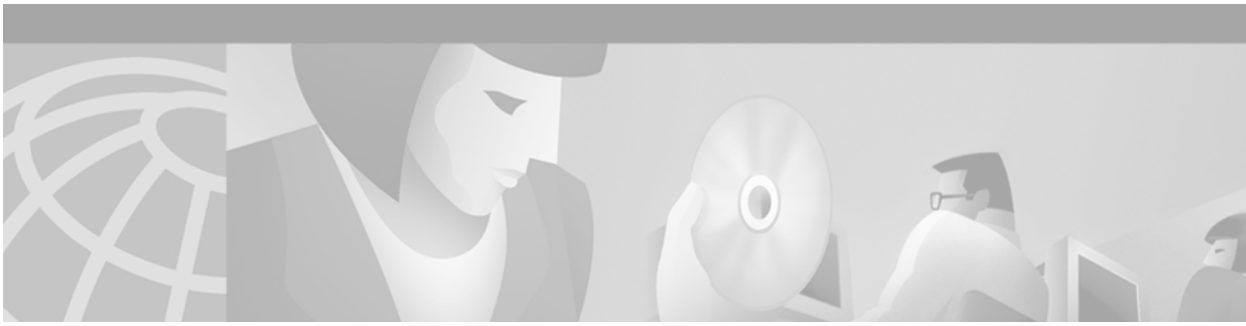

Release Notes for Cisco IGX 8400 Series Universal Router Module for Cisco IOS Release 12.2 XB

January 13, 2004

Cisco IOS Release 12.2(2) XB15

OL-1796-01 Rev. D1

These release notes for the Cisco IGX 8400 series universal router module (URM) describe the enhancements provided in Cisco IOS Release 12.2(2) XB15. These release notes are updated as needed.

For a list of the software caveats that apply to Release 12.2(2) XB15, see Caveats for Cisco IOS Release 12.2 XB, page 25.

Contents

These release notes describe the following topics:

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

Introduction

The Cisco IGX 8400 series platforms function as components of Cisco's end-to-end voice architecture. The Cisco IOS software runs only on the URM; all other components of the Cisco IGX 8400 series platform run Switched Software (SWSW).

The URM is a Cisco IOS-based IP router blade that enables users to provision Voice over IP (VoIP) and Voice over ATM (VoATM) on a Cisco IGX 8400 series platform. The voice and routing capabilities of the URM have been derived from the Cisco 3660 series routers, while the ATM capabilities of the URM have been derived from the existing enhanced Universal Switching Module (UXM-E) that is used on a Cisco IGX 8400 series platform.

In addition to VoIP and VoATM, IP routing and Cisco IOS command language interface (CLI) commands—which allow configuration of the voice ports and dial peers—are now available on the Cisco IGX 8400 series platforms.

The URM interoperates with all Cisco IOS-based voice products and supports 30 voice channels with high-complexity codec types and 60 voice channels with medium-complexity codec types. Note that only digital voice ports are supported on the URM; analog ports are not supported.

The Universal Router Module (URM) is an optional module for the Cisco IGX 8400 series and delivers high-density voice interfaces, Fast Ethernet connectivity and ATM switching. For further information about URM, refer to the "Universal Router Module" section on page 4.

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.2(2) XB15, see the "New and Changed Information" section on page 9 and the "Related Documentation" section on page 32.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(2) XB15 and includes the following sections:

Memory Recommendations

Table 1 Memory Recommendations for the Cisco IGX 8400 Series URM

Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
IP Plus	urm-is-mz	40 MB	128 MB	RAM
Enterprise Plus IPsec 3DES	urm-jk9s-mz	40 MB	128 MB	RAM
Enterprise Plus	urm-js-mz	40 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(2) XB15 supports the URM. This section provides an overview of the hardware of the Cisco IGX 8400 series switches and the URM.

IGX Switches

Like other Cisco switches, the IGX switch operates in public or private Wide Area Networks (WANs). An IGX switch can support OC3, T3, E3, T1, E1, Inverse Multiplexing Over ATM (IMA) for T1 or E1, fractional T1 or E1, or subrate digital transmission facilities. The IGX cell relay technology provides maximum throughput with minimum delays. Cell relay performance characteristics are the heart of efficient digital networks and make the IGX switch an ideal choice for a high-performance, multimedia platform. Key features of the IGX switch include:

- A 1-gigabit-per-second (Gbps) Cellbus for high-speed switching and a redundant 0.2 Gbps bus for backup.
- Full compatibility with BPX system software.
- Up to 64 circuit lines, 32 trunks, and 3500 connections on the Cisco IGX 8420 and IGX 8430.
- IGX configuration and management through Cisco WAN Manager or the same standard user interface used with the BPX WAN switching system software.
- High-performance switching suitable for a variety of protocols/applications, including Channel Associated Signaling (CAS), Asynchronous Transfer Mode (ATM), Frame Relay, voice, FAX, slow-scan and full-bandwidth video, and synchronous or asynchronous data.
- Six cabinet models, which consist of:
  - An 8-slot standalone unit (Model 8410, standalone)
  - An 8-slot rack-mount unit (Model 8410, rack-mount)
  - A 16-slot standalone unit (Model 8420, standalone)
  - A 16-slot rack-mount unit (Model 8420, rack-mount)
  - A 32-slot standalone unit (Model 8430, standalone)
  - A 32-slot rack-mount unit (Model 8430, rack-mount)
- Redundancy of controller cards, service module cards, system buses, and power supplies to provide hardware reliability.

- Hot-swappable modules to facilitate nonstop operation: service cards, NPMs, AC-power supplies, and fan tray assembly.
- 110/220 VAC and -48 DC power options for use in varied network environments.

Universal Router Module

The Universal Router Module (URM) is an optional module for the Cisco IGX 8400 series and delivers high-density voice interfaces, Fast Ethernet connectivity and ATM switching. The URM consists of the following cards:

- One URM front card

  The 1-slot-wide front card contains an embedded UXM-E and an embedded router (based on the Cisco 3660 series router) running Cisco IOS software. The front card integrates all memory components, including Battery-Backed RAM (BRAM) and Flash memory for the storage of Cisco IOS software.

- One URI-2FE2V back card

  The 1-slot-wide back card (BC-URI-2FE2VT1 or BC-URI-2FE2VE1) contains an installed voice and WAN interface card (VWIC) with a generic dual-port T1 or E1 digital voice interface. Integrated digital signal processors (DSPs) handle the packetization of voice streams. The back card provides the following physical interfaces:

  – Two Fast Ethernet interfaces (RJ-45)

  – Two T1 or E1voice ports (RJ-48)

  – One console port (RJ-45)

- One URI-2FE back card

  The back card provides the following physical interfaces:

  – Two Fast Ethernet interfaces (RJ-45)

  – One console port (RJ-45)

The URM can connect to another Cisco router in the following ways:

- Through its 155 Mbps ATM interface (on the embedded UXM-E in the URM front card) to the IGX backplane (ATM-to-ATM [URM to UXM] or ATM/FR SIW [URM to UFM] connections can be established with SWSW)
- Through its two Fast Ethernet Ports

For detailed information about the hardware of the URM, see the *Update to Cisco IGX 8400 Series Installation and Configuration and Reference* at http://www.cisco.com/univercd/cc/td/doc/product/wanbu/igx8400/9_3_20/update/9_3_22rn.htm.

For information on configuring voice features, see *Cisco IOS Voice Features on IGX 8400 Series Universal Router Module* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_igxxb.htm.

URM LAN

The Cisco IOS Release 12.2(2)XB introduces that URM LAN (BC-URI-2FE), a new IOS-based router blade that supports data only traffic on a Cisco IGX 8400 Series URM, providing routing capabilities that have been derived from the Cisco 3660 series routers. This feature also introduces support of AIM-VPN/HP, an optional Advance Integration Module (AIM) expansion card that offloads the tasks of encryption/decryption and authentication of user data from the IOS software. AIM-VPN/HP is a hardware Layer 3 (IPsec) encryption module that provide DES (56-bit) and 3DES (168-bit) IPsec encryption for multiple T1s or E1s of bandwidth. Hardware encryption is supported with the AIM-VPN/HP daughter module. This module is a field replaceable unit (FRU) and resides in the AIM slot of the URM.

URMs can be enabled with this new feature by upgrading to IGX switch software 9.3.30 and Cisco IOS Release 12.2(2)XB images, as well as by adding an AIM-VPN module.

The URM LAN supports Remote Router Configuration (RRC) which is an RAS feature allows first time configuration of a URM router blade in a remote IGX without connecting a terminal physically to the URM.

For more information, see *Installing VPN Encryption Modules in Cisco 2600 Series and Cisco 3600 Series Routers* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/aim_inst/vpn_aim.htm.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco IGX 8400 series URM, log in to the Cisco IGX 8400 series URM and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 XB Software (urm-is-mz), Version 12.2(2) XB15, RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

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

Software Requirements

A Cisco IGX 8400 series platform with a URM running Cisco IOS Release 12.2(2) XB15 requires Switch Software Net Revision 9.3.20 or later.

Features

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.2(2) XB15 supports the same feature sets as Cisco IOS Release 12.1(5) YA, but Cisco IOS Release 12.2(2) XB15 includes the URM LAN feature and two new images supported by the Cisco IGX 8400 series URM. The new images are Enterprise Plus and Enterprise Plus IPsec 3DES.

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

Table 2 lists the features and feature sets supported by the Cisco IGX 8400 series URM in Cisco IOS Release 12.2(2) XB15 and uses the following conventions:

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

Table 2 Feature List by Feature Set for the Cisco IGX 8400 Series Universal Router Module

Features	In	Software Images by Feature Sets		
		IP Plus	Enterprise Plus IPsec 3DES	Enterprise Plus
Connectivity				
COPS[1] for RSVP[2]	12.1(5)YA[3]	Yes	Yes	Yes
L2TP[4] Dial Out	12.1(5)YA[3]	Yes	Yes	Yes
L2TP Tunnel Management Enhancements	12.1(5)YA[3]	Yes	Yes	Yes
L2TP Tunnel Switching	12.1(5)YA[3]	Yes	Yes	Yes
IP Multicast				
Bidirectional PIM[5]	12.1(5)YA[3]	Yes	Yes	Yes
IGMP[6] Version 3	12.1(5)YA[3]	Yes	Yes	Yes
Multilayer Switching for IP Multicast	12.1(5)YA[3]	Yes	Yes	Yes
PIM Dense Mode State Refresh	12.1(5)YA[3]	Yes	Yes	Yes
Router-Port Group Management Protocol (RGMP)	12.1(5)YA[3]	Yes	Yes	Yes
Source-Specific Multicast	12.1(5)YA[3]	Yes	Yes	Yes
UDLR[7] Tunnel ARP[8] and IGMP Proxy	12.1(5)YA[3]	Yes	Yes	Yes
Management				
AutoInstall Using DHCP[9] for LAN Interfaces	12.1(5)YA[3]	Yes	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco IGX 8400 Series Universal Router Module

Features	In	Software Images by Feature Sets		
		IP Plus	Enterprise Plus IPsec 3DES	Enterprise Plus
Circuit Interface Identification MIB[10]	12.1(5)YA[3]	Yes	Yes	Yes
Class-Based Quality of Service MIB	12.1(5)YA[3]	Yes	Yes	Yes
Event MIB	12.1(5)YA[3]	Yes	Yes	Yes
Individual SNMP[11] Trap Support	12.1(5)YA[3]	Yes	Yes	Yes
Interface Index Persistence	12.1(5)YA[3]	Yes	Yes	Yes
Interface MIB for ATM[12] Subinterfaces	12.1(5)YA[3]	Yes	Yes	Yes
MSDP[13] MIB	12.1(5)YA[3]	Yes	Yes	Yes
Multicast Routing Monitor	12.1(5)YA[3]	Yes	Yes	Yes
NTP[14] MIB	12.1(5)YA[3]	Yes	Yes	Yes
Parser Cache	12.1(5)YA[3]	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	12.1(5)YA[3]	Yes	Yes	Yes
Subnetwork Bandwidth Manager	12.1(5)YA[3]	Yes	Yes	Yes
Quality of Service				
Class-Based Weighted Fair Queueing	12.1(5)YA[3]	Yes	Yes	Yes
Configurable per ATM-VC[15] Hold Queue Size	12.1(5)YA[3]	Yes	Yes	Yes
DiffServ[16] -Compliant WRED[17]	12.1(5)YA[3]	Yes	Yes	Yes
Express RTP and TCP[18] Header Compression	12.1(5)YA[3]	Yes	Yes	Yes
IP-to-ATM Class of Service (CoS)	12.1(5)YA[3]	Yes	Yes	Yes
Network-Based Application Recognition	12.1(5)YA[3]	Yes	Yes	Yes
RSVP Support for Low-Latency Queueing	12.1(5)YA[3]	Yes	Yes	Yes
Security				
AAA[19] Broadcast Accounting	12.1(5)YA[3]	Yes	Yes	Yes
AAA Server Group Deadtimer	12.1(5)YA[3]	Yes	Yes	Yes
Dial-on-Demand Authentication Enhancements	12.1(5)YA[3]	Yes	Yes	Yes
Interactive Voice Response for Cisco Access	12.1(5)YA[3]	Yes	Yes	Yes
Secure Shell Version 1 Integrated Client	12.1(5)YA[3]	Yes	Yes	Yes
Switches				
URM LAN	**12.2(2)XB**	Yes	Yes	Yes
Voice				
Answer Supervision Reporting	12.1(5)YA[3]	Yes	Yes	Yes
Asynchronous Rotary Line Queuing	12.1(5)YA[3]	Yes	Yes	Yes
Caller ID	12.1(5)YA[3]	Yes	Yes	Yes
Configurable Timers in H.225[20]	12.1(5)YA[3]	Yes	Yes	Yes
Dial Peer Enhancements	12.1(5)YA[3]	Yes	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco IGX 8400 Series Universal Router Module

Features	In	Software Images by Feature Sets		
		IP Plus	Enterprise Plus IPsec 3DES	Enterprise Plus
Ecosystem Gatekeeper Interoperability Enhancements	12.1(5)YA[3]	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements: Phase 2	12.1(5)YA[3]	Yes	Yes	Yes
Gateway-to-Gatekeeper Billing Redundancy	12.1(5)YA[3]	Yes	Yes	Yes
H.323[21] Support for Virtual Interfaces	12.1(5)YA[3]	Yes	Yes	Yes
H.323 Version 2, Phase 2	12.1(5)YA[3]	Yes	Yes	Yes
PSTN[22] Fallback	12.1(5)YA[3]	Yes	Yes	Yes
QSIG[23] Protocol Support	12.1(5)YA[3]	Yes	Yes	Yes
Session Initiation Protocol for Voice over IP	12.1(5)YA[3]	Yes	Yes	Yes
T.38 Fax Relay for VoIP H.323	12.1(5)YA[3]	Yes	Yes	Yes
Transparent Common Channel Signaling	12.1(5)YA[3]	Yes	Yes	Yes
Trunk Conditioning for FRF.11[24] and Cisco Trunks	12.1(5)YA[3]	Yes	Yes	Yes
V.110 Support	12.1(5)YA[3]	Yes	Yes	Yes
Voice Busyout Enhancements	12.1(5)YA[3]	Yes	Yes	Yes
Voice over ATM	12.1(5)YA[3]	Yes	Yes	Yes
VoIP Call Admission Control using RSVP	12.1(5)YA[3]	Yes	Yes	Yes
WAN Services				
ATM LANE[25] FSSR Protocol	12.1(5)YA[3]	Yes	Yes	Yes
Closed User Group Selection Facility Suppress Option	12.1(5)YA[3]	Yes	Yes	Yes
Debit Card for Packet Telephony	12.1(5)YA[3]	Yes	Yes	Yes
DNS[26] for X.25[27]	12.1(5)YA[3]	Yes	Yes	Yes
ISDN Network Side for ETSI[28] Net5 PRI[29]	12.1(5)YA[3]	Yes	Yes	Yes
PPPoE[30] on ATM	12.1(5)YA[3]	Yes	Yes	Yes
PPPoE over IEEE[31] 802.1Q VLANs[32]	12.1(5)YA[3]	Yes	Yes	Yes

1. COPS = Common Open Policy Service
2. RSVP = Resource Reservation Protocol
3. In Cisco IOS Release 12.1(5) YA, this feature supported the IP Plus image only. The Enterprise Plus IPsec 3DES and Enterprise Plus images are additional images supported by this feature in Cisco IOS Release 12.2(2) XB15.
4. L2TP = Layer 2 Tunnel Protocol
5. PIM = Protocol-Independent Multicast
6. IGMP = Internet Group Management Protocol
7. UDLR = Unidirectional Link Routing
8. ARP = Address Resolution Protocol
9. DHCP = Dynamic Host Configuration Protocol
10. MIB = Management Information Base

11. SNMP = Simple Network Management Protocol
12. ATM = Asynchronous Transfer Mode
13. MSDP = Multicast Source Discovery Protocol
14. NTP = Network Time Protocol
15. VC = virtual circuit
16. DiffServ = Differentiated Services
17. WRED = Weighted Random Early Detection
18. TCP = Transmission Control Protocol
19. AAA = authentication, authorization, and accounting
20. H.225 = An ITU standard that governs H.225.0 session establishment and packetization. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of RTP.
21. H.323 = Extension of ITU-T standard H.320 that enables videoconferencing over LANs and other packet-switched networks, as well as video over the Internet.
22. PSTN = plain old telephone service
23. QSIG = Q (point of the ISDN model) Signaling
24. FRF.11 = Frame Relay Forum implementation agreement for Voice over Frame Relay (v1.0 May 1997). This specification defines multiplexed data, voice, fax, DTMF digit-relay and CAS/Robbed-bit signaling frame formats, but does not include call setup, routing, or administration facilities.
25. LANE = LAN emulation
26. DNS = Domain Name System
27. X.25 = ITU-T standard that defines how connections between DTE and DCE are maintained for remote terminal access and computer communications in PDNs. X.25 specifies LAPB, a data link layer protocol, and PLP, a network layer protocol. Frame Relay has to some degree superseded X.25.
28. ETSI = European Telecommunication Standards Institute
29. PRI = Primary Rate Interface
30. PPPoE = Point-to-Point Protocol over Ethernet
31. IEEE = Institute of Electrical and Electronics Engineers
32. VLANs = virtual local-area networks. Note that the *PPPoE over IEEE 802.1Q VLANs* feature is sometimes referred to as the *PPP over Fast Ethernet 802.1Q* feature.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco IGX 8400 series URM for Cisco IOS Release 12.2(2) XB15.

New Hardware and Software Features in Cisco IOS Release 12.2(2)XB14 to Cisco IOS Release 12.2(2)XB15

No new hardware and software features are supported by the Cisco IGX 8400 series URM for Cisco IOS Release 12.2(2)XB14 to Cisco IOS Release 12.2(2)XB15.

New Hardware and Hardware Features in Cisco IOS Release 12.2(2)XB9 to Cisco IOS Release 12.2(2)XB13

Cisco IOS Release 12.2(2)XB9 through Cisco IOS Releae 12.2(2)XB13 do not support the CiscoIGX 8400 series URM.

Note Cisco IOS Release 12.2(2)XB9 is not distributed for widespread availability. Cisco IOS Release 12.2(2)XB13 does not exist.

New Hardware and Hardware Features in Cisco IOS Release 12.2(2)XB8

There are no new hardware and software features are supported by the Cisco IGX 8400 series URM for Cisco IOS Release 12.2(2)XB8.

New Hardware and Hardware Features in Cisco IOS Release 12.2(2)XB4 to Cisco IOS Release 12.2(2)XB7

Cisco IOS Release 12.2(2)XB4 through Cisco IOS Releae 12.2(2)XB7 do not support the CiscoIGX 8400 series URM.

New Hardware and Hardware Features in Cisco IOS Release 12.2(2)XB3

There are no new hardware and software features are supported by the Cisco IGX 8400 series URM for Cisco IOS Release 12.2(2)XB3.

New Hardware and Hardware Features in Cisco IOS Release 12.2(2)XB2

Cisco IOS Release 12.2(2)XB2 does not support the CiscoIGX 8400 series URM.

New Hardware and Hardware Features in Cisco IOS Release 12.2(2)XB1

Cisco IOS Release 12.2(2)XB1 does not support the CiscoIGX 8400 series URM.

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

The following new hardware feature is supported by the Cisco IGX 8400 series URM for Cisco IOS Release 12.2(2)XB.

URM LAN

The Cisco IOS Release 12.2(2)XB introduces that URM LAN (BC-URI-2FE), a new IOS-based router blade that supports data only traffic on a Cisco IGX 8400 Series URM, providing routing capabilities that have been derived from the Cisco 3660 series routers. This feature also introduces support of AIM-VPN/HP, an optional Advance Integration Module (AIM) expansion card that offloads the tasks of encryption/decryption and authentication of user data from the IOS software. AIM-VPN/HP is a hardware Layer 3 (IPsec) encryption module that provide DES (56-bit) and 3DES (168-bit) IPsec encryption for multiple T1s or E1s of bandwidth. Hardware encryption is supported with the AIM-VPN/HP daughter module. This module is a field replaceable unit (FRU) and resides in the AIM slot of the URM.

URMs can be enabled with this new feature by upgrading to IGX switch software 9.3.30 and Cisco IOS Release 12.2(2)XB images, as well as by adding an AIM-VPN module.

The URM LAN supports Remote Router Configuration (RRC) which is an RAS feature allows first time configuration of a URM router blade in a remote IGX without connecting a terminal physically to the URM.

For more information, see *Installing VPN Encryption Modules in Cisco 2600 Series and Cisco 3600 Series Routers* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/aim_inst/vpn_aim.htm.

New Software Features in Cisco IOS Release 12.2(2) XB15

There are no software features supported by the Cisco IGX 8400 series URM for Cisco IOS Release 12.2(2) XB15.

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

This section documents new software features that are supported by the Cisco IGX 8400 series URM for Release 12.1(5)YA. The following types of features are documented:

Connectivity Features

COPS for RSVP

Common Open Policy Service (COPS) is a protocol for communicating network traffic policy information to network devices. Resource Reservation Protocol (RSVP) is a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting across the Internet will perform at the desired speed and quality.

The COPS for RSVP feature gives network managers centralized monitoring and control of RSVP, including the ability to:

- Refer all RSVP flow requests to an external policy server for processing
- Accept or reject the flow based on policy decision
- Communicate information about flows installed on the router to policy servers to aid in management
- Permit policy servers to remove previously installed flows in order to meet bandwidth or policy requirements

L2TP Tunnel Management Enhancements

The L2TP Tunnel Enhancements feature fills an existing tunnel with sessions up to a configured limit. Then it creates a new tunnel to the next destination IP address in the configured load-sharing group. It fills this new tunnel to the limit.

L2TP Tunnel Switching

The L2TP Tunnel Switching feature is a tunnel aggregation feature. It enables entire tunnels to be switched in the existing VPDN Multihop feature. Previously, only individual sessions could be switched.

IP Multicast Features

Bidirectional PIM

Bidirectional PIM is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco IOS implementation of PIM supports three modes for a multicast group:

- Dense mode
- Sparse mode
- Bidirectional mode

A router can simultaneously support all three modes or any combination of them for different multicast groups. In bidirectional mode, traffic is only routed along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidirectional PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address does not need to be a router, but can be an unassigned IP address on a network that is reachable throughout the PIM domain. Using this technique is actually the preferred configuration for establishing a redundant RP configuration for bidirectional PIM.

IGMP Version 3

The Internet Group Management Protocol (IGMP) is a protocol used by IPv4 systems to report IP multicast group memberships to neighboring multicast routers. On networks with hosts directly attached, IGMP Version 3 (IGMPv3) adds support for "source filtering" which enables a multicast receiver to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. Based on this membership information, Cisco IOS software only forwards traffic that is requested by the host (or by other routers via Protocol Independent Multicast [PIM]) to that network. In addition to restricting traffic on the network of the receiver host, IGMPv3 membership information may also be propagated to multicast routing protocols to enable the forwarding of traffic from permitted sources or to restrict traffic from denied sources along the entire multicast data delivery path.

In the Source-Specific Multicast feature, hosts must explicitly include sources when joining a multicast group (this is known as "channel subscription"). IGMPv3 is the industry-designated standard protocol for hosts to signal-channel subscriptions in Source-Specific Multicast (SSM). In deployment cases where IGMPv3 cannot be used (for example, if it is not supported by the receiver host or its applications), there are two other mechanisms to enable SSM: URL Rendezvous Directory (URD) and IGMP v3lite.

PIM Dense Mode State Refresh

The PIM Dense Mode State Refresh feature keeps the pruned state in PIM dense mode from timing out by periodically forwarding a control message down the source-based distribution tree. The control message refreshes the prune state on the outgoing interfaces of each router in the distribution tree.

Router-Port Group Management Protocol

The Router-Port Group Management Protocol (RGMP) feature supports a Cisco protocol that restricts IP multicast traffic in switched networks. RGMP is a Layer 2 protocol that enables a router to communicate to a switch (or a networking device that is functioning as a Layer 2 switch) the multicast group for which the router would like to receive or forward traffic.

Source-Specific Multicast

The Source-Specific Multicast (SSM) feature is an extension of IP multicast, where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. When SSM is used, only source-specific multicast distribution trees (no shared trees) are created.

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is the core networking technology for the Cisco implementation of the IP Multicast light suite of solutions targeted for audio and video broadcast application environments.

UDLR Tunnel ARP and IGMP Proxy

Most protocols in the Internet assume that links are bidirectional. In particular, routing protocols used by directly connected routers no longer behave properly in the presence of a unidirectional link, such as a satellite link. The Unidirectional Link Routing (UDLR) feature enables a router to emulate the behavior of a bidirectional link for operation of IP over unidirectional links.

The UDLR Tunnel ARP and IGMP Proxy feature includes enhancements to the existing UDLR tunnel mechanism, support for the Address Resolution Protocol (ARP), and the addition of the Internet Group Management Protocol (IGMP) proxy mechanism.

Management Features

AutoInstall Using DHCP for LAN Interfaces

The AutoInstall Using DHCP for LAN Interfaces feature replaces the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces. AutoInstall is a Cisco IOS software feature that provides for the configuration of a new routing device automatically when the device is initialized. DHCP (defined in RFC 2131) is based on the Bootstrap Protocol, which provides the framework for passing configuration information to hosts on a Transmission Control Protocol (TCP)/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options. In Cisco IOS Release 12.1(5)YA, the IP address procurement phase of the AutoInstall process is now accomplished using DHCP for LAN interfaces. Prior to this release, IP addresses for LAN interfaces were obtained using BOOTP during the AutoInstall process. The AutoInstall Using DHCP for LAN Interfaces feature also allows the routing device to recognize IP address allocation messages coming from regular BOOTP servers, providing a seamless transition for those devices already using BOOTP servers for AutoInstall. This feature also allows for the uploading of configuration files using unicast Trivial File Transfer Protocol (TFTP).

Circuit Interface Identification MIB

The Circuit Interface Identification MIB feature adds support for a new Cisco enterprise MIB, used for monitoring individual circuits using SNMP. The Circuit Interface Identification MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object that can be used to provide a description of individual circuit-based interfaces (for example, interfaces using ATM or Frame-Relay). This description will then be returned when linkup and linkdown SNMP traps are generated for the described interface.

Class-Based Quality of Service MIB

The Class-Based Quality of Service Management Information Base (Class-Based QoS MIB) provides read access to class-based QoS configurations. This MIB also provides QoS statistics information based on the Modular QoS CLI, including information regarding class map and policy map parameters.

This Class-Based QoS MIB is actually two MIBs: CISCO-CLASS-BASED-QOS-MIB and CISCO-CLASS-BASED-QOS-CAPABILITY-MIB.

Event MIB

The Event MIB is an asynchronous notification mechanism standardized for use by network management systems using Simple Network Management Protocol (SNMP). The Event MIB provides the ability to monitor Management Information Base (MIB) objects on a local or remote system using SNMP and initiate simple actions whenever a trigger condition is met (for example, an SNMP trap can be generated when an object is modified). By allowing notifications based on events, the Network Management System (NMS) does not need to constantly poll managed devices to find out if something has changed. When combined with the Expression-MIB support, Event-MIB support in Cisco IOS software provides a flexible and efficient way to monitor complex conditions on network devices.

Individual SNMP Trap Support

The Individual SNMP Trap Support feature adds the ability to enable or disable SNMP system management notifications (traps) individually. SNMP traps that can be specified are “authentication”, “linkup”, “linkdown”, and “coldstart”. This feature expands the functionality of the **snmp-server enable traps snmp** command.

Interface Index Persistence

One of the identifiers most commonly used in SNMP-based network management applications is the Interface Index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface; as far as most software is concerned, the ifIndex is the "name" of the interface. Although there is no requirement in the relevant RFCs that the correspondence between particular ifIndex values and their interfaces be maintained across reboots, applications such as device inventory, billing, and fault detection increasingly depend on the maintenance of this correspondence.

Cisco IOS Release 12.1(5)YA adds support for an ifIndex value that can persist across reboots, allowing users to avoid the workarounds previously required for consistent interface identification. The Interface Index Persistence feature allows for greater accuracy when collecting and processing network management data by uniquely identifying input and output interfaces for traffic flows and SNMP statistics. Relating each interface to a known entity (such as an ISP customer) allows network management data to be used more effectively.

MSDP MIB

The Multicast Source Discovery Protocol (MSDP) MIB feature adds support in Cisco IOS software for the MSDP MIB. This MIB describes objects used for managing MSDP operations using Simple Network Management Protocol (SNMP). Documentation for this MIB exists in the form of an Internet Draft titled "Multicast Source Discovery Protocol MIB" (draft-ietf-msdp-mib-03.txt) and is available through the Internet Engineering Task Force (IETF) at http://www.ietf.org. Refer to the following document for further information:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5msdp.htm

NTP MIB

The Network Time Protocol (NTP) is used to synchronize timekeeping among a set of distributed time servers and clients. The Cisco NTP MIB enables users to remotely monitor an NTP server using the Simple Network Management Protocol (SNMP), provided the MIB itself is implemented on that server. Use of the NTP MIB to monitor the NTP status of routing devices is accomplished using software on a Network Management System (NMS). There are no new or modified Cisco IOS software commands associated with this feature.

The Cisco implementation of the NTP MIB is based on NTP version 3 (RFC-1305). The MIB objects are all read-only. SNMP requests are processed by reading the corresponding variables from the NTP subsystem and returning them in the response. The NTP MIB defines a set of NTP server system objects, including an NTP server peers table and an NTP server filter register table. For complete details on the Cisco implementation of the NTP MIB, see the MIB file itself ("CISCO-NTP-MIB.my", available through Cisco.com at http://www.cisco.com/public/mibs/v2/).

Parser Cache

The Parser Cache feature optimizes the parsing (translation) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines. This feature was developed to improve the scalability of the Cisco IOS software command-line interface (CLI) parser when processing large configuration files. This improvement is especially useful when thousands of virtual circuits must be configured for interfaces or hundreds of access lists (ACLs) are required. The parser chain cache can rapidly recognize and translate configuration lines that differ slightly from previously used configuration lines (for example, pvc 0/100, pvc 0/101, and so on). Testing indicates an improvement to load time of between 30% and 36% for large configuration files when using the parser cache.

The parser cache is enabled by default on all platforms using Cisco IOS 12.1(5)YA or later. A new command, **[no] parser cache**, allows the disabling or re-enabling of this feature.

SNMP Support for IOS vLAN Subinterfaces

The SNMP Support for IOS vLAN Subinterfaces enhancement provides sparse table support for Fast Ethernet subinterfaces similar to what is currently provided for Frame Relay subinterfaces.

Quality of Service Features

Configurable per ATM-VC Hold Queue Size

The Configurable per ATM-VC Hold Queue Size (for ATM Adapters) feature allows customers to specify the number of packets contained in the hold queue, per virtual circuit (VC), on ATM adapters that support per-VC queueing. By default, the queueing mechanism in use determines the size of the hold queue, and, therefore, the number of packets contained in the queue. This feature allows customers to expand the default hold queue size and change (or vary) the number of packets the queue can contain. With this new feature, the hold queue can contain a maximum of 1024 packets. This feature provides a new command, **vc-hold-queue**, that allows the customer to specify the number of packets contained in the per-VC hold queue. This can be a number from 5 to 1024.

DiffServ-Compliant WRED

The DiffServ-Compliant Weighted Random Early Detection (WRED) feature extends the functionality of WRED to enable support for Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB). This feature enables WRED to be compliant with the DiffServ standard and the AF PHB standard being developed by the Internet Engineering Task Force (IETF). This feature enables customers to implement AF PHB by coloring packets according to differentiated services code point (DSCP) values and then assigning preferential drop probabilities to those packets.This feature adds two new commands, **random-detect dscp** and **dscp**. It also adds two new arguments, *dscp-based* and *prec-based***,** to two existing WRED-related commands—the **random-detect** (interface) command and the **random-detect-group** command

Network-Based Application Recognition

Network-Based Application Recognition (NBAR) is a classification engine that recognizes a wide variety of applications, including web-based and other difficult-to-classify protocols that utilize dynamic TCP/User Datagram Protocol (UDP) port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by working with QoS features to provide bandwidth guarantees and limits, traffic shaping, and packet marking.

NBAR supports several new classification features:

- Classification of applications that dynamically assign TCP/UDP port numbers
- Classification of HTTP traffic by URL, HOST, or MIME type
- Classification of Citrix ICA traffic by application name
- Classification of application traffic using subport information

NBAR also can classify static port protocols. Although Access Control Lists (ACLs) can be used for this purpose, NBAR is easier to configure and can provide classification statistics that are not available when using ACLs.

NBAR provides a special Protocol Discovery feature that determines which application protocols are traversing a network at any given time. The Protocol Discovery feature captures key statistics associated with each protocol in a network. These statistics can be used to define traffic classes and QoS policies for each traffic class.

For additional information on NBAR, see the *Network-Based Application Recognition* feature module on Cisco.com and the Documentation CD-ROM.

RSVP Support for Low-Latency Queueing

RSVP is a network-control protocol that provides a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across networks achieve the desired quality of service (QoS).

RSVP enables real-time traffic (which includes voice flows) to reserve resources necessary for low latency and bandwidth guarantees.

RSVP uses weighted fair queuing (WFQ) to provide fairness among flows and to assign a low weight to a packet to attain priority. However, the preferential treatment provided by RSVP is insufficient to minimize the jitter because of the nature of the queuing algorithm itself. As a result, the low latency and jitter requirements of voice flows might not be met in the prior implementation of RSVP and WFQ.

Security Features

AAA Broadcast Accounting

The AAA Broadcast Accounting feature allows accounting information to be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

With the introduction of this feature, broadcasting is now allowed among groups of servers. The server groups can be either Remote Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+). And each server group can define its backup servers for failover independently of other groups. (Failover is a process that can occur when more than one server has been defined within a server group. Failover refers to the process by which information is sent to the first server in a server group; if the first server is unavailable, the information is sent to the next server in the server group. This process continues until the information is successfully sent to one of the servers within the server group or until the list of available servers within the server group is exhausted.)

AAA Server Group Deadtimer

The AAA Server Group Deadtimer feature allows each authentication, authorization, and accounting (AAA) server to be fully configured in the server group. Thus, you can direct AAA traffic to separate groups of servers that have different operational characteristics.

With the introduction of this feature, deadtime has been added as a new attribute to the server group structure. In addition, a separate timer has been attached to each server host in every server group. Therefore, when a server is found to be unresponsive after numerous retransmissions and timeouts, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. The timers are checked and subsequent requests to a server (once it is assumed to be dead) are directed to alternate timers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers (if running) for that server in all server groups.

If the timer has expired, only the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.

Note The deadtime attribute is supported only for RADIUS hosts.

Secure Shell Version 1 Integrated Client

Secure Shell (SSH) is a protocol that provides a secure remote connection to another router. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The Secure Shell Version 1 Integrated Client feature is an application running over TCP/IP to provide strong authentication and encryption. The SSH client enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network. The SSH client in Cisco IOS software works with publicly and commercially available SSH servers.

Voice Features

For information on configuring voice features, see the *Cisco IOS Voice Features on IGX 8400 Series Universal Router Module* feature module. For information on feature modules, see the "Feature Modules" section on page 33.

Answer Supervision Reporting

The Answer Supervision Reporting feature is an enhancement to the information request (IRR) Registration, Admission, and Status protocol (RAS) message that enables gatekeepers to maintain call accounting information by reporting the call connection time of connected calls to the gatekeeper.

In H.323 configurations, direct call-routed signaling is used by the endpoint (gateway). Gatekeepers do not have real-time knowledge or control over the state of a call and are dependent on the endpoints to provide them the necessary real-time information, such as the call connect time, call termination time, and call termination reason.

When a call ends, the gateway sends a Disengage Request (DRQ) message with the "BillingInformationToken" (which contains the duration of the call) to the gatekeeper. If the gatekeeper does not receive the DRQ message for some reason, the gatekeeper will not have the information about when the call started or the duration of the call, which is necessary to maintain accounting information.

The Answer Supervision Reporting feature addresses the need to report the call connection time to the gatekeeper upon the connection of a call and at periodic intervals thereafter. The Answer Supervision Reporting feature adds a proprietary Cisco parameter, the call connection time parameter, to the "perCallInfo" parameter in the "nonStandardData" field, which is located in the IRR message. When a CONNECT message is received, the originating gateway sends the unsolicited IRR message to its gatekeeper. On sending a CONNECT message, the terminating gateway sends the unsolicited IRR message to its gatekeeper. If the admission confirmation (ACF) message has a nonzero value for the IRR frequency parameter, the gateway sends the unsolicited IRR message to its gatekeeper at periodic intervals, which are determined by the value in the IRR frequency parameter.

Asynchronous Rotary Line Queuing

The Asynchronous Rotary Line Queuing feature allows Telnet connection requests to busy asynchronous rotary groups to be queued so that users automatically obtain the next available line, rather than needing to try repeatedly to open a Telnet connection. The Cisco IOS software sends a periodic message to the user to update progress in the connection queue.

Connections are authenticated using the method specified for the line configurations for the asynchronous rotary group. If a connection is queued, authentication is done prior to queuing and no authentication is done when the connection is later established.

Caller ID

Caller ID (sometimes called CLID or ICLID for incoming call line identification) is an analog service offered by a Central Office (CO), which supplies calling party information to subscribers. Typically, the calling party number, and sometimes the name, appears on a station (also called extension) device such as a PC telephony software application screen or the display on a telephone. Type 1 Caller ID provides the calling party information while the call is ringing, and Type 2 Caller ID provides the additional convenience of calling number display while the recipient is on another call. In this release, Cisco provides only Type 1 Caller ID support.

Configurable Timers in H.225

The Configurable Timers in H.225 feature allows users to configure the H.255 TCP connection timeout value for all outgoing call attempts (on a per-VoIP dial-peer basis).

In previous releases of the Cisco IOS software, the call attempt timeout was 15 seconds and could not be changed. In some cases, however, users might need a shorter timeout value to facilitate a faster fail-over. In other cases, users might need a greater timeout value.

The Configurable Timers in H.225 feature addresses those needs by allowing the user to override the default of 15 seconds and configure the timeout value.

Dial Peer Enhancements

The Dial Peer Enhancements are supported for Voice over IP, Voice over Frame Relay, and Voice over ATM. The following enhancements to dial peer configuration lower the complexity of dial planning and reduce the amount of effort in creating dial peer entries:

- Additional Dial String Symbols—These new dial string symbols are added: Percent, plus, question mark, period, brackets, and parenthesis.
- Translation Rule Implementation—When configuring your dial peers, you are provided with an option called the translation rule. This rule applies a translation rule to a calling party number (Automatic Number Identification [ANI]) or a called party number (Dial Number Information Service [DNIS]) for both incoming and outgoing calls within Cisco H.323 voice-enabled gateways. Also, the rule allows translation of the type of number. Refer to the Q.931 ITU specification for details.
- Number-Type Matching—To match on a number type for a dial peer call leg, the **numbering-type** command is used in dial-peer configuration mode.
- Digit Strip Option—When a called number is received and matched to a POTS dial peer, the matched digits are stripped and the remaining digits are forwarded to the voice interface. A new command, **digit strip**, makes this default behavior an option.

For more information, see the two *Dial Peer Enhancement* feature modules on Cisco.com at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dt0390s7.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtdpeer.htm

Ecosystem Gatekeeper Interoperability Enhancements

The Ecosystem Gatekeeper Interoperability Enhancements feature allows gateways to move between gatekeepers without requiring a reconfiguration of the gateway or a gatekeeper failover in the gateway.

Gateways can be configured to switch from their primary gatekeeper to an alternate gatekeeper if a failure or outage occurs. If an outage occurs and gateways move from one gatekeeper to another, there may be an imbalance in the number of gateways registered to each gatekeeper. The Ecosystem Gatekeeper Interoperability Enhancements helps to restore the balance (when the outage has been corrected) by allowing some of the gateways to be moved back to their proper gatekeepers.

The Ecosystem Gatekeeper Interoperability Enhancements feature supplements the existing support for alternate gatekeepers and adds support for the alternate gatekeeper field (altGKInfo) to the gatekeeper rejection (GRJ) and registration rejection (RRJ) messages. This allows a gateway to move between gatekeepers during the gatekeeper request (GRQ) and registration request (RRQ) phases.

Ecosystem Gatekeeper Interoperability Enhancements: Phase 2

The Ecosystem Gatekeeper Interoperability Enhancements: Phase 2 feature supplements the existing support for alternate gatekeepers and adds support for the alternate gatekeeper field (altGKInfo) to the admission rejection (ARJ). This allows a gateway to move between gatekeepers during the admission request (ARQ) phase.

The Ecosystem Gatekeeper Interoperability Enhancements: Phase 2 allows gateways to move between gatekeepers without requiring a reconfiguration of the gateway or a gatekeeper failover in the gateway.

Gateways can be configured to switch from their primary gatekeeper to an alternate gatekeeper if a failure or outage occurs. If an outage occurs and gateways move from one gatekeeper to another, there may be an imbalance in the number of gateways registered to each gatekeeper. The Ecosystem Gatekeeper Interoperability Enhancements: Phase 2 helps to restore the balance (when the outage has been corrected) by allowing some of the gateways to be moved back to their proper gatekeepers.

Gateway-to-Gatekeeper Billing Redundancy

The Gateway-to-Gatekeeper Billing Redundancy feature enhances the accounting capabilities of the Cisco H.323 gateway and provides support for Vocaltec gatekeepers. The Gateway-to-Gatekeeper Billing Redundancy feature provides redundant billing information to an alternate gatekeeper if the primary gatekeeper to which a gateway is registered becomes unavailable.

During the process of establishing a call, the primary gatekeeper sends an admission confirmation (ACF) message to the registered gateway. The ACF message includes the user's billing information and an access token. To provide the billing information to an alternate gatekeeper if the primary gatekeeper is unavailable when the call session ends, the access token information sent in the ACF message in now also included in the disengage request (DRQ) message that is sent to the alternate gatekeeper.

This features enables the alternate gatekeeper to obtain the billing information required to successfully complete the transaction.

H.323 Support for Virtual Interfaces

The H.323 Support for Virtual Interfaces feature allows users to configure the IP address of the gateway, so that the IP address included in the H.323 packet is deterministic and consistently indicates the same address for the source.

In previous releases of the Cisco IOS software, the source address included in the H.323 packet could vary depending on the protocol (RAS, H.225, H.245, or RTP). This made it difficult to configure firewall applications to work with H.323 messages.

The H.323 Support for Virtual Interfaces feature addresses that difficulty by allowing the user to explicitly configure an IP address to be used for all protocols.

H.323 Version 2, Phase 2

The Cisco H.323 Version 2, Phase 2 feature adds the following benefits to Cisco H.323 gatekeepers, gateways, and proxies:

- H.323v2 Fast Connect allows endpoints to establish media channels for audio exchange without waiting for a separate H.245 connection to be opened.
- H.245 tunneling allows H.245 messages to be encapsulated within Q.931 messages using H.225 (using Fast Connect) without the use of a separate H.245 TCP connection.
- H.450.2 Call Transfer Without Consultation and H450.3 Call Deflection provide a limited subset of features to support Internet call waiting
- H.235 security allows only duly authorized and authenticated gateways to access gatekeeper resources.
- Translation of Foreign Exchange Station (FXS) hookflash to H.245 user input along with the previously suggested translation of H.245 user input to FXO hookflash provides end-to-end hookflash relay in FXS-to-Foreign Exchange Office (FXO) configurations.
- Gatekeeper Transaction Message Protocol (GKTMP) for the Cisco gatekeeper with a corresponding user API for the UNIX environment, which allows a third party to develop elements to control and utilize a gatekeeper.
- Cisco gatekeeper supports the Gatekeeper MIB, which allows SNMP management.
- Gateway support for the Alternate Endpoint field in ACF allows third-party gatekeepers to provide more robust call establishment.
- Gateway support for network-based billing number on a per-interface basis allows third-party gatekeepers to obtain per-call interface usage information for billing or other purposes.
- Gateway support for the voice-port description allows third-party gatekeepers to obtain customer-specific, per-call interface usage information for billing or other purposes.

PSTN Fallback

PSTN Fallback provides a mechanism to monitor congestion in the IP network and either redirect calls to the PSTN or reject calls based on the network congestion. PSTN Fallback does not provide assurances that a call that proceeds over the IP network is protected from the effects of congestion. This is the function of the other QoS mechanisms such as IP RTP Priority or low-latency queueing (LLQ).

QSIG Protocol Support

QSIG Protocol Support allows Cisco voice-switching services to connect private branch exchanges (PBXs), key systems (KTs), and central office switches (COs) that communicate by using the Q Signaling (QSIG) protocol, which is becoming the standard for PBX interoperability in Europe and North America. QSIG is a variant of ISDN D-channel signaling. With QSIG, Cisco networks emulate the functionality of the public-switched telephone network (PSTN), and QSIG signaling messages allow the dynamic establishment of voice connections across a Cisco wide-area network (WAN) to a peer router, which can then transport the signaling and voice packets to a second private integrated services network exchange (PINX). QSIG enables digit forwarding on POTS (plain old telephone service) dial peers.

Session Initiation Protocol for Voice over IP

Voice over Internet Protocol (VoIP) currently implements ITU's H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. Session Initiation Protocol (SIP) is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999.

The Cisco SIP functionality enables the URM to signal the setup of voice and multimedia calls over IP networks; therefore, the SIP feature provides an alternative to H.323 within the VoIP internetworking software.

T.38 Fax Relay for VoIP H.323

T.38 Fax Relay for VoIP H.323 provides standards-based fax relay protocol support for H.323 gateways and gatekeepers. T.38 is an ITU-T recommended standard for fax relay. Since T.38 is a standards-based implementation for fax relay, Cisco gateways and gatekeepers are able to communicate with third-party H.323 devices that support T.38 protocol.

Transparent Common Channel Signaling

Transparent Common Channel Signaling (T-CCS) allows the connection of two PBXs with digital interfaces that use a proprietary or unsupported CCS protocol without the need for interpretation of CCS signaling for call processing. T1/E1 traffic is transported transparently through the data network and the feature preserves proprietary signaling. From the PBX standpoint, this is accomplished through a point-to-point connection. Calls from the PBXs are not routed, but follow a preconfigured route to the destination.

Trunk Conditioning for FRF.11 and Cisco Trunks

Trunk Conditioning for FRF.11 and Cisco Trunks is an enhancement that adds the following capabilities to the trunk conditioning feature on the URM:

- Busyout of ports interfacing with a local PBX if a network trunk is out of service (OOS)
- Suppression of voice traffic when no calls are in progress or when the network trunk is OOS

This feature applies to analog telephony connections and digital T1/E1 using CAS/robbed-bit "ABCD" signaling. It does not apply to digital T1/E1 connections using CCS type signaling.

V.110 Support

This feature implements the V.110 protocol on the URM.

Voice Busyout Enhancements

The local voice busyout feature provides a way to busy out a voice port if a monitored network interface changes state. When a monitored interface changes to a specified state—to out-of-service or in-service—the voice port presents a seized/busyout condition to the attached PBX or other customer premises equipment (CPE). The PBX or other CPE can then attempt to select an alternate route.

Local voice busyout is supported on analog and digital voice ports using channel associated signaling (CAS).

This feature allows you to perform the following tasks:

- Configure individual voice ports to enter the busyout state whenever specified network interfaces go out of service or come into service
- Force individual voice ports into the busyout state
- Define the voice-port actions for the busyout state
- Force one or more DS0 timeslots on a controller into the busyout state

Note This feature is different from busy-back, the signal sent from the network to the calling party to indicate a busy (or congested) state along the route.

Voice Over ATM

Voice over ATM enables a URM to carry voice traffic (for example, telephone calls and faxes) over an ATM network by using ATM encapsulation ATM adaptation layer (AAL) 5.

VoIP Call Admission Control using RSVP

The VoIP Call Admission Control using RSVP feature synchronizes RSVP procedures with H.323 Version 2 (Fast Connect) setup procedures to guarantee that the required Quality of Service (QoS) for VoIP calls is maintained across the IP network. In earlier Cisco IOS releases, VoIP gateways used H.323 Version 1 (Slow Connect) procedures when initiating calls requiring bandwidth reservation. This feature, which is enabled by default, allows gateways to use H.323 Version 2 (Fast Connect) for all calls, including those requiring RSVP.

WAN Services Features

Closed User Group Selection Facility Suppress Options

A closed user group (CUG) selection facility is a specific encoding element that allows a destination data terminal equipment (DTE) to identify the CUG to which the source and destination DTEs belong. The Closed User Group Selection Facility Suppress Option feature enables a user to configure an X.25 data communications equipment (DCE) interface or X.25 profile with a DCE station type to remove the CUG selection facility from incoming call packets destined for the preferential CUG only or for all CUGs. You can also remove the selection facility from a CUG with outgoing access (CUG/OA).

ISDN Network Side for ETSI Net5 PRI

The ISDN Network Side for ETSI Net5 PRI feature enables Cisco IOS to replicate the public switched network interface to a PBX that is compatible with the ETSI Net5 switch type.

Routers and PBXs are both traditionally CPE with respect to the public switched network interfaces. For Voice over IP (VoIP) applications, it is desirable to interface access servers to PBXs with the access server representing the public switched network.

Enterprise organizations use the current VoIP features with Cisco products to reduce long-distance costs for phone calls within and outside of their organizations. However, there are times that a call cannot go over VoIP and the call needs to be placed using the PSTN. The customer then must have two devices connected to a PBX to allow some calls to be placed using VoIP and some calls to be placed over the PSTN. In contrast, this feature allows Cisco access servers to connect directly to user-side CPE devices such as PBXs and allows voice calls and data calls to be placed without requiring two different devices to be connected to the PBXs.

This feature enables the access server to provide a standard ISDN PRI network-side interface to the PBXs and to mimic the behavior of legacy phone switches. To a PBX, the access server functions as a Net5 PRI switch. No change in PBX capability or behavior is required.

PPPoE on ATM

The PPPoE on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. With this model, each host utilizes its own PPP over Ethernet (PPPoE) stack and the user is presented with a familiar user interface. Access control, billing and type of service can be done on a per-user, rather than a per-site, basis. Before a point-to-point connection over Ethernet can be provided, each PPP session must learn the Ethernet address of the remote peer and establish a unique session identifier. A unique session identifier is provided by the PPPoE Discovery Stage protocol.

The PPPoE on ATM feature provides service-provider digital subscriber line (DSL) support. As service providers begin DSL deployments, two of their most significant goals are to ease and facilitate consumer end adoption and to preserve as much of the dialup model as possible. PPPoE serves to advance both of these goals by leveraging Ethernet scale curves and embedded base (such as ATM NICs) and by preserving the point-to-point session used by Internet service providers (ISPs) in today's dialup model.

PPPoE over IEEE 802.1Q VLANs

The PPPoE over IEEE 802.1Q VLANs feature adds support for running PPP over Fast Ethernet over IEEE 802.1Q encapsulation. IEEE 802.1Q encapsulation enables you to interconnect a virtual local area networks (VLAN)-capable router with another VLAN-capable device. The packets on the 802.1Q link contain a standard Fast Ethernet frame and the VLAN information associated with that frame.

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 3.

Table 3 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Caveats for Cisco IOS Release 12.2 XB

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

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

Open Caveats—Cisco IOS Release 12.2(2)XB15

There are no open caveats specific to Cisco IOS Release 12.2(2)XB15 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(2)XB15

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB15. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 4 Resolved Caveats for Cisco IOS Release 12.2(2)XB15

DDTS ID Number	Description
CSCec87533	ios fw hang then crash with h323 corrupt 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.

Open Caveats—Cisco IOS Release 12.2(2)XB14

There are no open caveats specific to Cisco IOS Release 12.2(2)XB14 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(2)XB14

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB14. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(2)XB14

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.
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.
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

Table 5 Resolved Caveats for Cisco IOS Release 12.2(2)XB14 (continued)

DDTS ID Number	Description
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.
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.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(2)XB14 (continued)

DDTS ID Number	Description
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.
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.

Table 5 Resolved Caveats for Cisco IOS Release 12.2(2)XB14 (continued)

DDTS ID Number	Description
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.
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.

No Caveats—Cisco IOS Release 12.2(2)XB9 to Cisco IOS Release 12.2(2)XB13

Cisco IOS Release 12.2(2)XB9 through Cisco IOS Release 12.2(2)XB12 does not support the Cisco IGX 8400 series URM.

Cisco IOS Release 12.2(2)XB13 does not exist, so no caveats are documented.

Open Caveats—Cisco IOS Release 12.2(2)XB8

There are no open caveats specific to Cisco IOS Release 12.2(2)XB8 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(2)XB8

There are no resolved caveats specific to Cisco IOS Release 12.2(2)XB8 that require documentation in the release notes.

Open Caveats—Cisco IOS Release 12.2(2)XB4 to Cisco IOS Release 12.2(2)XB7

Cisco IOS Release 12.2(2)XB4 through Cisco IOS Release 12.2(2)XB7 does not support the Cisco IGX 8400 series URM.

Resolved Caveats—Cisco IOS Release 12.2(2)XB4 to Cisco IOS Release 12.2(2)XB7

Cisco IOS Release 12.2(2)XB4 through Cisco IOS Release 12.2(2)XB7 does not support the Cisco IGX 8400 series URM.

Open Caveats—Cisco IOS Release 12.2(2)XB3

There are no open caveats specific to Cisco IOS Release 12.2(2)XB3 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(2)XB3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 6 Resolved Caveats for Cisco IOS Release 12.2(2)XB14

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

Open and Resolved Caveats—Cisco IOS Release 12.2(2)XB2

Cisco IOS Release 12.2(2)XB2 does not support the Cisco IGX 8400 series URM.

Open and Resolved Caveats—Cisco IOS Release 12.2(2)XB1

Cisco IOS Release 12.2(2)XB1 does not support the Cisco IGX 8400 series URM.

Open Caveats—Cisco IOS Release 12.2(2)XB

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

Resolved Caveats—Cisco IOS Release 12.2(2)XB

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

Related Documentation

The following sections describe the documentation available for the Cisco IGX 8400 series URM. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

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

Use these release notes with these documents:

- Release-Specific Documents, page 32
- Platform-Specific Documents, page 33
- Feature Modules, page 33
- Feature Navigator, page 34

Release-Specific Documents

Note Since Cisco IOS Release 12.2(2) XB15 is based on Cisco IOS Release 12.1(5) YA, Cisco IOS Release 1.21 documents are listed in this section.

The following documents are specific to or support Cisco IOS Release 12.2(2) XB15 and are located on Cisco.com and the Documentation CD-ROM:

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

  On Cisco.com at:

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

  On the Documentation CD-ROM at:

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

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

  Technical Documents

- The *"Caveats for Cisco IOS Release 12.2 XB" section on page 25*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2 XB" in these release notes, see *Caveats for Cisco IOS Release 12.1* and *Caveats for Cisco IOS Release 12.1 T*, which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.1 and Cisco IOS Release *12.1 T*.

  On Cisco.com at:

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

On the Documentation CD-ROM at:

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

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

Platform-Specific Documents

The documents listed below document the Cisco IGX 8400 series switches and are available on Cisco.com and on the Documentation CD-ROM.

- *Port Concentrator Shelf Installation, Release 1.0*
- *Cisco IGX 8400 Series Installation and Configuration Guide*
- *Update to the Cisco iGX 8400 Series Installation and Configuration Guide and Cisco IGX 8400 Series Reference Guide, Release 9.3.20*
- *Cisco IGX 8400 Series Reference Guide, Release 9.3.00*
- *Command Reference, Release 9.3.20*
- *Update to the Cisco WAN Switch Command Reference Guide*
- *Cisco IGX 8400 Series Regulatory Compliance and Safety Information*

  On Cisco.com at:

  Technical Documents: Cisco Product Documentation: WAN Switches: Cisco IGX 8400 Series

  On the Documentation CD-ROM at:

  Cisco Product Documentation: WAN Switches: Cisco IGX 8400 Series

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(2) XB15 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

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

On the Documentation CD-ROM at:

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

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

Cisco IOS Software Documentation Set

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

Note Since Cisco IOS Release 12.2(2) XB15 is based on Cisco IOS Release 12.1(5) YA, Cisco IOS Release 1.21 documents are listed in this section.

Documentation Modules

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

On Cisco.com at:

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

On the Documentation CD-ROM at:

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

Cisco IOS Release 12.1 Documentation Set Contents

Table 7 lists the contents of the Cisco IOS Release 12.1 software documentation set, which is available in electronic form and in printed form if ordered.

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

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.1

On the Documentation CD-ROM at:

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

Table 7 Cisco IOS Release 12.1 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management Cisco IOS User Interfaces Commands Cisco IOS File Management Commands Cisco IOS System Management Commands
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume I* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume II*	Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking
• *Cisco IOS Dial Services Configuration Guide: Terminal Services* • *Cisco IOS Dial Services Configuration Guide: Network Services* • *Cisco IOS Dial Services Command Reference*	Preparing for Dial Access Modem Configuration and Management ISDN and Signaling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Interworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces

Table 7 Cisco IOS Release 12.1 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS IP and IP Routing Configuration Guide* • *Cisco IOS IP and IP Routing Command Reference*	IP Addressing and Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring 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, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
• *Cisco IOS Multiservice Applications Configuration Guide* • *Cisco IOS Multiservice Applications Command Reference*	Multiservice Applications Overview Voice Video Broadband
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms Quality of Service Solutions
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation

Table 7 Cisco IOS Release 12.1 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Dial Services Quick Configuration Guide* • *Cisco IOS Software System Error Messages* • *New Features in 12.1-Based Limited Lifetime Releases* • *New Features in Release 12.1 T* • *Release Notes* (Release note and caveat documentation for 12.1-based releases and various platforms)	

Obtaining Documentation

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

World Wide Web

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

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 32.