



Text Part Number: 78-6618-05 Rev. B0

# Release Notes for Cisco AS5300 Universal Access Server/Voice Gateway for Cisco IOS Release 12.0 XH

---

**December 1, 2000**

These release notes for the Cisco AS5300 universal access server/Voice Gateway support Cisco IOS Release 12.0 XH, up to and including Release 12.0(4)XH4. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 12.0(4)XH4, see the “Caveats” section on page 22 and *Caveats for Release 12.0 T*. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

## Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 3
- New and Changed Information, page 11
- MIBs, page 14
- Important Notes, page 14
- Caveats, page 22
- Related Documentation, page 23
- Service and Support, page 28
- Cisco Connection Online, page 29
- Documentation CD-ROM, page 29

---

### Corporate Headquarters

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

Copyright © 1999  
Cisco Systems, Inc.  
All rights reserved.

## Introduction

This section contains information about the Cisco AS5300 universal access server/Voice Gateway and Early Deployment (ED) releases for the Cisco AS5300.

---

**Note** The AS5300/Voice Gateway is primarily supported with voice specific IOS releases, namely 12.0(2)XH and 12.0(4)XH. The first planned General Deployment (GD) release for these key Voice over IP (VoIP) features is 12.0(7)T.

---

The Cisco AS5300 is a versatile data communications platform that performs two functions in a single modular chassis depending on the installed feature cards and IOS images:

- Remote Access Server
- Voice Gateway

The remote access server is intended for Internet service providers (ISPs), telecommunications carriers, and other service providers that offer managed Internet connections, as well as medium to large sites that provide both digital and analog access to users on an enterprise network. By terminating both analog and digital calls on the same chassis simultaneously, the access server provides a clear, simple, and easy migration path from analog dial access services to digital dial access services.

The Cisco AS5300/Voice Gateway is a versatile data communications platform that provides the functions of an access server, router, and digital modem(s) in a single modular chassis. The AS5300 includes three feature card slots: one holds a T1/E1/PRI feature card, and the other two support modem feature cards or voice digital signal processor (DSP) feature cards. When equipped with modem cards, the AS5300 serves as a remote access concentrator for dial-up (modem or ISDN) Internet access. When equipped with voice feature cards and Voice IOS, the AS5300/Voice Gateway serves as a voice (VoIP) gateway. By using one slot for modems and the other for voice DSPs, the AS5300 can serve in both capacities. Modem, voice, or fax calls are routed to the appropriate cards/resources via Dialed Number Identification Service (DNIS).

For information on new features and Cisco IOS commands supported by Release 12.0 XH, see the “New and Changed Information” section on page 11 and the “Related Documentation” section on page 23.

## Early Deployment Releases

These release notes describe only Release 12.0 XH for Cisco AS5300 universal access server/Voice Gateway and do not describe features that are available in Release 12.0 or other Release 12.0 Early Deployment (ED) releases. Release 12.0 XH is an Early Deployment (ED) release based on Release 12.0 and announces fixes to software caveats and support for new Cisco hardware.

For information about features in Release 12.0, see *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

For information about features in 12.0 XH ED releases, see Table 1.

For information about features in other platforms, see *Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

**Table 1 Early Deployment Releases for the Cisco AS5300**

ED Release	Maintenance Release	Additional Software Features	VCWare Version	Comments
Release 12.0 XH	(2)	High-Density Voice with DSPM-549	4.04	
	(4)	<ul style="list-style-type: none"> <li>• H.323 Version 2</li> <li>• Settlements for Packet Voice</li> <li>• Debit Card for Packet Telephony</li> <li>• Interactive Voice Response</li> <li>• TDM hairpinning</li> <li>• High-Density Voice with DSPM-549</li> <li>• Single-Density Voice with DSPM-542</li> </ul>	4.09/4.10	
Release 12.0 XH1	(2)	None	4.04	Bug Fixes
Release 12.0 XH1	(4)	<ul style="list-style-type: none"> <li>- Support for AS5300/Voice Gateway serial backhaul cards, for Frame Relay, HDLC, PPP encapsulation of VoIP traffic</li> <li>- Alternate Gatekeeper function</li> <li>- Supports a subset “G.711 &amp; G.729(a) only” codec set.</li> </ul>	4.09/4.10	Bug Fixes

## System Requirements

This section describes the system requirements for Release 12.0(4)XH4:

- Memory Recommendations, page 3
- Hardware Supported, page 4
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4
- VCWare Requirements, page 5
- Modem Code Software, page 5
- Feature Set Tables, page 5

## Memory Recommendations

Table 2 describes the memory recommendations for the Cisco AS5300 platform feature sets supported by Cisco IOS Release 12.0(4)XH4.

**Table 2 Memory Requirements for the Cisco AS5300**

Feature Sets	Image Name	Software Image	Recommended Flash	Recommended DRAM	Runs From
IP Standard	IP Plus	c5300-is-mz	16 MB	64 MB	RAM
Enterprise Standard	Enterprise Plus	c5300-js-mz	16 MB	64 MB	RAM
	Enterprise Plus IPSec 56	c5300-js56i-mz	16 MB	64 MB	RAM

## Hardware Supported

Cisco IOS Release 12.0 XH supports the Cisco AS5300 universal access server/Voice Gateway. For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 11.

**Table 3 Supported Interfaces for the Cisco AS5300**

Interface Cards	Modem Cards
Ethernet RJ-45 (included w/ unit)	MICA modems
Ethernet/Fast Ethernet (RJ-45) (included w/ unit)	Microcom 56K modems
ISDN PRI	
E1-G.703/G.704	
Channelized T1 (4 ports) without serial support	
Channelized T1 (4 ports) with 4 serial ports	
Channelized T1 (8 ports) with 4 serial ports	
Channelized E1 (4 ports) without serial support	
Channelized E1 (4 ports) with 4 serial ports	
Channelized E1 (8 ports) with 4 serial ports	
HMM/48 channel	MICA
HMM/60 channel	MICA
DMM/96 channel	MICA
DMM/120 channel	MICA
48 Channel, TI C549-based VoIP feature card (Uses High Density AS53-VOXD DSP modules)	
60 Channel, TI C549-based VoIP feature card (Uses High Density AS53-VOXD DSP modules)	
24 Channel, TI C542-based VoIP feature card (First generation, uses AS53-6VOX DSP modules)	
48 Channel, TI C542-based VoIP feature card (First generation, uses AS53-6VOX DSP modules)	

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco AS5300, log in to the Cisco AS5300 and enter the **show version EXEC** command:

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) AS5300 Software c5300-js-mz, Version 12.0(4)XH4, RELEASE SOFTWARE
```

## Upgrading to a New Software Release

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99)* on CCO at:

**Service & Support: Product Bulletins: Software**

Under **Cisco IOS 12.0**, click **Cisco IOS Software Release 12.0 T Upgrade (#819: 1/99)**.

## VCWare Requirements

Use the Cisco AS5300 universal access server/Voice Gateway in Cisco IOS Release 12.0(4)XH4 with VCWare Version 4.09/4.10. Previous versions will not work. Please refer to the *Release Notes for Cisco VCWare Version 4.10 for Cisco AS5300/Voice Gateway Feature Cards*.

---

**Note** VCWare/DSPWare is not imbedded in IOS. It is only stored in the Voice Feature Card (VFC) Flash.

---

## Modem Code Software

Modem code is either stored in Flash memory or bundled in the Cisco IOS software image. Bundling eliminates the need to store separate modem code images. When the Cisco AS5300 is powered on, the system software unpacks the modem code and loads the proper code on the modem cards.

---

**Note** You could have received a later version of modem code than the one bundled with the Cisco IOS software. The modem code in Flash memory is mapped to the modems. Unless you fully understand how Cisco IOS software uses modem code, it is important to keep the factory configuration.

---

The modem code release notes are on CCO and the Documentation CD-ROM:

You can reach the release notes on CCO at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Firmware and Portware Information**

You can reach the release notes on the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Firmware and Portware Information**

## Feature Set Tables

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

Release 12.0(4)XH4 supports the same feature sets as Release 12.0(4)T, but Release 12.0(4)XH4 can include new features supported by the Cisco AS5300 universal access server/Voice Gateway.

**Table 4 Feature Sets Supported by Cisco AS5300**

Feature Sets	Image Names	Feature Set Matrix Term	Software Image
IP Standard	IP Plus	Plus	c5300-is-mz
Enterprise Standard	Enterprise Plus	Plus	c5300-js-mz
	Enterprise Plus IPsec 56	IPsec 56	c5300-js56i-mz



**Caution** Cisco IOS images with strong encryption (including, but not limited to 168-bit (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 due to United States government regulations. When applicable, purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

Table 5 lists the features and feature sets supported by the Cisco AS5300 universal access server/Voice Gateway in Cisco IOS Release 12.0 XH 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. For example, (7) means a feature was introduced in 12.0(7)T. If a cell in this column is empty, the feature was included in the initial base release.

**Note** This feature set table only contains a selected list of features. This table is not cumulative—nor does it list all the features in each image.

**Table 5 Selected Features Supported by the Cisco AS5300**

Feature	Software Images by Feature Set			
	In	IP Plus	Enterprise Plus	Enterprise Plus IPSec 56
<b>IBM Support</b>				
APPN High-Performance Routing		No	No	No
APPN MIB Enhancements		No	No	No
APPN over Ethernet LAN Emulation		No	No	No
APPN Scalability Enhancements		No	No	No
Bisync Enhancements: — Bisync 3780 Support — BSC Extended Addressing — Block Serial Tunneling (BSTUN) over Frame Relay		Yes	Yes	Yes
Cisco MultiPath Channel (CMPC)		No	No	No

**Table 5 Selected Features Supported by the Cisco AS5300 (continued)**

Feature	Software Images by Feature Set			
	In	IP Plus	Enterprise Plus	Enterprise Plus IPsec 56
DLSw+ Enhancements: — Backup Peer Extensions for Encapsulation Types — DLSw+ Border Peer Caching — DLSw+ MIB Enhancements — DLSw+ SNA Type of Service — LLC2-to-SDLC Conversion between PU4 Devices — NetBIOS Dial-on-Demand Routing — UDP Unicast Enhancement		Yes	Yes	Yes
FRAS Enhancements: — FRAS Boundary Network Node Enhancement — FRAS Dial Backup over DLSw+ — FRAS DLCI Backup — FRAS Host — FRAS MIB — SRB over Frame Relay		Yes	Yes	Yes
RIF Passthru in DLSw+		Yes	Yes	Yes
TN3270 LU Nailing		No	No	No
TN3270 Server Enhancements		No	No	No
Token Ring LANE		No	No	No
Tunneling of Asynchronous Security Protocols		Yes	Yes	Yes
<b>Internet</b>				
DRP Server Agent		Yes	Yes	Yes
DRP Server Agent Enhancements		Yes	Yes	Yes
<b>IP Routing</b>				
Voice over IP	(3)	Yes	Yes	Yes
Easy IP (Phase 1)		Yes	Yes	Yes
Easy IP (Phase 2) DHCP Server	(1)	Yes	Yes	Yes
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations		No	Yes	Yes
IP Enhanced IGRP Route Authentication	(1)	Yes	Yes	Yes
PIM Version 2	(1)	Yes	Yes	Yes
TCP Enhancements: — TCP Selective Acknowledgment — TCP Timestamp	(1)	Yes	Yes	Yes

## System Requirements

**Table 5 Selected Features Supported by the Cisco AS5300 (continued)**

Feature	Software Images by Feature Set			
	In	IP Plus	Enterprise Plus	Enterprise Plus IPsec 56
<b>LAN Support</b>				
AppleTalk Access List Enhancements		No	Yes	Yes
DECnet Accounting		No	Yes	Yes
IPX Named Access Lists		No	Yes	Yes
IPX SAP-after-RIP		No	Yes	Yes
NLSP Enhancements		No	Yes	Yes
NLSP Multicast Support		No	Yes	Yes
<b>Management</b>				
Cisco Call History MIB Command-Line Interface	(1)	Yes	Yes	Yes
Cisco IOS Internationalization	(1)	Yes	Yes	Yes
Entity MIB, Phase 1	(1)	Yes	Yes	Yes
Process MIB	(3)	Yes	Yes	Yes
ISDN MIB RFC 2127	(1)	Yes	Yes	Yes
SNMPv2C	(1)	Yes	Yes	Yes
SNMPv3	(3)	Yes	Yes	Yes
SNMP Inform Requests		No	Yes	Yes
Time-Based Access Lists	(1)	Yes	Yes	Yes
Virtual Profiles	(1)	Yes	Yes	Yes
VPDN MIB	(1)	Yes	Yes	Yes
VPDN MIB and Syslog Facility		Yes	Yes	Yes
<b>Multimedia</b>				
IP Multicast Load Splitting across Equal-Cost Paths	(1)	Yes	Yes	Yes
IP Multicast over ATM Point-to-Multipoint Virtual Circuits	(1)	No	No	No
PIM Version 2	(1)	Yes	Yes	Yes
IP Multicast over Token Ring LANs	(1)	Yes	Yes	Yes
Stub IP Multicast Routing	(1)	Yes	Yes	Yes
<b>Quality of Service</b>				
CLI String Search	(1)	Yes	Yes	Yes
RTP Header Compression		Yes	Yes	Yes
BERT/TDM	(3)	Yes	Yes	Yes
<b>Security</b>				
Automated Double Authentication		Yes	Yes	Yes
Certificate Authority Interoperability		No	No	Yes
Double Authentication	(1)	Yes	Yes	Yes
Encrypted Kerberized Telnet		No	No	Yes

**Table 5 Selected Features Supported by the Cisco AS5300 (continued)**

Feature	Software Images by Feature Set			
	In	IP Plus	Enterprise Plus	Enterprise Plus IPsec 56
HTTP Security	(1)	Yes	Yes	Yes
Internet Key Exchange Security Protocol		No	No	Yes
IPSec Network Security		No	No	Yes
IPSec with Triple-DES	(2)	No	No	No
MS-CHAP Support		No	Yes	Yes
Named Method Lists for AAA Authentication and Accounting		Yes	Yes	Yes
Per-User Configuration	(1)	Yes	Yes	Yes
Reflexive Access Lists	(1)	Yes	Yes	Yes
TCP Intercept		No	Yes	Yes
Vendor-Proprietary RADIUS Attributes	(1)	Yes	Yes	Yes
Vendor-Proprietary RADIUS —Additional Attributes		Yes	Yes	Yes
<b>Switching</b>				
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs		No	Yes	Yes
CLNS and DECnet Fast Switching over PPP		No	Yes	Yes
DECnet/VINES/XNS over ISL: — Banyan VINES Routing over ISL Virtual LANs — DECnet Routing over ISL Virtual LANs — XNS Routing over ISL Virtual LANs		No	Yes	No
Fast-Switched Policy Routing	(1)	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs		No	Yes	Yes
VIP Distributed Switching Support for IP Encapsulated in ISL		No	No	No
<b>Terminal Services</b>				
Telnet Extensions for Dialout		Yes	Yes	Yes
Virtual Templates for Protocol Translation		No	Yes	Yes
SS7/CCS7 Dial Access Solution (DAS)	(3)	Yes	Yes	Yes
Large Scale Dialout	(3)	Yes	Yes	Yes
<b>WAN Optimization</b>				
ATM MIB Enhancements		No	No	No
PAD Enhancements		No	Yes	Yes
PAD Subaddressing	(1)	Yes	Yes	Yes

## System Requirements

**Table 5 Selected Features Supported by the Cisco AS5300 (continued)**

Feature	Software Images by Feature Set			
	In	IP Plus	Enterprise Plus	Enterprise Plus IPsec 56
<b>WAN Services</b>				
Always On/Dynamic ISDN (AO/DI)		No	Yes	Yes
Bandwidth Allocation Control Protocol	(1)	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes
Dynamic Multiple Encaps for Dial-in over ISDN	(4)	Yes	Yes	Yes
E1 R2 Country Support <sup>1</sup>	(3)	Yes	Yes	Yes
E1 R1 Support for only Taiwan <sup>2</sup>	(3)	Yes	Yes	Yes
Enhanced Local Management Interface (ELMI)		Yes	Yes	Yes
Frame Relay Enhancements	(1)	Yes	Yes	Yes
Frame Relay MIB Extensions	(1)	Yes	Yes	Yes
Frame Relay Router ForeSight	(1)	Yes	Yes	Yes
ISDN Advice of Charge	(1)	Yes	Yes	Yes
ISDN Caller ID Callback	(1)	Yes	Yes	Yes
ISDN LAPB-TA	(4)	Yes	Yes	Yes
ISDN NFAS	(1)	Yes	Yes	Yes
Layer 2 Forwarding—Fast Switching	(1)	Yes	Yes	Yes
Leased-Line ISDN at 128 kbps		No	No	No
Microsoft Point-to-Point Compression (MPPC)		Yes	Yes	Yes
MS Callback	(1)	Yes	Yes	Yes
Modem Management Enhancements	(1)	Yes	Yes	Yes
Multiple ISDN Switch Types		Yes	Yes	Yes
National ISDN Switch Types for BRI and PRI Interfaces (NI2)		Yes	Yes	Yes
PPP over ATM		No	No	No
Stackable Home Gateway		Yes	Yes	Yes
Switched 56K Digital Connections		Yes	Yes	Yes
Telnet Extensions for Dialout		Yes	Yes	Yes
X.25 Enhancements	(1)	Yes	Yes	Yes
X.25 on ISDN	(1)	Yes	Yes	Yes
X.25 Switching between PVCs and SVCs		Yes	Yes	Yes
X.28 Emulation		Yes	Yes	Yes
<b>New</b>				
CNS Client for IOS	(4)	Yes	Yes	Yes
Debit Card for Packet Telephony	(4)XH	Yes	Yes	Yes
H.323 Version 2 Support	(4)XH	Yes	Yes	Yes

**Table 5 Selected Features Supported by the Cisco AS5300 (continued)**

Feature	Software Images by Feature Set			
	In	IP Plus	Enterprise Plus	Enterprise Plus IPsec 56
High Density Voice Support with DSPM-549	(4)XH	Yes	Yes	Yes
Interactive Voice Response (IVR)	(4)XH	Yes	Yes	Yes
Service Provider 1.0 Features	(3)	Yes	Yes	Yes
Open Settlements Protocol (OSP) for IP Telephony	(4)XH	No	No	Yes
Single Density Voice Support with DSPM-542	(4)XH	Yes	Yes	Yes
TDM Hairpinning	(4)	Yes	Yes	Yes

- 1 E1 R2 country support requires specific versions of Mica portware. For details, see the Mica portware release notes, which are available on CCO in the Software Center. Note that country support varies with the portware release level, and the release notes provide a list of countries.
- 2 E1 R1 signaling support for Taiwan requires MICA portware version 2.3.1.0.

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5300 universal access server/Voice Gateway for Release 12.0 XH.

### New Features in Release 12.0(4)XH4

#### H.323 Version 2 Support

H.323 Version 2 Support upgrades Cisco IOS software to comply with the mandatory requirements in the version 2 specification. This upgrade enhances the existing Voice Over IP GateWay, the Multimedia Conference Manager (GateKeeper and Proxy), and the dual tone multifrequency (DTMF) digital relay using H.245.

H.323 Version 2 defines a lightweight registration procedure that requires full registration for initial registration, but uses an abbreviated renewal procedure to update the gatekeeper and minimize overhead. Lightweight registration requires each endpoint to specify a TimeToLive (TTL) value in its Registration Request (RRQ) message.

The H.323 version 2 gateway supports the registration of fully-qualified E.164 numbers with the gatekeeper for phones connected directly to the gateway. Tunneling through H.225 User-to-User Information Element (UUIE) facilitates transparent handling of supplementary services between two endpoints through a VoIP network. This eliminates the need to interpret various supplementary signaling messages in the VoIP gateways.

#### Single Density Voice Support with DSPM-542

This feature implements voice support on the Cisco AS5300 using DSPM-542 digital signal processor (DSP) modules.

The benefits of voice features include:

- Support for Coder Negotiation

- Support for G.723.1 and G.729 voice coders
- Support for 14.4kb/s FAX Relay
- Support for DTMF Digit Relay via RTP
- Support for CODEC negotiation.

This release supports a C542 based VCWare that provides codec and feature interoperability between earlier generation, TI-C542 based AS5300/Voice Gateways, and the latest High Density versions. This release supports parallel C542 based VCWare/DSPWare and C549 based VCWare/DSPWare. However, note that the C542-based VCWare does not increase the number of calls supported on those earlier generation voice feature cards. Increasing support to 96/120 channels requires the latest generation (C549-based, AS53-VOXD based) voice feature cards.

### High Density Voice Support with DSPM-549

This release implements high-density voice support on the Cisco AS5300 by using DSPM-549 digital signal processor (DSP) modules. When equipped with Voice Feature Cards (VFCs) and voice-enabled Cisco IOS software, the AS5300/Voice Gateway supports carrier-class VoIP and FAX over IP services.

High-density voice support increases the voice capacity of a Cisco AS5300 up to 120 channels. This increase in voice support provides the voice density of up to four T1 lines (96 voice or FAX calls) or four E1 lines (120 voice or FAX calls).

A fully configured AS5300/Voice Gateway can support up to two high density (48/60 channel) voice feature cards, and therefore the system supports up to 96/120 simultaneous voice/fax calls (4T1/E1 density).

The benefits of high-density voice features include:

- Low cost per voice channel
- Support for industry-standard voice codecs, including G.711, G.729, and G.723.1
- Support for out-of-band dual-tone modulation frequency (DTMF) transport for coders that do not optimally transport DTMF
- Support for CODEC negotiation
- Configurable voice packet sizes

### Open Settlements Protocol (OSP) for IP Telephony

Internet voice telephony is often used for toll bypass by using an existing data network or the internet instead of PSTN trunking. Calls of this nature require an originating and terminating gateway to be completed. When the originating and terminating voice gateways are owned by 2 different carriers, settlement between these carriers is required. The Settlement for Packet Voice project implements a standardized settlement protocol which can be implemented between different vendors gateways and voice settlement servers.

The Cisco gateway based Settlement protocol interacts between carriers to create a single authentication at initialization. The authentication is the basis for the establishment of a secure communication channel between the Settlement system and the infrastructure component. This channel then allows the following three types of transactions to be handled:

- Call routing---The Settlement system can either accept a gateway endpoint from the requestor or assign one for the requestor.

- Call authorization---Based on the terminating endpoint address, the Settlement system determines whether the requesting gateway is permitted to originate calls for the terminating gateway. If the call is authorized, the Settlement system generates a token that allows the terminating gateway to accept the call.
- Call detail reporting---Each endpoint in a call leg reports when the call stops, along with the usual call details. The Settlement system reconciles the different reports of the calling and called parties and generates billing information. Call details are reported on a call-by-call basis.

---

**Note** Before downloading the software images containing Settlement for Packet Voice, please see the “Encryption Limitation on Open Settlements Protocol (OSP) for IP Telephony” on page 16.

---

### Debit Card Accounting and New RADIUS Attributes for IP Telephony

The Debit Card feature gives the ability to offer calling service with the use of debit accounting to service providers. The Debit Card feature and RADIUS specific enhancements also support Vendor Specific Attributes (VSA). The Debit Card for Packet Telephony on Cisco AS5300 works in tandem with the Cisco Interactive Voice Response (IVR) feature. The IVR voice scripts have been modified to use Tool Command Language (TCL) scripts.

The feature components consist of IVR functionality in Cisco IOS software that works in connection with an integrated third-party billing system. This includes the ability to maintain per-user credit balance information via a RADIUS interface to the Cisco IOS software. When these features are implemented, the billing system and IOS software functions enable a carrier to authorize voice calls and to debit individual user accounts in real time at the edges of a voice over IP network, without requiring external service nodes.

### Interactive Voice Response (IVR)

Cisco is building voice gateways to connect more traditional telephone networks to voice over IP (VoIP) networks. Customers who are installing VoIP networks often need a mechanism at the gateway to present a customized interface to the caller. The IVR feature was first made available to customers with Cisco IOS Release 11.(3)NA2, along with the Service Provider VoIP feature set. IVR with the addition of scripts using Tool Command Language (TCL) are being introduced with Cisco IOS Release 12.0(4)XH4. These TCL IVR scripts are the default scripts that must be used with the IVR application in Cisco IOS Release 12.0(4)XH4 and later releases. 12.0(4)XH4 are compatible with TCLware 1.0.x.

IVR consists of simple voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination. IVR provides the ability to:

- Play customized prompts
- Collect account numbers and PINs
- Collect destination phone numbers
- Perform AAA tasks interacting with a variety of servers

---

**Note** Changes by Cisco in the TCL-based IVR scripts will not require IOS revision updates, rather they will be downloadable via Flash - unlike the previous IVR implementation where scripts were imbedded in IOS. This will add greater flexibility in the release of subsequent scripts.

---

## MIBs

### Current MIBs

If you have an account with CCO, you can find the current list of MIBs supported by Cisco. To reach the *Cisco Network Management Toolkit*, go to CCO, press **Login**, and click to **Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**

### Deprecated and Replacement MIBs

Old Cisco Management Information Bases (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 NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 6:

**Table 6**            **Deprecated and Replacement MIBs**

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In development
OLD-CISCO-DECNET-MIB	
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	
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	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB

### Important Notes

The following sections contain important notes about Cisco IOS Release 12.0(4)XH4 that can apply to the Cisco AS5300 universal access server/Voice Gateway.

### Caveat CSCdr91706 and IOS HTTP Vulnerability

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

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

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

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

You are strongly encouraged to read the complete advisory, which is available at <http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>.

## Frame Relay/HDLC/PPP Encapsulation and Backhaul of VoIP Traffic

12.0(4)XH1 is the first AS5300/Voice Gateway IOS release that supports the use of serial ports or T1/E1 ports for Frame Relay/HDLC/PPP encapsulation and backhaul of VoIP traffic. In other words, all previous IOS releases limited the AS5300/Voice Gateway to passing calls between TDM (T1/E1) ports and Ethernet (10/100 Base T) ports. Therefore, previous releases only supported the use of the earlier generation 4CT1/4CE1 feature cards. Encapsulating and backhauling VoIP traffic onto Frame Relay/HDLC/PPP links required the use of a separate router on the same Ethernet network to encapsulate and pass VoIP traffic into a serial backhaul link (and vice versa).

Release 12.0(4)XH1 supports the use of the AS5300's 4CT1+ Serial port and 4CE1+ Serial port feature cards, previously only supported for AS5300 access server (modem/ISDN termination) applications. It is important to note that there are very defined limits to the use of native encapsulation and backhaul and, in fact it is strongly recommended that dedicated routers (such as Cisco 3600, 7200, 7500) be dedicated to backhaul of VoIP traffic via Frame Relay/HDLC/PPP links. Voice quality is directly affected by latency, and CPU load and as a result, this section highlights some key requirements and limitations associated with use of native FR/HDLC/PPP encapsulation for voice applications using the AS5300/Voice Gateway.

### Summary Highlights of Operational Limits with Backhaul/Encapsulation Enabled:

In order to maintain high performance, including low latency (less than 200 ms round trip delay), high call success rate (99% CSR), and optimal voice quality, Cisco only supports use of native FR/HDLC/PPP encapsulation given the following conditions/caveats:

- VAD and voice compression codecs should be enabled for all calls, i.e. G.729, G.723.1, etc.
- Sustained call rate not to exceed 1 call/sec.
- Limit of two serial ports enabled, each limited to a bandwidth/clock rate to a maximum of 2Mbs serial ports, *or* a limit of one T1/E1 channelized backhaul port used for a total maximum of 1-3MBs bandwidth.
- A 2:1 ratio of TDM calls/bandwidth to encapsulated VoIP bandwidth should be maintained, i.e. 48/60 TDM calls should be encapsulated and carried via a 1 - 2MB/s serial link or into a 1 T1/E1/PRI link. Four T1/E1 of TDM traffic (96/120 calls) should be routed via two 2Mbs serial backhaul links.
- Compressed RTP - IP/UDP/RTP header compression (CRTP) must be disabled
- CRTP should **not** be enabled on the AS5300/Voice Gateway, except for a few very limited cases, specifically where less than 10–24 total calls are to be processed. It is strongly suggested that offload Cisco routers (for example 7200/7500 series) be specifically dedicated for any CRTP requirements. As of this writing, CRTP is processed switched and will create significant load on

the AS5300's main CPU/router resource, and therefore will have negative effect on the AS5300's sustained call success rate, packet latency, and voice quality, if CRTP attempted for more than 10–24 simultaneous calls.

And even in the case of a very low expected call volume, a simulation of the proposed network environment should first be tested to validate achievable call success rate, low latency with CRTP enabled. If native CRTP is deemed necessary, Call rate should be limited to 0.5 calls/sec (1 call every 2 secs).

These caveats are provided for guidance, and there are a wide variety of other backhaul scenarios that may be well supported by the AS5300/Voice Gateway, particularly for low volume applications. When considering other configurations, bear in mind that there are many other VoIP features, processes, and conditions that contribute to system load, including call volume, H.323 RAS transactions, AAA/RADIUS negotiation, SNMP polling, IVR, Open Settlements Protocol transactions, enabling debugs (including “show” commands), etc. This section is provided as a result of extensive characterization testing performed on the AS5300/Voice Gateway while a variety of previously mentioned capabilities were enabled.

## Encryption Limitation on Open Settlements Protocol (OSP) for IP Telephony

Open Settlements Protocol (OSP) for IP Telephony is offered only in crypto images; they are under export controls. All users must be entitled before they can receive 56 or 56i images. You (and your customers) can entitle yourselves by filling out the forms located at the following URL:

<http://www.cisco.com/kobayashi/library/12.0>

- If you are not already entitled for crypto images, the bottom link at the above URL will read:  
“Apply for Cisco IOS Cryptographic Software under export licensing controls”
- If you are entitled, it will read:  
"Download Cisco IOS cryptographic software under export licensing controls"

Once you are entitled, you will be able to see crypto images in the upgrade planner. Also, once you are entitled, you do not have to entitle yourself again, unless you are coming from a different host. You do not have to entitle yourself for every release because entitlement is good for all releases.

## DSPM-542 and DSPM-549 Restrictions

The following restrictions apply to the DSPM-542 and/or DSPM-549.

- You cannot mix DSPM-542s and DSPM-549s on the same voice carrier card and same AS5300/Voice Gateway.

The DSPM-542 uses the AS53-6VOX DSP module with one of the following configurations:

- AS53-T1-24VOX
  - AS53-T1-48VOX
  - AS53-E1-30VOX
  - AS53-E1-60VOX
- If G.711 is used for more than 100 calls (in the case of 4 E1s), then VAD should be enabled to assure optimal performance and high Call Success Rate.

- The AS5300/Voice Gateway is rated to support up to two calls per second on a sustained basis. While the system does not prevent a higher call rate from being processed, the call success rate and CPU utilization can be adversely affected beyond two calls per second. (This call rate assumes a packet size no less than 20ms.)
- The use of the 10ms packet size (the lowest value) is not supported or recommended for high volume applications, or when you have more than 48 T1 or 60 E1 channel requirements.

## Cisco IOS Syslog Failure

Certain versions of Cisco IOS software can fail when they receive invalid User Datagram Protocol (UDP) packets sent to their syslog ports (port 514). At least one commonly used Internet scanning tool generates packets that cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security crackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that needs to be reconfigured by its administrator. Some Cisco IOS devices can hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must visit the device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices indicate that they were “restarted by power-on,” even when that was not the case.

Assume that any potential attacker knows the existence of this problem and the ways to exploit it. An attacker can use tools available to the public on the Internet and does not need to write any software to exploit the vulnerability. Minimal skill is required and no special equipment is required.

Despite Cisco specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this problem.

This vulnerability notice was posted on Cisco’s World Wide Web site:

<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>

This information was also sent to the following e-mail and USENET news recipients:

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [bugtraq@netspace.org](mailto:bugtraq@netspace.org)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [first-info@first.org](mailto:first-info@first.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [nanog@merit.edu](mailto:nanog@merit.edu)

### Affected Devices and Software Versions

Table 7 describes hardware and software that are affected by this problem. Affected versions include Releases 11.3 AA, 11.3 DB, and all 12.0 versions (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 7. Cisco is correcting the problem in certain special releases, will correct it in future maintenance and interim releases, and intends to provide fixes for all affected IOS variants. See Table 7, *Affected and Repaired Software Versions* for details.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the “Workarounds” section on page 19 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running Cisco IOS software, log in to the device and enter the **show version** command. Cisco IOS software will identify itself simply as “IOS” or “Internetwork Operating System Software.” Other Cisco devices do not have the **show version** command and identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, uBR900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the uBR7200), 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Some versions of the Catalyst 2900XL LAN switch
- Cisco DistributedDirector

Affected software versions, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this problem.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines
- MGX (formerly known as the AXIS shelf)
- Host-based software
- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This vulnerability has been assigned Cisco bug ID CSCdk77426.

## Solution

Cisco offers free software updates to correct this vulnerability for all affected customers—regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software versions. Table 7 gives Cisco’s projected fix dates.

Make sure that your hardware has adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release, for example, from 11.2[11]P to 11.2[17]P, but it is often a factor when you upgrade between major releases, for example, from 11.2 P to 11.3 T.

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require you to upgrade to a new major release. Cisco recommends that you carefully plan for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco's World Wide Web site at:

<http://www.cisco.com>

If you have service contracts, you can obtain new software through your regular update channels (generally through Cisco's World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you do not have service contracts, you can upgrade to only obtain the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. You can only upgrade to the software described in one row of Table 7—except when no upgrade within the same row is available in a timely manner.

Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- [tac@cisco.com](mailto:tac@cisco.com)

Give the URL of this notice (<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>) as evidence for a free update. Customers with no contracts must request for free updates through the TAC. For software updates, please do not contact either "psirt@cisco.com" or "security-alert@cisco.com".

## Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to port 514. You can do this by either using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.

If you use an input access list, apply it to all interfaces to which attackers can send datagrams. Interfaces include not only physical LAN and WAN interfaces but also virtual subinterfaces of those physical interfaces—as well as virtual interfaces and interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device's own IP addresses—as well as at any broadcast or multicast addresses on which the Cisco IOS device may be listening. Be sure to block both old-style "all-zeros" broadcasts and new-style "all-ones" broadcasts. It is not necessary to block traffic being forwarded to other hosts—only traffic actually addressed to the Cisco IOS device.

No single input access list works in all configurations. Be sure you know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed—other than as a workaround for this problem:

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0 0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in
```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets can be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device—as well as traffic destined to the device. If the IOS device is expected to forward syslog packets, you will have to filter in detail. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

### Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released Cisco IOS version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) to 12.0(2.3). The first fixed interim version of Release 12.0 mainline software is Release 12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

If you are running Release 12.0(2) and want to fix this problem without risking possible instability presented by installing the 12.0(2.4) interim release, you can upgrade to Release 12.0(2a). Release 12.0(2a) is a “code branch” from the Release 12.0(2) base, which will merge back into the Release 12.0 mainline at Release 12.0(2.4).

Special releases, like 12.0(2a), are one-time spot fixes, and they will not be maintained. Thus, the upgrade path from Release 12.0(2a) is to Release 12.0(3).

---

**Note** All dates within this table are subject to change.

---

Table 7 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix <sup>1</sup>	First Fixed Interim Release <sup>2</sup>	Fixed Maintenance Release <sup>3</sup>
<b>Unaffected Releases</b>				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
<b>Releases Based on 11.3</b>				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999 <sup>4</sup>	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
<b>Releases Based on 12.0</b>				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(3), 1-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S <sup>5</sup> , 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC-12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0 (3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T.
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, uBR7200, uBR900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 18-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999	Merged	Upgrade to 12.0(3)T

- 1 A special fix is a one-time release that provides the most stable immediate upgrade path.
- 2 Interim releases are tested less rigorously than regular maintenance releases; interim releases can contain serious bugs.
- 3 Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.
- 4 All dates in this table are estimates and are subject to change.
- 5 This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release.

## Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

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

All caveats in Release 12.0 and Release 12.0 T are also in Release 12.0 XH.

For information on caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.0*.

For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T*, which lists severity 1 and 2 caveats, and is located on CCO and the Documentation CD-ROM.

---

**Note** If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS BugToolkit: Cisco Bug Navigator II**, or at: [http://www.cisco.com/support/bugtools/Bug\\_root.html](http://www.cisco.com/support/bugtools/Bug_root.html).

---

## Open Caveats—Release 12.0(4)XH4

This section describes possibly unexpected behavior by Release 12.0(4)XH4.

### Miscellaneous

- CSCdp40681

The `socket_recv()` current does not clear the READ event under some error condition. This results in the READ event staying in the process event queue. The process will be waken up to process the even and `socket_recv()` would return the same error causing the process to spin in the loop. The problem was found with CCH323\_CT process in some cases spin with 98% CPU. with socket read error similar to the one below:

```
Nov 22 19:01:45.941: process_get_socket_event(): pid 111, proc_soc 0x6226FD08 fd 3 mask
0x1 sock 0x62779184, sock->next 0x627BA000
*Nov 22 19:01:46.865: process_get_socket_event(): pid 111, proc_soc 0x6226FD08 fd 3
mask 0x1 sock 0x62779184, sock->next 0x627BA000
*Nov 22 19:01:46.865: SOCKET: Read failed: socket 0x62779184 can't read anymore
*Nov 22 19:01:46.865: process_get_socket_event(): pid 111, proc_soc 0x6226FD08 fd 2
mask 0x1 sock 0x627BA000, sock->next 0x6260E8B8
*Nov 22 19:01:46.865: SOCKET: Read failed: socket 0x627BA000 can't read anymore 3d18h:
%SYS-3-MSGLOST: 47995 messages lost because of queue overflow
*Nov 22 19:01:46.941: SOCKET: Read failed: socket 0x62779184 can't read anymore
*Nov 22 19:01:47.869: process_get_socket_event(): pid 111, proc_soc 0x6226FD08 fd 3
mask 0x1 sock 0x62779184, sock->next 0x627BA000
*Nov 22 19:01:47.873: SOCKET: Read failed: socket 0x62779184 can't read anymore
*Nov 22 19:01:47.873: process_get_socket_event(): pid 111, proc_soc 0x6226FD08 fd 2
mask 0x1 sock 0x627BA000, sock->next 0x6260E8B8
*Nov 22 19:01:47.873: SOCKET: Read failed: socket 0x627BA000 can't read anymore
```

## Resolved Caveats—Release 12.0(4)XH4

No resolved caveats have been reported for Release 12.0(4)XH4 at this time.

## Related Documentation

The following sections describe the documentation available for the Cisco AS5300 universal access server/Voice Gateway. These documents consist of hardware and software installation guides, Cisco IOS configuration 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 CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 23
- Platform-Specific Documents, page 24
- Feature Modules, page 24
- Cisco IOS Software Documentation Set, page 25

## Release-Specific Documents

The following documents are specific to Release 12.0 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.0*

On CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on CCO at:

**Technical Documents: Product Bulletins**

- *Caveats for Cisco IOS Release 12.0* and *Caveats for Release 12.0 T*

As a supplement to the caveats listed in “Caveats” in these release notes, see *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T*, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0 XH.

On CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats**

---

**Note** If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS BugToolkit: Cisco Bug Navigator II**, or at: [http://www.cisco.com/support/bugtools/Bug\\_root.html](http://www.cisco.com/support/bugtools/Bug_root.html).

---

## Platform-Specific Documents

These documents are available for the Cisco AS5300 universal access server/Voice Gateway on CCO and the Documentation CD-ROM:

- *Cisco AS5300 Chassis Installation Guide*
- *Cisco AS5300 Module Installation Guide*
- *Cisco AS5300 Software Configuration Guide*
- *Quick Start Guide Cisco AS5300 Universal Access Server Setup and Configuration*
- *Configuring Cisco IOS Software Features*
- *New and Changed Commands for the Cisco AS5300*
- *Dial Case Study*
- Modem information—firmware and portware release notes, configuration notes, command references, FAQs (frequently asked questions)
- *Regulatory Compliance and Safety Information*
- Documentation for spare parts—removal and replacement procedures for modem modules, feature cards, power supply

On CCO at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Access Servers: Cisco AS5300**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300**

## Feature Modules

Feature modules describe new features supported by Release 12.0 XH 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 CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation: New Features in 12.0-Based Limited Lifetime Releases: New Features in Release 12.0 XH**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation: New Features in 12.0-Based Limited Lifetime Releases: New Features in Release 12.0 XH**

## 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, which are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

### Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, 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 CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

You can reach these documents on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References**

You can reach these documents on the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References**

### Release 12.0 Documentation Set

Table 8 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.

---

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

---

You can reach the Cisco IOS documentation set on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0**

You can reach the Cisco IOS documentation set on the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0**

**Table 8 Cisco IOS Software Release 12.0 Documentation Set**

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• <i>Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Configuration Fundamentals Command Reference</i></li> </ul>	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <li>• <i>Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Bridging and IBM Networking Command Reference</i></li> </ul>	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set
<ul style="list-style-type: none"> <li>• <i>Dial Solutions Configuration Guide</i></li> <li>• <i>Dial Solutions Command Reference</i></li> </ul>	X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 1</i></li> <li>• <i>Network Protocols Command Reference, Part 1</i></li> </ul>	IP Overview IP Addressing and Services IP Routing Protocols
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 2</i></li> <li>• <i>Network Protocols Command Reference, Part 2</i></li> </ul>	AppleTalk Novell IPX

**Table 8 Cisco IOS Software Release 12.0 Documentation Set (continued)**

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 3</i></li> <li>• <i>Network Protocols Command Reference, Part 3</i></li> </ul>	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> <li>• <i>Security Configuration Guide</i></li> <li>• <i>Security Command Reference</i></li> </ul>	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> <li>• <i>Wide-Area Networking Configuration Guide</i></li> <li>• <i>Wide-Area Networking Command Reference</i></li> </ul>	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> <li>• <i>Voice, Video, and Home Applications Configuration Guide</i></li> <li>• <i>Voice, Video, and Home Applications Command Reference</i></li> </ul>	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features
<ul style="list-style-type: none"> <li>• <i>Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Quality of Service Solutions Command Reference</i></li> </ul>	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Command Summary</i></li> <li>• <i>Dial Solutions Quick Configuration Guide</i></li> <li>• <i>System Error Messages</i></li> <li>• <i>Debug Command Reference</i></li> </ul>	

---

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

---

## Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in “Service and Support” of *Cisco Information Packet* shipped with your product.

---

**Note** If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

---

For service and support for a product purchased directly from Cisco, use CCO.

## Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

[http://www.cisco.com/kobayashi/technotes/serv\\_tips.shtml](http://www.cisco.com/kobayashi/technotes/serv_tips.shtml)

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: Technical Tips**.

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Lists tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.

- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Lists other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

## Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can reach CCO in the following ways:

- WWW: <http://www.cisco.com>
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact [cco-help@cisco.com](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).

---

**Note** If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or [tac@cisco.com](mailto:tac@cisco.com). To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or [cs-rep@cisco.com](mailto:cs-rep@cisco.com).

---

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which package that ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at [http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml).

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

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 23.

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco *NetWorks* logo, Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQ Logo, iQ Readiness Scorecard, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, WebViewer, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0010R)

Copyright © 1999&2000, Cisco Systems, Inc.  
All rights reserved.