Release Notes for the Cisco 3600 Series Modular Access Routers for Cisco IOS Release 12.2(15)ZJ5

April 26, 2004

Cisco IOS Release 12.2(15)ZJ5

OL-4375-01 Rev G0

These release notes for the Cisco 3600 series modular access routers 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" section on page 29. See also *Caveats for Cisco IOS Release 12.2 T*, which is updated for every maintenance release and is located on Cisco.com.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* located on Cisco.com.

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.

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

OL-4375-01 Rev G0

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

Cisco IOS Release 12.2(15)ZJ5 supports the Cisco 3631, Cisco 3640, Cisco 3640A, Cisco 3661, and Cisco 3662 modular access routers.

The Cisco 3600 Series is a family of modular, multiservice access platforms for medium and large-sized offices and smaller Internet Service Providers. With over 70 modular interface options, the Cisco 3600 family provides solutions for data, voice video, hybrid dial access, virtual private networks (VPNs), and multiprotocol data routing. The high-performance, modular architecture protects customers' investment in network technology and integrates the functions of several devices into a single, manageable solution.

Cisco extended the successful Cisco 3600 Series with the Cisco 3660 multiservice access platform. The Cisco 3660 provides higher densities, greater performance, and more expansion capabilities. The additional power and performance of the Cisco 3660 platform enables new applications, such as packetized voice aggregation and branch office ATM access ranging from T1/E1 IMA to OC-3. The Cisco 3660 modular access routers consists of two router models: Cisco 3661 and Cisco 3662.

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.2(15)ZJ5, see "New and Changed Information" section on page 8 and "Related Documentation" section on page 48.

Early Deployment Releases

These release notes describe Cisco IOS Release 12.2(15)ZJ5 for the Cisco 3600 series modular access routers. 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 new features supported by the Cisco 3600 series modular access routers in Cisco IOS Release 12.2(15)ZJ5. See "Platform-Specific Documents" section on page 48 for a list of the documentation specific to the Cisco 3600 series modular access routers.

Table 2 Early Deployment Release New Features for the Cisco 3600 series modular access routers

ED Release	Additional Software Features[1] and MIBs[2]	Additional Hardware	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
Cisco IOS Release 12.2(15)ZJ1	• Support for the Cisco Intrusion Detection System (IDS) network module	• Cisco Intrusion Detection System (IDS) network module – NM-CIDS-K9	Now

Table 2 Early Deployment Release New Features for the Cisco 3600 series modular access routers (continued)

ED Release	Additional Software Features[1] and MIBs[2]	Additional Hardware	Hardware Availability
Cisco IOS Release 12.2(15)ZJ	• Cisco IOS MGCP Gateway Support for Cisco CallManager Network Specific Facilities • Cisco SIP Survivable Remote Site Telephony (SRST) • Cisco Survivable Remote Site Telephony (SRST) Version 3.0 • Cisco IOS Telephony Services Version 3.0 • Custom Tone Download to Cisco IOS MGCP Gateways from Cisco CallManager • DPNSS Backhaul • Enhanced ITU-T G.168 Echo Cancellation • Enhancements to the 16- and 36-Port Ethernet Switch Module • FRSVC over ISDN • MGCP-Controlled Backhaul of BRI Signaling • Private Line Automatic Ringdown for Trading Turrets • Support for IP communications voice/fax network modules • Support for NM-16A/S network modules • Support for VIC2- voice interface cards	• High-density, synchronous/asynchronous serial network module – NM-16 A/S • IP communications voice/fax network modules – NM-HD-1V – NM-HD-2V – NM-HD-2VE • Voice Interface Cards: – VIC2-2FXS – VIC2-2FXO, VIC2-4FX – VIC2-2BRI-NT/TE – VIC2-2E&M	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)ZJ5 and includes the following sections:

Memory Recommendations

Table 3 displays the memory recommendations of the Cisco IOS feature sets for the Cisco 3631, Cisco 3640/3640A, Cisco 3661, and Cisco 3662 routers for Cisco IOS Release 12.2(15)ZJ5.

Cisco 3631, Cisco 3640/3640A, Cisco 3661, and Cisco 3662 routers are available with a 32-MB or 48-MB Flash memory card.

Table 3 Cisco Release 12.2(15)ZJ5 Memory Recommendations for the Cisco 3631, Cisco 3640/3640A, Cisco 3661, and Cisco 3662 Routers

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Cisco 3631				
Telco Feature Set	c3631-telco-mz	32 MB	128 MB	RAM
Telco Plus Feature Set	c3631-telcoent-mz	64 MB	128 MB	RAM
Cisco 3640/3640A				
IP Plus	c3640-is-mz	32 MB	96 MB	RAM
Enterprise Plus	c3640-js-mz	32 MB	128 MB	RAM
Enterprise Plus/H.323 MCM	c3640-jsx-mz	32 MB	128 MB	RAM
IP/FW/IDS Plus IPSEC 3DES	c3640-ik9o3s-mz	32 MB	128 MB	RAM
Enterprise/FW/IDS Plus IPSEC 3DES	c3640-jk9o3s-mz	32 MB	128 MB	RAM
Cisco 3660				
IP Plus (Standard Feature Set)	c3660-is-mz	32 MB	128 MB	RAM
Enterprise Plus (Standard Feature Set)	c3660-js-mz	64 MB	128 MB	RAM
Enterprise Plus/H.323 MCM	c3660-jsx-mz	64 MB	128 MB	RAM
IP/FW/IDS Plus IPSEC 3DES	c3660-ik9o3s-mz	64 MB	128 MB	RAM
Enterprise/FW/IDS Plus IPSEC 3DES	c3660-jk9o3s-mz	64 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(15)ZJ5 supports the following Cisco 3600 series platforms:

- Cisco 3631
- Cisco 3640, Cisco 3640A
- Cisco 3661, Cisco 3662

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 8.

For a complete list of network modules and interface cards supported on Cisco 3600 series modular access routers, refer to the "Relevant Interfaces and Modules" table on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps274/products_relevant_interfaces_and_modules.html

For additional information about supported hardware for this platform and release, please 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

Determining Your Software Release

To determine the version of Cisco IOS software running on the Cisco Cisco 3600 series modular access routersr, log in to the router and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 ZJ Software (C3600-js-mz), Version 12.2(15)ZJ, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Cisco IOS Upgrade Ordering Instructions* located at: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm.

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 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.

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

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

To determine which software images (feature sets) in Cisco IOS Release 12.2(15)ZJ 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)ZJ, 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 3600 series modular access routers in 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 48.

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 Cisco 3600 series modular access routers 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 Cisco 3600 series modular access routers 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 Cisco 3600 series modular access routers 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)ZJ2

No new hardware and software features are supported by the Cisco 3600 series modular access routers for Cisco IOS Release 12.2(15)ZJ2.

New Hardware in Release 12.2(15)ZJ1

Cisco Intrusion Detection System (IDS) Network Module (NM-CIDS-K9)

Cisco IOS Release 12.2(15)ZJ1 introduces the Cisco Intrusion Detection System (IDS) network module, part number NM-CIDS-K9. The Cisco IDS network module is installed on a Cisco 3725 or a Cisco 3745 chassis to provide full-featured intrusion-protection services within the router. The Cisco IDS network module provides the ability to:

- inspect all traffic traversing the router.
- identify malicious activity.
- terminate illegitimate traffic.
- integrate the Cisco IDS functionality into the branch office router.
- implement full-featured Cisco IDS at your remote branch offices.
- install theCisco IDS network module in any one of the network module slots on the Cisco 2600, 3600, and 3700 series routers.

Note The IDS network module is not supported on the Cisco 3620, Cisco 3631, Cisco 3640, and Cisco 3640A modular access routers.

The Cisco IDS network module provides up to 45 Mbps of intrusion detection capability. Only one Cisco IDS network module is supported per router and is not hot-swappable. The network module runs the latest version of the Cisco IDS software, version 4.1.

You can manage and retrieve events from the Cisco IDS network module through Cisco IOS CLI or through one of these Cisco IDS managers—IDS Device Manager or Management Center for IDS Sensors.

The Cisco IDS network module supports the following interfaces:

- One internal 10/100 Ethernet port—connects to the router's backplane
- One external 10/ 100-based Ethernet port—used for device management (management of other routers and/or PIX Firewalls to perform shunning) and command and control of the Cisco IDS network module by the Cisco IDS manager.

For instructions on accessing the Cisco IDS documentation on Cisco.com, refer to the *Cisco Intrusion Detection System (IDS) Hardware and Software Version 4.1 Documentation Guide* that shipped with your IDS router module. It is at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/15593_01.htm

For basic installation information, refer to "Connecting Cisco Intrusion Detection System Network Modules," *in Cisco Network Modules Hardware Installation Guide*, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/index.htm

New Software Features in Release 12.2(15)ZJ1

Support for the Cisco Intrusion Detection System (IDS) Network Module

Cisco IOS Release 12.2(15)ZJ1 introduces support for the Cisco Intrusion Detection System (IDS) network module, part number NM-CIDS-K9. The Cisco IDS network module provides full-featured intrusion-protection services for the Cisco 3661 and Cisco 3662 modular access routers. The Cisco IDS network module provides the ability to inspect all traffic traversing the router, to identify malicious activity, and to terminate illegitimate traffic.

The IDS router module supports the following software:

- Cisco IOS software 12.2(15)ZJ1 or later
- Cisco IDS software 4.1 or later

Note The IDS network module is not supported on the Cisco 3620, Cisco 3631, Cisco 3640, or Cisco 3640A modular access routers.

The IDS network module supports the following feature sets in Cisco IOS Release 12.2(15)ZJ1:

- IOS IP/FW/IDS/Plus IPSEC 3DES
- IOS Enterprise/FW/IDS/Plus IPSEC 3DES

Note All IDS network modules have Online Insertion Removal (OIR) support, but OIR is supported only on the Cisco 3660 series and Cisco 3745 platforms.

The following Cisco IOS command is new to support the IDS network module:

service-module ids-sensor *slot_number*/**0** {**reload**|**reset**|**session**|**shutdown**|**status**}

Note Do not confuse Cisco IOS Firewall IDS (a software-based intrusion-detection application that runs in the Cisco IOS) with the IDS that runs on the IDS network module. The IDS network module runs Cisco IDS version 4.1. Because performance can be reduced and duplicate alarms can be generated, we recommend that you do not run Cisco IOS Firewall IDS and Cisco IDS version 4.1 simultaneously.

For instructions on accessing the IDS documentation on Cisco.com, refer to the *Cisco Intrusion Detection System (IDS) Hardware and Software Version 4.1 Documentation Guide* that shipped with your IDS router module. It is at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/15593_01.htm

New Hardware in Release 12.2(15)ZJ

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

IP Communications Voice/Fax Network Modules

Cisco IOS Release 12.2(15)ZJ introduces new voice/fax network modules that support IP communications. The IP communications voice/fax network modules provide the ability to directly connect the PSTN and legacy telephony equipment to the Cisco 3600 series modular access routers, enabling important applications such as IP telephony, toll bypass, and full gateway integration.

Voice network modules convert telephone voice signals into a form that can be transmitted over an IP network. These modules have one or two slots for installing supported interface cards. Voice interface cards (VICs) or voice/WAN interface cards (VWICs) installed in the voice network module provide physical connections to the telephony equipment or network.

The new network modules that support the IP communications voice/fax feature are:

- NM-HD-1V
- NM-HD-2V
- NM-HD-2VE

Note These network modules are not supported on the Cisco 3631 modular access routers.

The new network modules support the following new VIC2 voice interface cards (VICs):

- VIC2-2FXS—two-port voice interface card, FXS

  An FXS interface connects directly to a standard telephone, fax machine, or similar device. This interface supplies ringing voltage, dial tone, and so on to the station.

- VIC2-2FXO—two-port voice interface card, FXO (Universal); supports CAMA with software configuration.

  An FXO interface connects local calls to a central office or PBX. This is the interface a standard telephone provides.

- VIC2-4FXO—four-port voice interface card, FXO (Universal); supports CAMA with software configuration.
- VIC2-2E&M—two-port voice interface card, E&M

  E&M is a signaling technique for two-wire and four-wire telephone and trunk interfaces. The E&M interface typically connects remote calls from an IP network to a PBX.
- VIC2-2BRI-NT/TE—2-port voice interface card, BRI

  The ISDN BRI voice interface card provides a client-side (TE) ISDN S/T physical interface for connection to an NT1 terminating an ISDN telephone network. Each of its two ports can carry two voice calls (one over each ISDN B channel), for a total of four calls per ISDN BRI card.

Note The VIC2-2FXO, VIC2-4FXO, VIC2-2E&M, and VIC2-2BRI-NT/TE voice interface cards replace the VIC-2FXO, VIC-4FXO, VIC-2E&M, and VIC-2BRI-NT/TE voice interface cards, respectively.

The new network modules support the following existing VICs and voice WAN interface cards (VWICs):

- VIC-2DID—two-port DID voice interface card

  A Direct Inward Dial (DID) voice interface enables a Cisco 2600 series, Cisco 3600 series, or Cisco 1700 series router to provide DID service to extensions on a PBX.
- VIC-4FXS/DID—four-port FXS or DID VIC

Note Cisco 3640 and Cisco 3660 routers do not support DID on the VIC-4FXS/DID card in this release.

Note The supported VICs require Cisco IOS Release 12.2(15)ZJ or later.

The new NM-HD-2VE network module supports the following existing 1- and 2-port T1/E1 multiflex trunk WAN interface cards (VWICs):

- VWIC-2MFT-T1—two-port T1 RJ-48 Multiflex Trunk Interface Card
- VWIC-1MFT-T1—one-port T1 Multiflex Trunk Interface Card
- VWIC-2MFT-T1-DI—two-port T1 Multiflex Trunk Interface Card with Drop and Insert
- VWIC-1MFT-E1—one-port E1 Multiflex Trunk Interface Card
- VWIC-2MFT-E1—two-port E1 Multiflex Trunk Interface Card
- VWIC-2MFT-E1-DI—two-port E1 Multiflex Trunk Interface Card with Drop and Insert
- VWIC-1MFT-G703—one-port E1 Multiflex Trunk Interface Card with G.703 support
- VWIC-2MFT-G703—two-port E1 Multiflex Trunk Interface Card with G.703 support

The 1- and 2-port T1 and E1 multiflex trunk interface cards support generic single- or dual-port T1 or E1 trunk interfaces for voice, data, and integrated voice and data applications. These cards provide basic structured and unstructured service for T1 or E1 networks.

Note The supported VWICs require Cisco IOS Release 12.2(15)ZJ or later.

NM-16 A/S Network Module

The NM-16 A/S is a slow-speed, high-density serial network module (NM) offering asynchronous and synchronous interfaces and flexible port configuration.

- Synchronous interfaces that support a data rate of up to 128 Kbps.
- Asynchronous interfaces that support a data rate of up to 115.2 Kbps.
- Configurable data terminal equipment (DTE) and data circuit-terminating equipment (DCE)

These network modules are not supported on the Cisco 3640 and Cisco 3640A routers.

New Software Features in Release 12.2(15)ZJ

The following new software features are supported by the Cisco 3600 series modular access routers in Cisco IOS Release 12.2(15)ZJ:

- Cisco IOS MGCP Gateway Support for Cisco CallManager Network Specific Facilities
- Cisco SIP Survivable Remote Site Telephony (SRST)
- Cisco Survivable Remote Site Telephony (SRST) Version 3.0
- Cisco IOS Telephony Services Version 3.0
- Custom Tone Download to Cisco IOS MGCP Gateways from Cisco CallManager
- DPNSS Backhaul
- Enhanced ITU-T G.168 Echo Cancellation
- Enhancements to 6- and 36-Port Ethernet Switch Network Modules
- FRSVC Over ISDN
- MGCP-Controlled Backhaul of BRI Signaling
- Private Line Automatic Ringdown for Trading Turrets
- Support for IP Communications Voice/Fax Network Modules
- Support for the NM-16A/S Network Modules

Cisco IOS MGCP Gateway Support for Cisco CallManager Network Specific Facilities

The Cisco IOS MGCP Gateway Support for Cisco CallManager Network Specific Facilities (NSF) feature is an enhancement to Cisco CallManager functionality. It enables users to configure the NSF ISDN information element of the route pattern.

The ISDN NSF route pattern design has been changed in the Cisco CallManager database to enable invocation of facilities or services on a call-by-call basis.

The NSF information is used in ISDN PRI call setup for outgoing calls and includes carrier identification code (CIC) and service parameters. The NSF configuration tasks are done in Cisco CallManager.

The NSF configuration has been added in the route pattern user interface page for Media Gateway Control Protocol (MGCP) controlled PRI ports. Without the NSF configuration, users have to configure their associated gateways as stand-alone H.323 gateways for which NSF services are configured locally within the router. With NSF configured, NSF can be used on a call-by-call basis.

For additional prerequisite and configuration information, refer to the *Cisco IOS MGCP Gateway Support for Cisco CallManager Network Specific Facilities* feature module at:

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

Restrictions

This feature is not supported on the Cisco 3620 and Cisco 3631 routers.

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

Restrictions

This feature is not supported on the Cisco 3631 routers.

Cisco IOS Telephony Services 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:
  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 Graphical User Interface (GUI) enhancements

  The Cisco CME 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

Restrictions

This feature is not supported on the Cisco 3631 routers.

Custom Tone Download to Cisco IOS MGCP Gateways from Cisco CallManager

Cisco IOS Release 12.2(15)ZJ introduces the Custom Tone Download to Cisco IOS MGCP Gateways from Cisco CallManager feature. This feature implements the downloading of region-specific tones and the associated frequencies, amplitudes, and cadences using XML-based configuration files during gateway registration. The feature also supports the generation of tones up to four frequencies by the Cisco IOS Media Gateway Control Protocol (MGCP) gateway. The feature supports dual tones and sequential tones.

The MGCP gateway handles the translation between voice signals and the packet network and interacts with Cisco CallManager. Cisco CallManager performs signal and call processing. The Custom Tone Download to Cisco IOS MGCP Gateways from Cisco CallManager feature enables the gateway to use the tone information in the custom tone tables that have been downloaded from the TFTP server in an XML-based configuration file.

When Cisco CallManager requests a specific tone, the gateway references the custom tone table associated with the network locale of the voice port.

When the gateway registers to Cisco CallManager, or if the gateway restarts or resets, the network locale for each port is downloaded to the gateway. Once the custom tone specification is downloaded to the gateway, it can also be used in H.323 mode if the gateway loses connectivity to Cisco CallManager.

This feature supports one new Cisco IOS command and three modified Cisco IOS commands:

- **ccm-manager download-tones** command (new)
- **cptone** command (modified)
- **debug ccm-manager** command (modified)
- **show ccm-manager** command (modified)

For additional command syntax information, prerequisite and configuration information, refer to the *Custom Tone Download to Cisco IOS MGCP Gateways from Cisco CallManager* feature module at:

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

Restrictions

Only one gateway supports the download of up to two custom tones, that is, no more than two custom tone tables will be downloaded to one gateway even if there are more that two countries or regions configured for the gateway.

This feature is not supported on the Cisco 3631 routers.

DPNSS Backhaul

This feature introduces support for Digital Private Network Signaling System (DPNSS) Layer 2 functionality on the Cisco gateway (GW) for Cisco IOS Release 12.2(15)ZJ. This feature supports layer 3 backhauling to a Cisco PGW2200 using DPNSS and Digital Access Signaling System (DASS) User Adaptation (DUA) over Stream Control Transmission Protocol (SCTP).

DPNSS was developed by British Telecom and is used in the United Kingdom and some parts of Europe. DPNSS is a standard and open protocol used between PBXs in a private network that enables complex features to work on a network basis. This feature applies the DPNSS backhaul solution on Cisco gateways to provide connectivity and services to the PBXs running the DPNSS protocol.

Note The DPNSS protocol can run on both T1 and E1 interfaces, but only E1 interfaces are supported by this feature.

The DPNSS Backhaul feature includes the following benefits:

- DUA works with existing Q.931 or DPNSS and DASS-2 protocols on an application server process (ASP), in this case, the Cisco PGW2200.
- The IDSN User Adaptation Layer (IUA) with DUA and SCTP protocol stacks are written to be portable across operating systems and products.
- Memory allocation and system performance are not negatively affected by this feature.

For additional information, refer to the *Digital Private Network Signaling System Backhaul* feature module at:

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

Prerequisites

- You must have a suitable customer premises equipment (CPE) gateway with DPNSS backhaul capability and Media Gateway Control Protocol (MGCP) control for bearer circuit connections.
- You must be running Cisco PGW2200 release 9.4 or a later release.

Restrictions

- The DPNSS Backhaul feature does not support Layer 3 debugging at the GW.

Enhanced ITU-T G.168 Echo Cancellation

The third-party extended echo canceller (EC) feature is used in Cisco gateways with Cisco IOS Release 12.2(15)ZJ. The extended EC feature uses the Cisco voice digital signal processor (DSP) code base (DSPWare).

The G.168 extended EC feature provides an alternative to the Cisco-proprietary G.165 EC with improved performance for trunking gateway applications. The G.168 extended EC increases the configurable tail length from a maximum of 32 ms to a maximum of 64 ms. The ITU-T G.165 standard EC is still supported in this release.

This version of the extended EC feature adds support for the following:

- High- and medium-complexity C5421 DSP in NM-HDA voice cards
- Medium-complexity C5421 DSP in AIM-VOICE cards
- Medium-complexity digital C5409 DSP and high-complexity analog WICs in the Cisco Catalyst 4000 Access Gateway Module (AGM)
- Medium-complexity C549 DSP digital and analog in the Cisco MC3810 and Cisco 2400 platforms
- The command-line interface (CLI) has been modified to make the extended EC the default.

Cisco IOS software supports the following improvements with the extended EC:

- Configuration and reporting of extended echo path capacity
- Configuration and reporting of worst-case echo return loss (ERL)
- Test mode support for manually freezing, thawing, and clearing the EC h-register
- Reporting of statistics for location of the largest reflector
- Reporting of the internal state of the EC

This feature provides the following additional benefits:

- No changes to platform—Improves platform functionality by updating the EC module through a DSPWare upgrade and a Cisco IOS software upgrade
- Enabling and disabling of nonlinear processor—Enables and disables nonlinear processor (NLP) spectrally matched comfort noise
- Echo return loss (ERL) configuration—Can be set to three values: 0 dB, 3 dB, and 6 dB
- Expansion of Echo Canceller Capacity—EC capacity is expanded to 64 ms

For additional information, refer to the *Enhanced ITU-T G.168 Echo Cancellation* feature module at:

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

Restrictions

- Not all Cisco platforms that use C542 and C549 DSPs support the extended EC. All other platforms continue to use the Cisco-proprietary 32-ms EC by default.
- The NM-2V does not support the extended EC on the Cisco 3600 series.
- This feature is not supported on the Cisco 3631 routers.

Enhancements to 6- and 36-Port Ethernet Switch Network Modules

The feature support on the 16- and 36-port Ethernet switch network modules has been significantly enhanced in Cisco IOS Release 12.2(15)ZJ to include the following improvements.

Feature Enhancement	Description
802.1x	Supports new standard. IEEE 802.1x port-based authentication prevents unauthorized devices (clients) from gaining access to the network.
BackboneFast	BackboneFast provides fast convergence in the network backbone after a spanning-tree topology change occurs.
Layer 2 and Layer 3 CoS/DSCP Priority Mapping	IP Differentiated Services Code Point (IP DSCP) and class of service (CoS) marking priorities protect the performance of mission-critical applications.
Rate Limiting	QoS ACLs provide inbound and outbound rate limiting.
Security ACL	QoS ACLs define security policies.
IGMP Snooping	Internet Group Management Protocol (IGMP) snooping constrains the flooding of multicast traffic by dynamically configuring the interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast devices.
Per-Port Storm Control	Per-port storm control prevents broadcast, multicast, and unicast storms. Per-port storm-control uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.
Routed Ports	A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support subinterfaces. Routed ports can be configured with a Layer 3 routing protocol.
Fallback Bridging for SVIs (Switch Virtual Interfaces)	Fallback bridging forwards non-IP traffic between two or more VLANs. With fallback bridging, the switch bridges together two or more VLANs or routed ports, essentially connecting multiple VLANs within one bridge domain. Fallback bridging forwards traffic that the multilayer switch does not route and forwards traffic belonging to a nonroutable protocol such as DECnet.

Note RFC 2284, *PPP Extensible Authentication Protocol (EAP)*, is the new RFC that supports the 16- and 36-port Ethernet switch network module feature enhancements.

All Cisco 3600 series platforms are supported in the enhancements.

There are 47 new Cisco IOS commands that support the feature enhancements. For information on the commands, refer to the "Command Reference" section of the *16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series* feature module at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/fz1636nm.htm

For additional information on the feature enhancements, also refer to the *16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series* feature module at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/fz1636nm.htm

FRSVC Over ISDN

The Frame Relay Switched Virtual Circuits over ISDN feature provides support for Frame Relay switched virtual circuits (SVCs) over ISDN BRI lines. Before the introduction of this feature, Frame Relay over ISDN supported Frame Relay permanent virtual circuits (PVCs) only. Frame Relay SVCs can be configured on Dialer or BRI interfaces the same way that SVCs are configured on serial interfaces.

For additional information on Frame Relay, refer to the "Configuring Frame Relay" chapter of the *Cisco IOS Wide-Area Networking Configuration Guide* for Cisco IOS Release 12.2 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcffrely.htm

For additional information on Frame Relay SVCs, refer to the "Configuring Frame Relay SVCs" section in the "Configuring Frame Relay" chapter of the *Cisco IOS Wide-Area Networking Configuration Guide* for Cisco IOS Release 12.2 at the same URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcffrely.htm

MGCP-Controlled Backhaul of BRI Signaling

The Media Gateway Control Protocol (MGCP)-Controlled Backhaul of Basic Rate Interface (BRI) Signaling in Conjunction with Cisco CallManager feature is introduced on the Cisco 3600 series in Cisco IOS Release 12.2(15)ZJ.

The Media Gateway Control Protocol (MGCP)-Controlled Backhaul of Basic Rate Interface (BRI) Signaling in Conjunction with Cisco CallManager feature provides MGCP service to remote-office media gateways that connect by means of ISDN BRI trunks to a centralized Cisco CallManager media-gateway controller for the purpose of call processing. D-channel signal information is backhauled to the call manager through a Transmission Control Protocol (TCP) session.

Should connection to the primary call manager fail, call processing reverts to a backup call manager until the connection to the primary is restored. Should connections to the primary and all backups fail, call processing reverts to H.323 on the media gateway. When a connection is restored, call processing reverts to the primary or other available call manager and to MGCP.

Feature benefits include the following:

- Centralized call-management architecture, enabling a high degree of network control
- Short voice cut-through times
- Graceful evolution to new technology and to Architecture for Voice, Video, and Integrated Data (AVVID)

For additional information, refer to the *MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco CallManager* feature module at the following URL:

http://www.cisco.com/en/US/products/software/ios122/122newft/122limit/122z/122zj15/ftbribkh.htm

Prerequisites

Media Gateway

You need a supported Cisco 3600 series, router equipped with the following:

- 16-MB Flash memory
- 64-MB DRAM
- BRI voice interface card: VIC-2BRI-NT/TE or VIC-2BRI-S/T-TE
- Voice network module: NM-1V or NM-2V

Media-Gateway Controller

You need one or more Cisco CallManager systems, Version 3.3(2) Feature Pack 1 or higher.

Restrictions

- Only the ETSI BRI basic-net3 switch type is supported in this release.
- This feature is not supported on the Cisco 3631 routers.

Private Line Automatic Ringdown for Trading Turrets

Cisco IOS Release 12.2(15)ZJ introduces the Private Line Automatic Ringdown (PLAR) for Trading Turrets feature. This feature delivers Private Line Automatic Ringdown for the connection of turrets for the financial industry—primarily for corporations and enterprises that use turrets and POTS telephones for trading. Implementation of this feature ensures that a call between traders on a PLAR connection will be maintained if one of the traders goes on-hook or on-hold. This new capability also ensures that bandwidth is used only when needed.

The following Cisco IOS command was modified to support this feature:

- **connection** command—the **tied** keyword was added.

For additional command syntax and configuration information, refer to the *Private Line Automatic Ringdown for Trading Turrets* feature module at:

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

Prerequisite

To run Private Line Automatic Ringdown for Trading Turrets, you must install an IP Plus image (minimum) of Cisco IOS Release 12.2(15)ZJ or a later release.

Restrictions

- This feature is supported only for FXS loopstart ports and digital E&M immediate-start ports. When a voice port is configured with an incorrect destination number that may or may not be a valid number, the call may not perform as expected. There is no cross-checking for turret PLAR from the origination voice port, but there is a check on the terminating voice port to prevent accepting a call from a calling party that is not preconfigured.
- This feature is not supported on the Cisco 3631, Cisco 3640, and Cisco 3640/A routers.

Support for IP Communications Voice/Fax Network Modules

Cisco IOS Release 12.2(15)ZJ introduces support for the following new IP Communications Voice/Fax Network Modules:

- NM-HD-1V
- NM-HD-2V
- NM-HD-2VE

These network modules provide the ability to directly connect the PSTN and legacy telephony equipment to Cisco 2600XM series, Cisco 3600 series, and Cisco 3700 series modular access routers, enabling important applications such as IP telephony, toll bypass, and full gateway integration. These network modules support the following interface cards:

- New interface cards supported on all three network modules:
  - VIC2-2FXS
  - VIC2-2FXO
  - VIC2-4FXO
  - VIC2-2E&M
  - VIC2-2BRI-NT/TE
- Existing interface cards supported on NM-HD-2VE only:
  - VWIC-2MFT-T1
  - VWIC-1MFT-T1
  - VWIC-2MFT-T1-DI
  - VWIC-1MFT-E1
  - VWIC-2MFT-E1
  - VWIC-2MFT-E1-DI
  - VWIC-1MFT-G703
  - VWIC-2MFT-G703

The IP Communications Voice/Fax Network Modules bring next-generation features to voice network modules. Features supported in this release include the following:

- Channel group support for up to 32 channels
- Flex option for configuring codec complexity—This new option allows the DSP to process up to 16 channels. In addition to continuing support for configuring a fixed number of channels per DSP, the flex option enables the DSP to handle a flexible number of channels. The total number of supported channels varies from 6 to 16, depending on which codec is used for a call. Therefore, the channel density varies from 6 per DSP (high-complexity codec) to 16 per DSP (g.711 codec).
- Software-based echo cancellation up to 32-millisecond conversion
- Digital: BRI, PRI, and CAS
- Analog: FXS, FXO, E&M, and DID
- Signaling channel allocation
- CAMA-configured signaling
- Voice channel allocation
- Voice port independent channel allocation

- Hairpinning
  - Digital to digital (same card)
  - Analog to digital (same card)
- Channel bank support—Analog voice ports are internally connected to a DS0 time slot on a digital T1/E1 interface. All the signaling is transparently sent between the analog voice port and DS0 time slot, and will not be seen by the higher layer voice software.
- DSP crash recovery
- FXO/FXS Caller ID Type 1 and Type 2
- Trunk alarm handling

Prerequisites

- This feature requires Cisco IOS Release 12.2(15)ZJ or a later release.
- This feature requires 128 MB of RAM.

Cisco IOS Command Changes

The following commands are new or modified to support this feature:

- **codec complexity** command—the **flex** keyword was added
- **connect** command—the **voice-port** keyword was added

For additional command syntax information, prerequisite and configuration information, refer to the *IP Communications Voice/Fax Network Modules* feature module at:

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

Restrictions

This feature is not supported on the Cisco 3631 routers.

Support for the NM-16A/S Network Modules

Cisco IOS Release 12.2(15)ZJ introduces support for the NM-16A/S network module. The NM-16A/S is a slow-speed, high-density serial network module (NM) offering asynchronous and synchronous interfaces and flexible port configuration.

The NM-16A/S offers:

- Synchronous interfaces that support a data rate of up to 128 kbps
- Asynchronous interfaces that support a data rate of up to 115.2 kbps
- Configurable DTE and DCE

Note The NM-16A/S networking module uses a Cisco patented 12-in-1 Smart Serial cable.

With the appropriate serial transition cable, the ports on the NM-16A/S networking module can provide an EIA/TIA-232, EIA/TIA-449, V.35, X.21, EIA/TIA-530 DTE, or NRZ/NRZI serial interface.

The NM-16 A/S can provide an EIA/TIA-530A DTE interface.

The following Cisco IOS commands are introduced or modified to support this feature:

- **clock rate command—**modified to include the **line** keyword
- **debug serial lead-transition command—new**
- **ignore command—new,** interface configuration mode

For additional command syntax and configuration information, refer to the *NM-16A/S* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/gtnm16as.htm

Restrictions

- The NM-16A/S is factory configurable and not field upgradable.
- This feature is not supported on the Cisco 3640, and Cisco 3640/A routers.

Limitations and Restrictions

The Cisco 3620 routers are not supported in this release.

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 3600 series modular access routers.

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

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.

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 4 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.

Table 4 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ5 (continued)

DDTS ID Number	Description
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.
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.

Table 4 Resolved Caveats for Cisco IOS Release 12.2(15)ZJ5 (continued)

DDTS ID Number	Description
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.
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 5 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 6 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 6 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 6 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 6 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 6 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, issue **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 6 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

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)ZJ1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 7 Open Caveats for Cisco IOS Release 12.2(15)ZJ1

DDTS ID Number	Description
CSCea65197	No fast busy when SIP AA trigger is disabled Symptoms: The user is disconnected without any busy tones when transferred to unreachable destination. Conditions: This behavior can occur when the transferrer uses SIP BYE/ALSO to transfer the call and the transfer target is an invalid or unassigned number. Workaround: There is no workaround.
CSCeb22796	Transferrer leg not getting released for SIP call Symptoms: ITS-A----VoIP(SIP)----CSPS----ITS-B IP Phone-A1 calls IP Phone-B1, call connected IP Phone-B1 transfers IP Phone-A1 to IP Phone-A2 or FXS-A2 on alerting Call is transferred IP Phone-A1 and IP Phone-A2 or FXS-A2 can talk, but IP Phone-B1 does not get released cleanly. Instead it hears a fastbusy and displays unknown number. SIP messages show that the call transaction leg does not exist. Conditions: This behavior can occur when the transferee and transfer-to endpoints are attached to the same gateway and the transfer is committed during alerting. Workaround: There is no workaround.
CSCeb27770	ephone keeps ringing when Disc with PI is received Symptoms: ephone --- 1760 ITS --- BRI --- PSTN PSTN calls ephone, PSTN hangs up before ephone answers. PSTN sends Disconnect with PI = 8, ephone keeps on ringing Workaround: Configure the **disc_pi_off** command on the voice-port.

Table 7 Open Caveats for Cisco IOS Release 12.2(15)ZJ1 (continued)

DDTS ID Number	Description
CSCeb37176	Caller-ID update is wrong in Caller-id block situations Symptoms: The remote party display information is not updated properly after a call transfer. Conditions: IP Phone A1 calls IP Phone B1 across VoIP. A1 blocks caller-id presentation by dialing *123 before dialing the destination digits. IP Phone B1 correctly displays "Private." For a transfer commit while alerting, the following behavior is seen: 1. IP Phone A1 presses the transfer button and dials IP Phone A2 (which is on the same Gateway as A1). 2. IP Phone A2 rings, then IP Phone A1 presses transfer. 3. When IP Phone A2 answers, IP Phone A2 and IP Phone B1 are connected successfully and: a. IP Phone B1 sees IP Phone A2's number (as expected). b. IP Phone A2 changes display from "From IP Phone A1" to "From Private" instead of "From IP Phone B1." For a transfer commit after connect, the following behavior is seen: 1. IP Phone A1 presses the transfer button and dials IP Phone A2 (which is on the same Gateway as A1). 2. IP Phone A2 answers. 3. On IP Phone A1 there are 2 displays: a. To IP Phone B1. b. To IP Phone A1 and IP Phone A2's phone number (incorrect). 4. On pressing transfer: a. IP Phone B1 sees IP Phone A2's number. b. IP Phone A2 changes display from "From IP Phone A1" to "From Private" instead of "From IP Phone B1." Workaround: There is no workaround.
CSCeb42731	HD-2VE can only support up to 31 hdlc channels Symptoms: The network module NM-HD-2VE can only support up to 31 HDLC channels. Workaround: There is no workaround.
CSCin46584	IPIPgw doesn’t transfer the IEs completely Symptoms: • An INFO message received after CONNECT is not forwarded to the other call leg. • A NOTIFY message received before CONNECT is not forwarded to the other call leg. Conditions: This behavior occurs when the default session application is set to process the call. Workaround: Configure the **application session** command on the incoming dial-peer.

Table 7 Open Caveats for Cisco IOS Release 12.2(15)ZJ1 (continued)

DDTS ID Number	Description
CSCuk41974	Ringback tone and fast busy tone not as per the cptone configured Symptoms: The ringback tone provided during alerting and the fast busy tone provided at the end of the call is not as per the cptone configured on the gateway under the voice-port. Workaround: There is no workaround.
CSCuk42727	E_DSM_DSP_PROTOCOL_ERROR during fax pass through call Symptoms: S:S_DSM_BRIDGED E:E_DSM_DSP_PROTOCOL_ERROR] when making a Fax pass through call. Workaround: There is no workaround.

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)ZJ5. 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
CSCea22283	Wrong voice mail box selected when call fwded across multiple phones Symptoms: Caller reaches original destination's voicemail when forwarded-to destination is not available. Conditions: If a call is forwarded across multiple IP phones, the voicemail box selected is that of the originally called number. For example: A calls B and the call is forwarded to C. C does not answer and the call gets forwarded to B's voice mail (instead of C's voicemail). Workaround: There is no workaround.

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

DDTS ID Number	Description
CSCea87260	dpnss: channels not kept in OOS when E1 controller/serial int down Symptoms: The DLCs end up in the "IDLE" state even though there is a shutdown on the controller/interface. Conditions: When there is a shutdown on the controller/interface and PGW requests GW to bring up the DLCs. Workaround: There is no workaround.
CSCeb01098	Release Source not being set by new Session app Symptoms: The Release Sources reported in the radius accounting record or the gateway's call history record for the incoming and outgoing legs don't match. This behavior does not affect the voice call. Conditions: This behavior may occur when the default voice application handles the incoming call. Workaround: Configure the **application default.c.old** command on the incoming dial-peer used for the call.
CSCuk42484	wrong cause value when transferring to busy/unallocated number Symptoms: The wrong cause value is provided when transferring a call to an unallocated or busy destination. Conditions: This behavior can occur when an incoming call VoIP call is handled by the app-h450-transfer.2.0.0.3.tcl application. The gateway will place an outbound VoIP call instead of disconnecting the incoming call with the appropriate cause code under the following two conditions: • If the transfer target is a telephony or ITS destination that is busy or unallocated, and • If there is a VoIP dial-peer that matches the transfer target phone number In this case, the final cause value returned to the incoming call will depend on the outgoing call setup request. Workaround: There is no workaround.
CSCuk43681	call mishandled when calling an unallocated number Symptoms: Congestion tone is not provided to the caller when a call setup attempt fails with cause 'Temporary Failure'(41 / 0x29). Workaround: There is no workaround.

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
CSCea22283	Wrong voice mail box selected when call forwarded across multiple phones Symptoms: Caller reaches original destination's voicemail when forwarded-to destination is not available. Conditions: If a call is forwarded across multiple IP phones, the voicemail box selected is that of the original called number. For example: A calls B and the call is forwarded to C. C does not answer and the call gets forwarded to Be's voice mail (instead of A's voicemail). Workaround: There is no workaround.
CSCea31140	dpnss layer 2 fails to receive frames with debug on Symptoms: Router fails to receive and send any DPNSS signalling frames. Conditions: This happens when 1) debugs like the **debug isdn Q921** command are turned on, 2) IUA backhaul connection of the GW to the PGW is not established yet, and 3) SABMRs are received from the peer PBX to bring up DLCs on the interface. Workaround: Reload the router.
CSCea38543	7902 as XOR cannot make consult-transfer on alerting Symptoms: Transfer-with-consultation does not work properly with ITS. Blind transfer still works. Workaround: Disable transfer-with-consultation on the ITS when handling the 7902 phone. Use blind transfer only with the 7902 in ITS.
CSCea87260	dpnss: channels not kept in OOS when E1 controller/serial int down Symptoms: The DLCs end up in the IDLE state even though there is a shut on the controller/interface. Conditions: When there is a shut on the interface/controller and PGW instructs GW to bring up the DLCs. Workaround: There is no workaround.
CSCea89997	High Pitch Sound heard if pick up phone during ringing with NM-HDA Symptoms: For users using an NM-HDA FXS voice-port, if user picks up the phone during the ring-on cycle, user will hear a high pitch sound (distorted ringing) until ring-off. If user picks up the phone during the ring-off cycle, this problem will not occur. Conditions: Using NM-HDA network module on an FXS interface. Workaround: There is no workaround.

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

DDTS ID Number	Description
CSCeb01098	Release Source not being set by new Session app Symptoms: The Release Sources reported in the radius accounting record or the gateway's call history record for the incoming and outgoing legs don't match. This behavior does not affect the voice call. Conditions: This behavior may occur when the default voice application handles the incoming call. Workaround: Configure the **application session.c.old** command on the incoming dial-peer used for the call.
CSCeb11681	3745 crashes on call transfer between PRI and BRI Symptoms: The gateway may reload when an IP phone transfers a call. This may happen when the transferred party is connected through ISDN PRI and the transfer target is connected through ISDN BRI. Workaround: There is no workaround.
CSCuk41974	Ringback tone and fast busy tone not as per the cptone configured Symptoms: The ringback tone provided during alerting, and the fast busy tone provided at the end of the call is not as per the cptone configured on the gateway under the voice-port. Workaround: There is no workaround.
CSCuk42484	wrong cause value when transferring to busy/unallocated number Symptoms: The wrong cause value is provided when transferring a call to an unallocated or busy destination. Conditions: This behavior can occur when an incoming call VoIP call is handled by the app-h450-transfer.2.0.0.3.tcl application. If the transfer target is telephony or ITS destination that is busy or unallocated, and if there is a VoIP dial-peer that matches the transfer target phone number, the gateway will place an outbound VoIP call instead of disconnecting the incoming call with the appropriate cause code. In this case, the final cause value returned to the incoming call will depend on the outgoing call setup request. Workaround: There is no workaround.
CSCuk42727	E_DSM_DSP_PROTOCOL_ERROR during fax pass through call Symptoms: S:S_DSM_BRIDGED E:E_DSM_DSP_PROTOCOL_ERROR] when making a Fax pass through call. 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)ZJ5. 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

DDTS ID Number	Description
CSCdz59865	Routed port back to L2 port and unnumbered serial interface. Symptoms: Changing a routed port back to a L2 port causes a serial interface to be left configured with the **IP unnumbered** command while the routed port interface no longer exists. Conditions: Configure a serial interface with **ip unnumbered fastether** *1/0* where the fastether 1/0 is a routed port. Then change back the routed port to L2 port (switched port). This leaves the serial interface configured with **ip unnumbered fastether***1/0*, but there is no interface (routed port) with a valid IP addresses. Workaround: Don't use the **Unnumbered** command.
CSCdz72542	storm-control and no storm-control become global mode Symptoms: Incomplete Storm control CLI will switch configuration mode to global mode rather than per port Storm control configuration mode. Conditions: Configuring the **no storm-control** command in interface configuration mode. Workaround: Use the **no storm-control broadcast | unicast | multicast** command instead of just the **no storm-control** command in interface configuration mode.
CSCdz76940	Fast switching not working on Routed Port. Symptoms: Routed port does not fast-switch IP traffic although router is configured for IP fast-switching Conditions: Configure IP fast switching. Workaround: There is no workaround.
CSCdz87738	show isdn status does not retrieve all info Symptoms: Output of the **show isdn status** command doesn't display the isdn status information of all the isdn interfaces. Conditions: The problem appears only when one of the interfaces is configured with a switch type of primary-dpnss. Workaround: Use the **show isdn status** *serial-interface-number* command to get the output of an individual interface.

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

DDTS ID Number	Description
CSCea02355	rare ip packets may cause input queue wedge 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
CSCea26990	Routed port to Stacking-partner and still associated to IP address. Symptoms: Routed port converted back to L2 (switchport) and used as stacking partner retains OSPF configuration as seen in show ip ospf interface. Conditions: Change a routed port to L2 (switchport) without explicitly removing IP address. Workaround: There is no workaround.
CSCea30041	L2 port down down, but displays linkup UP UP message continuously. Symptoms: Fails to bring link UP UP when configured to speed 10 and adjacent router's on-board fe is configured to speed auto. Also displays wrong message about the link changing state to UP UP. Conditions: L2 port configured for 10 MB and other router as speed auto. Workaround: Set speed manually.
CSCea34734	dpnss: calls on virtual channels fail Symptoms: When the PBX sends a call on a Virtual B-Channel, IOS acks the packet correctly and attempts to send it on to the PGW. The PGW does not do anything, and no call trace is created. Either the PGW does not handle the virtual call or the packet is misformed. Workaround: There is no workaround.
CSCea40714	Router crash at Dpnss_test_frame_timer when unconfiguring pri-nfas Symptoms: Router unexpectedly reloads when pri-group is unconfigured on the controller using the **no pri-group timeslots 1-31** command. Conditions: None. Workaround: There is no workaround.

Related Documentation

The following sections describe the documentation available for the Cisco Cisco 3600 series modular access routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents. Use these release notes with these documents:

Platform-Specific Documents

These documents are available for the Cisco 3600 series modular access routers on Cisco.com:

- Quick Start Guide documents for the Cisco 3600 series
- Hardware Installation Documents for Cisco3600 series
- Software Configuration Documents for Cisco 3600 series
- Regulatory Compliance and Safety Documents for Cisco 3600 series

On Cisco.com at:

Products & Services: Routers: Cisco 3600 Series Multiservice Platforms: Technical Documentation

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

Cisco Product Documentation: Access Servers and Routers: Modular Access Routers: Cisco 3600 Series Routers

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(15)ZJ 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, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On Cisco.com, beginning under the **Products & Services** heading:

Cisco IOS Software: Cisco IOS Software Releases: Cisco IOS Release 12.2 T: Technical Documentation: Configuration Guides and Command References

Release 12.2 Documentation Set

Note You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the paper documents were printed.

On Cisco.com, beginning under the **Products & Services** heading:

Cisco IOS Software: Cisco IOS Software Releases: Cisco IOS Release 12.2 Mainline: Configuration Guides and Command References

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
• *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

Table 11 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *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
• *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

Table 11 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *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)	

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 48