in-band DTMF digits; they are capable of sending only out-of-band DTMF digits. To support SCCP devices, originating and terminating SIP gateways can now use Cisco proprietary NOTIFY-based out-of-band DTMF relay.

NOTIFY-based out-of-band DTMF relay sends messages bidirectionally between the originating and terminating gateways for a DTMF event during a call. In addition, NOTIFY-based out-of-band DTMF relay can be used by analog phones attached to analog voice ports (FXS) on the router.

- SIP Register Support

  With H.323, Cisco IOS gateways can register E.164 numbers of a POTS dial peer with a gatekeeper, which informs the gatekeeper of a user's contact information. SIP gateways now allow the same functionality, but with the registration taking place with a SIP proxy or registrar. SIP gateways allow registration of E.164 numbers to a SIP proxy or registrar on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and local SCCP phones.

For additional information, refer to the *SIP Survivable Remote Site Telephony (SRST)* feature module at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/ftspsrst.htm

Cisco Survivable Remote Site Telephony (SRST) Version 3.0

The Cisco SRST Version 3.0 feature supports the following enhancements:

- Cisco IP Phone 7902G Support

  The Cisco IP Phone 7902G, is a cost-effective, entry-level IP phone addressing the voice communications needs of a lobby, laboratory, manufacturing floor, or hallway—or other areas where only basic calling capability is required. The Cisco IP Phone 7902G is a single-line IP phone, with fixed feature keys that provide one-touch access to the redial, transfer, conference, and voice-mail access features. Consistent with other Cisco IP phones, the Cisco IP Phone 7902G supports in-line power, which allows the phone to receive power over the LAN. This capability gives the network administrator centralized power control—translating into greater network availability.

  For further information, go to Cisco.com and click **Products & Service**, **IP Phone**, **Cisco 7900 Series IP Phones**, **Product Literature**, and **Data Sheets** or go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7902/index.htm.

- Cisco IP Phone 7912 Support

  The Cisco IP Phone 7912G provides core business features and addresses the communication needs of a cubicle worker who conducts low to medium telephone traffic. The Cisco IP Phone 7912G offers four dynamic soft keys that guide a user through call features and functions. The graphic capability of the display provides a rich user experience by providing calling information and intuitive access to features.

  The Cisco IP Phone 7912G supports an integrated Ethernet switch, providing LAN connectivity to a collocated PC. In addition, the Cisco IP Phone 7912G supports in-line power, which allows the phone to receive power over the LAN. This capability gives the network administrator centralized power control, translating into greater network availability. The combination of in-line power and Ethernet switch support reduces cabling needs to a single wire to the desktop.

  For further information, go to Cisco.com and click **Products & Service**, **IP Phone**, **Cisco 7900 Series IP Phones**, **Product Literature**, and **Data Sheets**.

- Customized System Message for Cisco IP Phones

  The display message that appears on Cisco IP Phone 7905G, Cisco IP Phone 7910, Cisco IP Phone 7940, and Cisco IP Phone 7960 units when they are in fallback mode can be customized. The new system message command allows you to edit these display messages on a per router basis.

- Consultative Call Transfer Using the H.450.2 Standard

  Cisco SRST V1.0 allowed only blind call transfers, in which a transferring party did not have the ability to announce or consult with a destination party before transferring a call. Cisco SRST V1.0 used a Cisco SRST proprietary mechanism to perform these blind transfers. Cisco SRST V3.0 adds the ability to perform call transfers with consultation or blind using the ITU-T H.450.2 standard for H.323 calls.

- Dual-Line Mode

  A new keyword has been added to the **max-dn** command allows you to set IP phones to dual-line mode. Each dual-line IP phone must have one voice port and two channels to handle two independent calls. This mode enables call waiting, call transfer, and conference functions on a single ephone-dn. Dual-line mode works with all phone types. The max-dn command is a global command that affects all IP phones on an Cisco SRST router.

- European Date Formats

  The date format on Cisco IP phone displays can be configured with the following two additional formats:

  yy-mm-dd (year-month-day)

  yy-dd-mm (year-month-day

- Music-on-Hold for Multicast from Flash Files

  Cisco SRST can be configured to support continuous multicast output of music-on-hold (MoH) from a Flash MoH file in Flash memory.

- Ringing Timeout Default

  A ringing timeout default can be configured for extensions on which no-answer call forwarding has not been enabled. Expiration of the timeout causes incoming calls to return a disconnect code to the caller. This mechanism provides protection against hung calls for inbound calls received over interfaces such as foreign exchange office (FXO) that do not have forward-disconnect supervision.

- Show ephone Command

  The **show ephone** command has been enhanced to display the following:

  - Configuration and status of phones of the specified type (new keywords:7914, 7905, 7935, ATA)
  - Status of all phones with the call-forwarding all calls (CFA) feature enabled on at least one of their DNs (new keyword:cfa),

- Syslog Messages for Phone Registrations

  Diagnostic messages are added to the system log whenever a phone registers or unregisters from Cisco SRST.

- Three-Party G.711 Ad Hoc Conferencing

  Cisco SRST supports three-party ad hoc conferencing using G.711. For conferencing to be available, an IP phone must have a minimum of two lines connected to one or more buttons.

- Additional language support on Cisco IP Phones

  Several international languages and call-progress tone sets are newly supported. The set of supported languages varies by phone type.

- New and modified commands

  There are approximately 10 new and modified commands. They are described at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/srs30/srs_cmds.htm

For further information about the SRST Version 3.0 features, refer to the *Cisco SRST System Administrator Guide Version 3.0* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/itsv30/index.htm

ROM Monitor Commands

Cisco IAD2430 Series Integrated Access Devices adds modified and new ROM monitor commands for downloading a software image by TFTP for disaster recovery and for FPGA selection.

The tftpdnld Command

The **tftpdnld** [**-r**] command downloads a Cisco IOS software image from a LAN server to DRAM using TFTP. Only the **-r** option for this command is supported in Cisco IOS Release 12.2(15)ZJ.

tftpdnld [**-r**]—Begins the TFTP copy procedure.

- **r**—Loads the Cisco IOS software image only to DRAM and launches the image without writing the image to compact flash.

The **tftpdnld** [**-r**] command requires you to specify certain variables in the following syntax:

```
VARIABLE_NAME=value
```

The following variables are required:

- IP_ADDRESS—IP address for the router you are using.
- IP_SUBNET_MASK—Subnet mask for the router you are using.
- DEFAULT_GATEWAY—Default gateway for the router you are using.
- TFTP_SERVER—IP address of the server from which you want to download the image file.
- TFTP_FILE—Name of the file that you want to download.

The following **tftpdnld** command variables are optional:

- TFTP_VERBOSE—Print setting. The default is 1.
  - 0=quiet—After you enter the **tftpdnld** [**-r**] command, the prompt

    ```
    Do you wish to continue? y/n:
    ```

    is the only information that appears until the command completes successfully or fails.
  - 1=progress—Displays the state of the required **tftpdnld** command variables. Also displays progress characters to indicate successful and lost packet transmissions.
  - 2=verbose—Displays all progress print setting messages, along with error information. The information provided by this print setting may be useful when debugging interface link and configuration problems that may prevent connecting to the TFTP server.
- TFTP_RETRY_COUNT—Number of times from 1 to 65535 that the ROM monitor retries ARP and ACK. The default is 7 retries.
- TFTP_TIMEOUT—Overall timeout of the download operation in seconds. The range is from 1 to 65535 seconds. The default is 7200 seconds.
- TFTP_CHECKSUM—Performs a checksum test on the image: 0=checksum off, 1=checksum on. The default is 1.

- FE_SPEED_MODE—Sets the Fast Ethernet speed and duplex mode. 0=10 Mbps half-duplex mode, 1=10 Mbps full-duplex mode, 2=100 Mbps half-duplex mode, 3=100 Mbps full-duplex mode, 4=auto-negotiation. The default is 4.

After you specify the variables, you must reenter the **tftpdnld** [**-r**] command. For example:

```
rommon 1 > IP_ADDRESS=172.15.19.11
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=172.16.19.1
rommon 4 > TFTP_SERVER=172.15.20.10
rommon 5 > TFTP_FILE=/tftpboot/c2600-i-mz
rommon 6 > tftpdnld [-r]

     IP_ADDRESS=172.15.19.11
     IP_SUBNET_MASK=255.255.255.0
     DEFAULT_GATEWAY=172.16.19.1
     TFTP_SERVER=172.15.20.10
     TFTP_FILE=/tftpboot/2600-i-mz

Invoke this command for disaster recovery only.

When the process is complete, the IOS prompt appears on your screen.
```

FPGA Commands

The new **fpga-pref** command selects the FPGA to use for the next reload only. The argument is either **system** or **readonly**.

The **show fpga** command shows the currently running FPGA and the FPGA set to run on the next reload.

The following is sample output taken from the **show version** command:

```
Router> show version

System fpga version is 20001E
System readonly fpga version is 15001C
Option for system fpga is 'system'.
```

The following sample output is displayed for the system FPGA when a reload command is issued and the router returns to the ROMMON prompt:

```
FPGA readonly version:0015001C
FPGA upgrade version :0020001E
Upgrade FPGA currently running
```

The following is sample output for the **showfpga** command:

```
rommon 1 > showfpga
ReadOnly FPGA version is: 0015001c
Upgrade FPGA version is : 0020001e
Upgrade FPGA currently running
System will select FPGA for next IOS boot
```

The following is sample output for the **fpga-pref** command:

```
rommon 2 > fpga-pref
usage: fpga-pref [readonly|system]
```

network-clock-participate Command

The **network-clock-participate** command has been modified to be more applicable to onboard framers. This is because the onboard framers for the Cisco IAD2430 Series Integrated Access Devices reside on the mother board. The modified syntax adds the controller type parameter to identify the onboard framer. The change is also more consistent with the syntax of the **network-clock-select** command.

The previous syntax inferred that the WAN interface card (WIC) resided in the WIC slot. The following is an example of the previous syntax:

```
network-clock-participate wic <slot#> port <port#>
network-clock-participate wic 1 port 0
```

The following is an example of the modified syntax:

```
network-clock-participate <controller type> <slot#/port>
network-clock-participate t1 1/0
```

Limitations and Restrictions

Unsupported Features

The Cisco IAD2430 Series Integrated Access Devices does not support the following in Cisco IOS Release 12.2(15)ZJ5:

- ATM
- E1 is not currently supported on the T1/E1 port.

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

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

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

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(15)ZJ5 that can apply to the Cisco IAD2430 Series Integrated Access Devices.

Initialization

At initialization, the default network clock algorithm selects one of the controllers present as a default network clock. The default network clock algorithm provides a best estimate of the clocking system. However there is no guarantee that all applications relying on clock accuracy will work after initialization.

We recommend that when the user powers up the system, it should be the user’s practice to make sure that network clocks are configured properly for the applications to work, with consideration for the specific network system requirements present at the moment.

If you wish to view the current primary clock, use the **show network-clocks** or **show run** command. Note that the **show network-clocks** and **show run** commands do not display the default network clock, which is selected by the default network clock algorithm.

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml

Field Notices and Bulletins

For general information about the types of documents listed in this section, refer to the following document:

http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/1654_pp.htm

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html.
- Product Bulletins—If you have an account on Cisco.com, you can find product bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find product bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.
- *What’s Hot in Software Center*—*What’s Hot in Software Center* provides information about caveats that are related to deferred software images. If you have an account on Cisco.com, you can access *What’s Hot for IOS Releases* at http://www.cisco.com/kobayashi/sw-center or by logging in and selecting **Technical Support: Software Center: Cisco IOS Software: What’s Hot in Software Center**.

- *What's New for IOS* — *What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging into Cisco.com and selecting **Technical Support:Software Center:Products and Downloads:Cisco IOS Software**.

Caveats for Cisco IOS Release 12.2(15)ZJ

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 selected severity 3 caveats are included in the caveats document.

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

All caveats in Cisco IOS Release 12.2 T and Cisco IOS Release 12.2(15)T are also in Cisco IOS Release 12.2(15)ZJ5.

For information on caveats in Cisco IOS Release 12.2 T and Cisco IOS Release 12.2(15)T, see *Caveats for Cisco IOS Release 12.2* T. These documents lists severity 1 and severity 2 caveats and only selected severity 3 caveats, and are located on Cisco.com and the Documentation CD-ROM.

Caveat numbers and brief descriptions for Release 12.2(15)ZJ5 are listed in this section.

Note If you have an account on Cisco.com, you can use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com by clicking the Log In button on the right side, go to the drop down menu on the top bar of the page and select **Technical Support**: **Tools & Utilities: Software Bug Toolkit (under Troubleshooting Tools)**. Another option is to enter the following URL in your web browser or go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Open Caveats—Cisco IOS Release 12.2(15)ZJ5

There are no open caveats specific to Cisco IOS Release 12.2(15)ZJ5 that require documentation in these release notes.

Resolved Caveats—Cisco IOS Release 12.2(15)ZJ5

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZJ5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ5

DDTS ID Number	Description
CSCdz30977	modem passthrough: option to eliminate glitch for low-speed modem Symptoms: V.22B modem connections may not work reliably over modem pass- throughs. Conditions: This symptom is observed on V.22B modems when a pair of voice gateways have digital voice ports that are driven by different clock sources. High-speed modem connections (V.32, v32bis) are not affected by this condition. Workaround: There is no workaround.
CSCdz84583	IOS fw allowing forged packets for a session initiated from inside A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software. A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ5 (continued)

DDTS ID Number	Description
CSCeb52066	NAT: Provide an API to get the pre-natted TCP Seq/Ack Numbers A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software. A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.
CSCec59206	Bus error in nat translating RSHELL packets Symptoms: A router may reload unexpectedly because of a bus error when it accesses a low address during the translation of TCP port 514. Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(5) and that is configured for Network Address Translation (NAT). Workaround: Prevent the translation of TCP port 514.
CSCed35253	Router crash due to corrupted data in list with IOS-firewall Symptoms: A router may reload unexpectedly after it attempts to access a low memory address. Conditions: This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature. Workaround: Disable IP Inspect and IDS.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ5 (continued)

DDTS ID Number	Description
CSCed93836	modifications needed to syn rst packet response A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software. A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Open Caveats—Cisco IOS Release 12.2(15)ZJ4

Cisco IOS Release 12.2(15)ZJ4 is not distributed for widespread availability.

Resolved Caveats—Cisco IOS Release 12.2(15)ZJ4

Cisco IOS Release 12.2(15)ZJ4 is not distributed for widespread availability.

Open Caveats—Cisco IOS Release 12.2(15)ZJ3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)ZJ3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 6 Open Caveats for Cisco IOS Release 12.2(15)ZJ3

DDTS ID Number	Description
CSCeb67032	CFAll after a full-blind transfer between ITSs not working Symptoms: A caller doing a blind transfer sees the error message, "Unable to transfer" on their IP phone even though the destination is ringing. Conditions: An ITS fxs/ipphone calls another ITS ip phone. The second ITS ip phone initiates a full blind transfer to a third ITS iphone. The third ITS phone has Call Forward All set to an ITS fxs phone. Workaround: There is no workaround.
CSCin46584	IPIPgw doesnt transfer the IEs completely Symptoms: The IEs are not propagated by the IPIPGW to the originating gateway . This might affect the interoperablity between a call manager and IPIP gateway. Workaround: There is no workaround.
CSCin51176	The outbound VOIP dialpeer is not selected with called-number alone Symptoms: A voice gateway incorrectly matches the wrong outbound dial-peer using called number digits collected from INFO messages. Conditions: For a non-DID call using overlap signaling, the SETUP message contains all the called number digits required to place a call. The gateway does not receive an info complete, a T302 expiry, or subsequent INFO messages. The dial-peer mismatch occurs when the initial interdigit timeout expires because incorrect called number digits are used to find a matching dial-peer. Workaround: There is no workaround.
CSCin55495	After sending PROGRESS with PI the OGW is not sending the CONNECT Symptoms: A CONNECT message is received on the terminating gateway (TGW) but is never seen on the originating gateway (OGW). Conditions: This happens when the enhanced default application is used on the terminating gateway and the terminating gateway receives a PROGRESS message with an inband progress indicator. Workaround: Configure the "default.c.old" application on the terminating gateway.

Resolved Caveats—Cisco IOS Release 12.2(15)ZJ3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZJ3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 7 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ3

DDTS ID Number	Description
CSCdx76632	as5300 crashed in MultiBitDecode Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.
CSCdx95698	No Ringback on transfer on using Ivr clid_authen_collect Symptoms: Ringback is not heard on the originating phone when a blind transfer is initiated. Conditions: An IVR script on a gateway processes an incoming PSTN call, including prompting for a destination number. Once the call is established with the destination, the destination party transfers the originating party to another destination. During this transfer, the originating party should hear the ringing for the destination. Workaround: There is no workaround.
CSCea19885	Bus error at address 0xD0D0D0B, Process CCH323_CT Symptoms: A Cisco router that has a voice feature such as H.323 enabled may reload because of a bus error at address 0xD0D0D0B. Conditions: This symptom is observed on a Cisco 3700 series but may also occur on other routers. Workaround: There is no workaround.

Table 7 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ3

DDTS ID Number	Description
CSCea27536	Router crash when H323v3/v4 pkts pass through NAT router Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml. NAT router (which is H323v2 stack aware) crashes when H323v3/v4 pkt is processed as "ip nat service h323all" is turned on. Workaround: Turn off "ip nat service h323all" or move to 12.3T image (which has NAT-H323v3/v4) support
CSCea32240	H323 crashes in strncpy when receiving invalid setup packet Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.
CSCea33065	H323 Spurious memory access in h450ProcRcvdApdus Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Table 7 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ3

DDTS ID Number	Description

CSCea33499	Symptoms: The gateway is not sending **RSIP:restart** when the digital voice-ports are configured as Media Gateway Control Protocol (MGCP) endpoints. Because of this, the call agent is not informed of the status of the MGCP endpoints and it rejects the NTFY messages from the gateway.
	Workaround: After configuring the MGCP endpoints for the digital-port, perform the following in the configuration mode to restart the MGCP application:
	`Router(config)# no mgcp`
	`Router(config)# mgcp`
	This should make the router send **RSIP:restart** to the call agent.

CSCea36231	Router hangs when receive in invalid h225 setup Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.
CSCea46342	h.323 crashes in ACFnonStandardInfo DEC_ERR=13 Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Table 7 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ3

DDTS ID Number	Description
CSCea51030	h323: proxy crashes when malformed h225 setup message received Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.
CSCea51076	h323: proxy crashes when processing invalid h225 setup messafe Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.
CSCea54851	h323 proxy: crash at pxy_proc_recv_SETUP when invalid h225 setup rx Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Table 7 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ3

DDTS ID Number	Description

CSCeb65637	Unable to set the H.323 callIdentifier from Tcl IVR script
	Symptoms: Call setup to an IP network may be delayed or rejected.
	Further Problem Description: A call setup without an incoming call leg results in a H.225 SETUP or remote access server (RAS) admission message with the callIdentifier field value of zeroes.
	Conditions: TCL IVR script attempts to set up a call without specifying the incoming leg.
	Workaround: The workarounds are:
	1. Set up a call with an incoming leg.
	2. Enter **set callinfo**(**newguid**) to force the call setup to generate new conferenceID and callIdentifier fields. This assumes that the generated GUID does not affect the billing system or the remote endpoint.
	Example:
	`set callinfo(newguid) true`
	`leg setup $dest_nr callinfo`

CSCeb71588	Digital MGCP endp doesnt become active after creation till mgcp res Symptoms: When digital voice port on Cisco IAD2430 router is added to POTS dial-peer with application mgcpapp, it does not notify Media Gateway Control Protocol (MGCP) call agent and become active automatically. Conditions: Configure a POTS dial-peer for a digital voice port with application mgcpapp. Workaround: After configuring the PORT dialpeer, enter **no mgcp** and followed by MGCP CLIs to bring the digital voice port active.
CSCeb78836	h323: software forced crash if bad packet received and debug opened Symptoms: Cisco IOS software may cause a Cisco router to reload unexpectedly when the router receives a malformed H.225 setup message. Conditions: This symptom is observed on a Cisco 1700 series that runs Cisco IOS Release 12.2(13c). The symptom occurs when the following **debug** privileged EXEC commands are enabled: • **debug h225 asn1** • **debug h225 events** • **debug h225 q931** Workaround: There is no workaround.

Table 7 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ3

DDTS ID Number	Description
CSCec07327	Cannot Loop IAD2432 T1 Controller Symptoms: Onboard framer misses the first FDL request. PRM transmission to CO timing is wrong. Work around: The customer must issue the FDL twice with "no *xxxx*" in between when the Cisco IAD2430 boots up. After that, the Cisco IAD2430 operates correctly. There is no workaround for the second problem with PRM.
CSCin51788	progress_ind connect PI is not sent from TGW to OGW Symptoms: A CONNECT message arrives at an originating gateway (OGW) with an incorrect progress indicator. Conditions: On the terminating gateway's (TGW) incoming dial-peer configuration, define a progess indicator for the connect event by using **progress-ind connect enable** *8*. Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(15)ZJ2

There are no open caveats specific to Cisco IOS Release 12.2(15)ZJ2 that require documentation in these release notes.

Resolved Caveats—Cisco IOS Release 12.2(15)ZJ2

There are no resolved caveats specific to Cisco IOS Release 12.2(15)ZJ2 that require documentation in these release notes.

Open Caveats—Cisco IOS Release 12.2(15)ZJ1

There are no open caveats specific to Cisco IOS Release 12.2(15)ZJ1 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(15)ZJ1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZJ1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 8 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ1

DDTS ID Number	Description
CSCdz71127	corrupted packet can cause input queue wedge - reg to CSCdx02283 Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available. Cisco has made software available, free of charge, to correct the problem. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml
CSCeb24528	Show voice DSP active does not show any O/P when call is active Symptoms: When the **show voice dsp active** command is issued while an active call is on an onboard analog FXS voice port which uses DSP, no entry is shown for the active onboard analog FXS voice port. Workaround: There is no workaround.
CSCeb28838	Vinetic devices failed download PRAM during IOS bootup Symptoms: After extensive hours of RDT testing, on-board AVM failed to download EDSP PRAM FW during IOS boot up. Problem: IOS boot up with on-board analog voice ports is not working properly. Workaround: Reboot the router again.
CSCeb29193	DSP5510 egress failure Symptoms: After extensive hours of RDT testing, Diagnostic test failed to send packet to DSP. Problem: DMA engine used to send packet to DSP sometimes locks up after reboot. Workaround: Reboot the router again.

Open Caveats—Cisco IOS Release 12.2(15)ZJ

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)ZJ and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 9 Open Caveats for Cisco IOS Release 12.2(15)ZJ

DDTS ID Number	Description
CSCeb28838	Vinetic devices failed download PRAM during IOS bootup Symptoms: After extensive hours of RDT testing, on-board AVM failed to download EDSP PRAM FW during IOS boot up. Problem: IOS boot up with on-board analog voice ports is not working properly. Workaround: Reboot the router again.
CSCeb29193	DSP5510 egress failure Symptoms: After extensive hours of RDT testing, Diagnostic test fail to send packet to DSP. Problem: DMA engine used to send packet to DSP sometimes locks up after reboot. Workaround: Reboot the router again.
CSCeb32390	Invalid PRI configuration with insufficient DSPs message Symptoms: Pri-group config appears in show run output, even though “insufficient DSP" message says that 1-24 timeslots cannot be configured on an 8FXS when pri is configured with service Media Gateway Control Protocol (MGCP) . Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(15)ZJ

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZJ. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 10 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ

<table>
<tr><th>DDTS ID Number</th><th>Description</th></tr>
<tr><td><b>CSCea02355</b></td><td>
<p>rare ip packets may cause input queue wedge</p>
<p>Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.</p>
<p>Cisco has made software available, free of charge, to correct the problem.</p>
<p>This advisory is available at</p>
<p>http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml</p>
</td></tr>
<tr><td><b>CSCea14844</b></td><td>
<p>CAS doesn’t work if channel group configured first</p>
<p>Description: If a channel group is configured before a DS0 group for the same controller, the CAS voice ports remain in a seized state.</p>
<p>Symptoms: The <b>show voice call summary</b> command shows all ports in the BUSYOUT state:</p>
<pre>
S2431-16#show vo ca su

PORT CODEC VAD VTSP STATE VPM STATE
===== ===== === ===== ===== =========
1/0:3.13   -   -   -   EM_ONHOOK
1/0:3.14   -   -   -   EM_BUSYOUT
1/0:3.15   -   -   -   EM_BUSYOUT
1/0:3.16   -   -   -   EM_BUSYOUT
1/0:3.17   -   -   -   EM_BUSYOUT
1/0:3.18   -   -   -   EM_BUSYOUT
1/0:3.19   -   -   -   EM_BUSYOUT
1/0:3.20   -   -   -   EM_BUSYOUT
1/0:3.21   -   -   -   EM_BUSYOUT
1/0:3.22   -   -   -   EM_BUSYOUT
1/0:3.23   -   -   -   EM_BUSYOUT
1/0:3.24   -   -   -   EM_BUSYOUT
</pre>
<p>Workaround: Configure the DS0 group first and then the channel group.</p>
</td></tr>
<tr><td><b>CSCea19203</b></td><td>
<p>Voice path confirmation faiures with codec g.729 and no vad</p>
<p>Description: With the G.728r8 codec, voice path confirmation failures are seen if VAD is turned off. With VAD turned on, 100-percent path confirmation is seen.</p>
<p>Symptoms: Even though call setup is 100 percent, there are voice-quality issues, which cause path confirmation to fail.</p>
<p>Workaround: There is no workaround. However, you will obtain about 90-percent call success with the G.729 codec and no VAD. Turn on VAD if you need 100-percent call success.</p>
</td></tr>
</table>

Table 10 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ (continued)

<table>
<tr><th>DDTS ID Number</th><th>Description</th></tr>
<tr><td><b>CSCea27687</b></td><td>

ISDN layer 2 doesn’t come up when PRI backhaul session configured ft

Description: The Backhaul Session Manager (BSM) has two modes, fault tolerant (FT) and non-fault-tolerant (NFT). NFT mode works correctly, but if the BSM is configured FT, ISDN layer 2 does not come up.

Symptoms: ISDN Layer 2 does not come up.

```
S2431-16#show isdn stat

Global ISDN Switchtype = primary-ni
ISDN Serial1/0:23 interface
        ******* Network side configuration *******
        dsl 0, interface ISDN Switchtype = primary-ni
        L2 Protocol = Q.921  L3 Protocol(s) = BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask: 0x807FFFFF
    Number of L2 Discards = 0, L2 Session ID = 3
    Total Allocated ISDN CCBs = 0
```

Workaround: Unless you need to test the failover case, use the Backhaul Session Manager in non-fault-tolerant mode. Only one session group per session set can be defined in this mode.

</td></tr>
<tr><td><b>CSCeb28773</b></td><td>

GT96K DMA Out-of-range Interrupt causes failure of tftpdnld -r

Symptoms: Occasionally the **tftpdnld** command from rommon fails to load the IOS image and run IOS.

Problem: IOS image is not loaded.

Workaround: Reboot and/or power cycle the router.

</td></tr>
<tr><td><b>CSCeb36010</b></td><td>

2430-24FXS crashes with interface dialer command

Symptoms: Router fails with illegal access and unexpected exception when **interface dialer 0** command is entered.

Workaround: There is no workaround.

</td></tr>
</table>

Related Documentation

The following sections describe the documentation available for the Cisco IAD2430 Series Integrated Access Devices. 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, except for feature modules, which are available online on Cisco.com and http://www.cisco.com/univercd/home/index.htm. Use these release notes with these documents:

- Platform-Specific Documents, page 37
- Feature Modules, page 37
- Cisco Feature Navigator, page 38
- Cisco IOS Software Documentation Set, page 38

Platform-Specific Documents

These documents are available for the Cisco IAD2430 Series Integrated Access Devices on Cisco.com and the Documentation CD-ROM:

- *Cisco IAD 2430 Series Integrated Access Device Hardware Installation Guide*
- *Cisco IAD 2430 Series Integrated Access Device Software Configuration Guide*
- *Cisco IAD 2430 Series Integrated Access Device Quick Start Guide*
- *Cisco IAD2430 Series Regulatory Compliance and Safety Information*

On Cisco.com at:

Products and Services: Cisco Voice Gateways: Cisco IAD2400 Series Integrated Access Devices: Technical Documentation: Cisco IAD2430 Series Integrated Access Devices

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

Cisco Documentation:_**Access Servers & Routers: Integrated Access Devices: Cisco IAD2430 Series IADs**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Access Servers & Routers: Integrated Access Devices: Cisco IAD2430 Series IADs**

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(15)ZJ5 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:

Products and Services: **Cisco IOS Software**: **Cisco IOS Software Releases:**
Cisco IOS Release 12.2 T: Technical Documentation: Feature Guides

On Cisco Connection Online (CCO), http://www.cisco.com/univercd/home/index.htm, at:

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

Cisco Feature Navigator

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

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

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

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

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

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

Documentation Modules

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

On Cisco.com at:

Products and Services: **Cisco IOS Software**: **Cisco IOS Releases 12.2**: **Instructions and Guides**

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

Cisco IOS Software: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**

Release 12.2 Documentation Set

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 paper documents were printed.

Table 11 lists the contents of the Cisco IOS Release 12.2 software documentation set.

On Cisco.com at:

Products and Services: **Cisco IOS Software**: **Cisco IOS Releases 12.2**: **Instructions and Guides**

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

Cisco IOS Software: **Cisco IOS Release 12.2**

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco.com. From Cisco.com, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Table 11 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 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 11 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	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 Novell IPX
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *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

Table 11 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *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
• *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
• *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 NASI Telnet TN3270 XRemote 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)	

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco TAC Website

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

http://www.cisco.com/tac

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

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

Opening a TAC Case

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

TAC Case Priority Definitions

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

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

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

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

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

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 37