



Text Part Number: 78-6918-03

Release Notes for Cisco AS5300 Series Universal Access Servers for Cisco IOS Release 12.0 XJ

October 4, 1999

These release notes for Cisco AS5300 series universal access servers support Cisco IOS Release 12.0(4)XJ. 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 or related documents.

For a list of the software caveats that apply to Release 12.0(4)XJ, see the *Caveats for Cisco IOS Release 12.0 T* document that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM. For additional information about caveats that apply to Release 12.0(4)XJ, see the "Caveats" section on page 19 of this document.

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 13
- Important Notes, page 13
- Caveats, page 19
- Related Documentation, page 23
- Service and Support, page 28
- Cisco Connection Online, page 29
- Documentation CD-ROM, page 30

Corporate Headquarters

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

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

Introduction

The Cisco AS5300 universal access server 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 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.

For information on new features and Cisco IOS commands supported by Release 12.0(4)XJ, see the “New and Changed Information” section on page 13 and the “Related Documentation” section on page 23.

Early Deployment Releases

These release notes describe only features unique to Release 12.0(4)XJ for Cisco AS5300 series universal access servers and do not describe features that are available in Release 12.0 or other Release 12.0 Early Deployment (ED) releases. Release 12.0(4)XJ is an Early Deployment (ED) release based on Release 12.0 and announces fixes to software caveats and support for new Cisco hardware or software.

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 other 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 Universal Access Server

ED Release	Maintenance Release	Additional Software Features	Additional Hardware Features	Availability
Release 12.0 XH	(4)	<ul style="list-style-type: none"> • High-Density Voice with DSPM-549 • Single Density Voice with DSPM-542 • H.323 Version 2 Support • Settlement For Packet Voice • Debit Card for Packet Telephony • Interactive Voice Response (IVR) 	None	Now
Release 12.0 XD	(2)	None	8 E1/T1 and 240 Modem Upgrade New Feature Boards: <ul style="list-style-type: none"> • Channelized T1 (4 ports) • Channelized E1 (4 ports) • Channelized T1 (8 ports) • Channelized E1 (8 ports) • MICA modems carrier card with DMMs (up to 120 modems each) 	Now

System Requirements

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

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

Memory Requirements

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

Table 2 Memory Requirements for the Cisco AS5300

Feature Sets	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs From
Enterprise Standard Feature Set	Enterprise	c5300-j-mz	8 MB Flash	32 MB DRAM	RAM
	Enterprise Plus	c5300-js-mz	8 MB Flash	32 MB DRAM	RAM
	Enterprise Plus 40	c5300-js40-mz	8 MB Flash	32 MB DRAM	RAM
	Enterprise Plus IPsec 3DES	c5300-jk2s-mz	8 MB Flash	32 MB DRAM	RAM
	Enterprise Plus IPsec 56	c5300-js56i-mz	8 MB Flash	32 MB DRAM	RAM
IP Standard Feature Set	IP	c5300-i-mz	8 MB Flash	32 MB DRAM	RAM
	IP Plus	c5300-is-mz	8 MB Flash	32 MB DRAM	RAM
	IP Plus 40	c5300-is40-mz	8 MB Flash	32 MB DRAM	RAM
	IP Plus IPsec 3DES	c5300-ik2s-mz	8 MB Flash	32 MB DRAM	RAM
	IP Plus IPsec 56	c5300-is56i-mz	8 MB Flash	32 MB DRAM	RAM
IP/IPX/AT/DEC Standard Feature Set	IP/IPX/AT/DEC	c5300-d-mz	8 MB Flash	32 MB DRAM	RAM
	IP/IPX/AT/DEC Plus	c5300-ds-mz	8 MB Flash	32 MB DRAM	RAM

Note A Cisco AS5300 with an 8-port ISDN PRI interface card requires 64 MB of DRAM.

Hardware Supported

Table 3 lists the interfaces and modem cards supported by the Cisco AS5300 series universal access servers using Cisco IOS Release 12.0(4)XJ. For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 13.

Table 3 Supported Interfaces for the Cisco AS5300 Universal Access Servers

Interface Cards	Modem Cards	In ¹
Ethernet RJ-45	MICA modems	
Ethernet/Fast Ethernet (RJ-45)	Microcom 56K modems	
ISDN PRI	None	
E1-G.703/G.704	None	
Channelized T1 (4 ports) without serial support	None	
Channelized T1 (4 ports) with 4 serial ports	None	
Channelized T1 (8 ports) with 4 serial ports	None	
Channelized E1 (4 ports) without serial support	None	
Channelized E1 (4 ports) with 4 serial ports	None	
Channelized E1 (8 ports) with 4 serial ports	None	
Voice over IP (VoIP) feature card (VFC)	None	

¹ The number in the “In” column indicates the Cisco IOS release in which the interface was first introduced. If a cell in this column is empty, the interface was included in the base release.

Determining the Version of Your Software Release

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

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (c5300-js-n), Version 12.0(4)XJ, 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)**.

Modem Code Software

Cisco IOS Release 11.2(2) and later releases, including Release 12.0(4)T, include bundled modem code for the Cisco AS5300, which is the firmware or portware that runs on the Microcom 12-port and MICA 6-port modem cards. Modem code is bundled with the Cisco IOS software image to eliminate the need to store separate modem code. When the Cisco AS5300 access server starts, the Cisco IOS software unpacks the modem code and loads the proper code onto the modem cards.

The **show modem mapping** command lists all versions of modem code running on the modem modules, residing in system Flash, and bundled with Cisco IOS software. Enter the **show modem mapping** command to determine if you need to update your modem code files.

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:

Service & Support: Technical Documents: Cisco Product Documentation: 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)XJ supports the same feature sets as Release 12.0(4)T, but Release 12.0(4)XJ can include new features supported by the Cisco AS5300 series universal access servers.

Table 4 Feature Sets Supported by Cisco AS5300 Series Universal Access Servers

Feature Sets	Image Names	Feature Set Matrix Term	Software Image
IP/IPX/AT/DEC Standard Feature Set	IP/IPX/AT/DEC	Basic	c5300-d-mz
	IP/IPX/AT/DEC Plus	Plus	c5300-ds-mz
IP Standard Feature Set	IP	Basic	c5300-i-mz
	IP IPSec 3DES Plus	Basic, 3DES, Plus	c5300-ik2s-mz
	IP Plus	Plus	c5300-is-mz
	IP Plus 40	Plus 40	c5300-is40-mz
	IP Plus IPSec 56	Plus, IPSec 56	c5300-is56i-mz
Enterprise Standard Feature Set	Enterprise	Basic	c5300-j-mz
	Enterprise IPSec 3DES Plus	Basic, 3DES, Plus	c5300-jk2s-mz
	Enterprise Plus	Basic, Plus	c5300-js-mz
	Enterprise Plus 40	Plus 40	c5300-js40-mz
	Enterprise Plus IPSec 56	Plus, 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.

Table 5 lists the features and feature sets supported by the Cisco AS5300 series universal access servers in Cisco IOS Release 12.0(4)XJ 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, (4) means a feature was introduced in Release 12.0(4)T. If a cell in this column is empty, the feature was included in the initial base release.

Table 5 Selected Features Supported by the Cisco AS5300 Universal Access Server

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 56 3DES ¹	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56	Enterprise Plus IPsec 56 3DES ²
IBM Support													
APPN High-Performance Routing		No	No	No	No	No	No	No	No	No	No	No	No
APPN MIB Enhancements		No	No	No	No	No	No	No	No	No	No	No	No
APPN over Ethernet LAN Emulation		No	No	No	No	No	No	No	No	No	No	No	No
APPN Scalability Enhancements		No	No	No	No	No	No	No	No	No	No	No	No
Bisync Enhancements:		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
— Bisync 3780 Support													
— BSC Extended Addressing													
— Block Serial Tunneling (BSTUN) over Frame Relay													
Cisco MultiPath Channel (CMPC)		No	No	No	No	No	No	No	No	No	No	No	No

Table 5 Selected Features Supported by the Cisco AS5300 Universal Access Server (continued)

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 56 3DES ¹	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56	Enterprise Plus IPsec 56 3DES ²
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		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	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		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
TN3270 LU Nailing		No	No	No	No	No	No	No	No	No	No	No	No
TN3270 Server Enhancements		No	No	No	No	No	No	No	No	No	No	No	No
Token Ring LANE		No	No	No	No	No	No	No	No	No	No	No	No
Tunneling of Asynchronous Security Protocols		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Internet													
DRP Server Agent		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DRP Server Agent Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Selected Features Supported by the Cisco AS5300 Universal Access Server (continued)

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus 56	IP Plus 56 3DES ¹	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus 56	Enterprise Plus 56 3DES ²
IP Routing													
Easy IP (Phase 1)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Easy IP (Phase 2) DHCP Server	(1)	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations		No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Enhanced IGRP Route Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Enhancements: — TCP Selective Acknowledgment — TCP Timestamp		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN Support													
AppleTalk Access List Enhancements		No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DECnet Accounting		No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Named Access Lists		No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX SAP-after-RIP		No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NLSP Enhancements		No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
NLSP Multicast Support		No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management													
Cisco Call History MIB Command-Line Interface		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS Internationalization		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB, Phase 1		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN MIB RFC 2127	(1)	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SNMPv2C		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv3	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Inform Requests		No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Time-Based Access Lists	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Profiles		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Selected Features Supported by the Cisco AS5300 Universal Access Server (continued)

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 56 3DES ¹	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56	Enterprise Plus IPsec 56 3DES ²
VPDN MIB and Syslog Facility		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia													
IP Multicast Load Splitting across Equal-Cost Paths		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast over ATM Point-to-Multipoint Virtual Circuits		No	No	No	No	No	No	No	No	No	No	No	No
PIM Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast over Token Ring LANs		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stub IP Multicast Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quality of Service													
CLI String Search	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RTP Header Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BERT/TDM	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security													
Automated Double Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Certificate Authority Interoperability		No	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes
Double Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encrypted Kerberized Telnet		No	No	No	No	No	No	No	No	No	No	Yes	Yes
HTTP Security		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Internet Key Exchange Security Protocol		No	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes
IPsec Network Security		No	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes
IPsec with Triple-DES	(2)	No	No	No	No	Yes	No	No	No	No	No	No	Yes
MS-CHAP Support		No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Named Method Lists for AAA Authentication and Accounting		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Per-User Configuration		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reflexive Access Lists		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Intercept		No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes

System Requirements

Table 5 Selected Features Supported by the Cisco AS5300 Universal Access Server (continued)

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 56 3DES ¹	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56	Enterprise Plus IPsec 56 3DES ²
Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Vendor-Proprietary RADIUS —Additional Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching													
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs		No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CLNS and DECnet Fast Switching over PPP		No	No	No	No	No	No	No	Yes	Yes	Yes	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	No	No	No	No	No	No	Yes	Yes	No	No	No
Fast-Switched Policy Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs		No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VIP Distributed Switching Support for IP Encapsulated in ISL		No	No	No	No	No	No	No	No	No	No	No	No
Terminal Services													
Telnet Extensions for Dialout		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Templates for Protocol Translation		No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
SS7/CCS7 Dial Access Solution (DAS)	(3)	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes
Large Scale Dialout	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Voice Technologies													
Voice over IP	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Store and Forward Fax	(4) XJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Selected Features Supported by the Cisco AS5300 Universal Access Server (continued)

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 56 3DES ¹	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56	Enterprise Plus IPsec 56 3DES ²
WAN Optimization													
ATM MIB Enhancements		No	No	No	No	No	No	No	No	No	No	No	No
PAD Enhancements		No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
PAD Subaddressing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services													
Always On/Dynamic ISDN (AO/DI)		No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Bandwidth Allocation Control Protocol		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Multiple Encaps for Dial-in over ISDN	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
E1 R2 Country Support ³		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
E1 R1 Support for only Taiwan ⁴		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced Local Management Interface (ELMI)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay MIB Extensions		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Router ForeSight		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Advice of Charge		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Caller ID Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Forwarding—Fast Switching		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Leased-Line ISDN at 128 kbps		No	No	No	No	No	No	No	No	No	No	No	No
ISDN LAPB-TA	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Point-to-Point Compression (MPPC)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Modem Management Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Selected Features Supported by the Cisco AS5300 Universal Access Server (continued)

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 56 3DES ¹	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56	Enterprise Plus IPsec 56 3DES ²
Multiple ISDN Switch Types		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
National ISDN Switch Types for BRI and PRI Interfaces (NI2)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP over ATM		No	No	No	No	No	No	No	No	No	No	No	No
Stackable Home Gateway		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Switched 56K Digital Connections		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Telnet Extensions for Dialout		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 on ISDN		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Switching between PVCs and SVCs		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.28 Emulation		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous													
Service Provider 1.0 Features	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1 This image is not available in Release 12.0(1)T. It is available in Release 12.0(2)T and later 12.0 T releases.
 2 This image is not available in Release 12.0(1)T. It is available in Release 12.0(2)T and later 12.0 T releases.
 3 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.
 4 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 series universal access servers for Release 12.0(4)XJ.

New Features in Release 12.0(4)XJ

The following new software features are supported by the Cisco AS5300 in Cisco IOS Release 12.0(4)XJ.

Store and Forward Fax

The Store and Forward Fax feature enables Cisco AS5300 access servers to transmit and receive faxes across packet-based networks. This feature is an implementation of the RFC 2305 proposed standard from the Internet Engineering Task Force (IETF), which is the same as the T.37 recommendation from the International Telegraph Union (ITU). With this feature, your access server becomes a multiservice platform, supplying both data and fax communication. With Store and Forward Fax, you can:

- Send and receive faxes to and from Group 3 fax devices
- Receive faxes that can be delivered as e-mail attachments
- Create and send a standard e-mail message that can be delivered as a fax to a standard Group 3 fax device

Store and Forward Fax functionality is facilitated through Simple Mail Transfer Protocol (SMTP). Additional functionality is provided in this feature to enable confirmed delivery, capabilities negotiation, and session delivery, using existing SMTP mechanisms such as Extended Simple Mail Transfer Protocol (ESMTP).

Store and Forward Fax functionality is limited by the following hardware dependencies:

- With MICA modems, only FAX Out is supported
- With Microcom modems, both FAX Out and FAX In are supported
- Store and Forward Fax is not supported with voice feature cards (VFCs)

Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that can apply to the CiscoAS5300 series universal access servers.

Cisco IOS Syslog Failure

Certain versions of Cisco IOS software may fail or hang 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, which can cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security attackers. 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 have been observed to hang when attacked instead of failing. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung 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 may indicate that they were “restarted by power-on,” even when that is not the case.

Assume that any potential attacker is likely to know the existence of this vulnerability 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.

Even though Cisco has specifically invited such reports, to date Cisco has received no actual reports of malicious exploitation of this vulnerability.

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
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu

Affected Devices and Software Versions

Table 6 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 6. 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 6, *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 16 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 6 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 6—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)

Important Notes

- +1 408 526 7209 (toll call from anywhere in the world)
- 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.

Important Notes

Table 6 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix ¹	First Fixed Interim Release ²	Fixed Maintenance Release ³
Unaffected Releases				
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
Releases Based on 11.3				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 15-FEB-1999 ⁴	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, 15-FEB-1999
Releases Based on 12.0				
12.0	12.0 Mainline	12.0(2a), 15-FEB-1999	12.0(2.4)	12.0(4), 12-APR-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 15-FEB-1999	12.0(2.4)T	12.0(3)T1, 15-MAR-1999
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(3)T1
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)T1
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, 15-FEB-1999	Merged	Upgrade to 12.0(3)T1
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, 15-FEB-1999	Merged	Upgrade to 12.0(3)T1
12.0(1)XE	Short-life release	12.0(2)XE, 15-FEB-1999	Merged	Upgrade to 12.0(3)T1

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.

Deprecated MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBs are currently migrated 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 7:

Table 7 **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
OLD-CISCO-XNS-MIB	

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(4)XJ.

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 **Service & Support: Online Technical Support: Software Bug Toolkit**, or at <http://www.cisco.com/support/bugtools>.

Open Caveats—Release 12.0(4)XJ

This section describes possibly unexpected behavior by Release 12.0(4)XJ. Unless otherwise noted, these caveats apply to all 12.0 releases up to and including 12.0(4)XJ.

Basic System Services

- CSCdm11467
SegV Exception in peer_list_sum, NTP related
When utilising ntp private mode and control type messages for remote query it is possible to see a router crash or traceback messages .

IBM Connectivity

- CSCdm89688
Removing the **client ip ...** configuration command may cause the router to unexpectedly restart due to a software forced crash.

Interfaces and Bridging

- CSCdk66951
When configuring a new E1 interface on a Port Adapter in a VIP2 based system ALL active E1's will go down.
The E1's don't have to be on the same VIP2
This event has been observed when configuring the following: 1) timeslots on the controller, 2) encapsulation type on the interface.
Currently there is no workaround.
Configuration changes on an E1 controller have to be executed in a maintenance window until this behaviour has been corrected.
- CSCdm61866
Alignment error messages on dot1q over IPX SAP.
*Jul 8 11:50:37: %ALIGN-3-CORRECT: Alignment correction made at 0x605B8E70 reading 0x63E5A6F1 *Jul 8 11:50:37: %ALIGN-3-TRACE: -Traceback= 605B8E70 60095714 60095700 00000000 00000000 00000000 00000000 00000000
However this alignment errors do not effect the connectivity or cause packet loss.
- CSCdm88103
Under certain conditions when IRB is enabled, and appletalk routing only is enabled at the interface level, appletalk routing will not work properly. The main problem is that appletalk broadcasts will not be seen on an interface, so the router will not see neighboring appletalk routers, will not receive routing updates, and will not be able to process appletalk arp packets. Some appletalk packets may actually be bridged to other appletalk routed interfaces in which the bridge-group corresponding with the BVI is defined. In a working scenerio, we should see the following mac address programmed in the output of a "show smf" command: 0900.07ff.ffff 75 RCV Appletalk broadcast In this scenerio, this mac address will be missing. The workaround is to define an additional appletalk cable-range (or address) and apple zone on the bvi.

IP Routing Protocols

- CSCdm84348
After reloading BGP-3-BADROUTEMAP: Bad parameters in the route-map <name> applied for Dampening is logged every minute on 12.0(5)T (not on 12.0(4)T)
A **sho ip bgp dampened-paths** shows % dampening reconfiguration in progress
Doing a **no bgp dampening route-map <name> bgp** makes both issues go away.
- CSCdp05931
BGP will not send the default route to its neighbor when "default-originate" is configured.
- CSCdp09342
In some circumstances, EIGRP will not automatically install and advertise PPP host routes created through dial-in.
Workaround: Perform redistribute connected under EIGRP on the router receiving the dial connections.

Miscellaneous

- CSCdk41197
Customer has to issue the command **clear interface bri X**, where X is the interface number of the 4000 8 port MBRI module that has a layer 2 state of "AWAITING_ESTABLISHMENT" for one Spid and "TEL_ASSIGNED" for the other Spid. The interface that gets stuck in this state is not always the same and it occurs at random times. It is not periodic.
After issuing the **clear interface** command, the layer 2 of the affected port changes to state "MULTIPLE_FRAME_ESTABLISHED" for both Spids. At this time, another ISDN call is able to be placed.
- CSCdk46853
In Release 11.2P and 11.3 when Fast Ethernet subinterfaces are configured for encryption, if the crypto map is only applied to the main interface and the IP address is configured in the subinterface, the packets could be switched in the clear. In Release 12.0, enabling CEF could cause the packets to get dropped.
- CSCdk55110
When tunneling IPX over an ip tunnel, and when using an extended inbound access list for IP on the tunnel interface, the IPX traffic gets blocked by the access list. As a workaround a **permit gre** statement could be added in the extended access-list.
- CSCdk66567
If Token Ring is the endpoint of an encrypted tunnel, extra packets are generated.
Symptoms are a high CPU load (mainly taken by the Crypto Engine) and bogus addresses when enabling the **debug tunnel** command.
The workaround is to use the interface command **tunnel sequence-datagrams** on both endpoints of the tunnel.

- CSCdm59422

The RPM is a NPE-150 based router card capable to sustain traffic up-to 150,000pps. The RPM limits it to 62,000pps because of it's single switch interface design. Under heavy load (data or controlled traffic) the CPU utilization increases which breaks the IPC communication channel between the PXM and RPM card, due to which PXM declares RPM as Failed. Under such condition the provisioning commands will time-out as the PXM assumes that the RPM card is not available, whereas the RPM will continue to pass traffic.

It is recommended for OSPF configurations to limits the number of networks to 20 or less and the MPLS configuration to limit the interface to 100 or less. Doing so will guarantee a sustainable traffic with a low CPU utilization and hence the CPU will be able to service IPC channel traffic.

- CSCdm76565

When the DHCP client makes the DHCP request, the DHCP server returns the request, however, when the return packet is going through the router, the router is putting 0.0.0.0 as the giaddr address when it should put the router's ethernet address.

- CSCdm90364

For the CCBS feature (Call Completion to Busy Subscribers), when PBX sends a PROGRESS message, the voice cut-through does'nt happen. Hence, though CCBS does work, the message played to inform the caller that he/she will get a ringback when the callee is on-hook is not heard by the caller.

- CSCdp02448

If the AS5300 is used according to specification: (maximum of 2 calls/sec/interface), this problem will not occur. If the AS5300 is overloaded for several days (greater than 2 calls/sec/interface), it will run out of memory and a reload will be required.

- CSCdp02586

SNA Switch DLUR may fail LU-LU sessions with 0x08A00002 when uninterpreted PLU names are requested by the dependent LU.

- CSCdp06714

When a virtual access interface is reused via recycling mechanism, it causes memory leaks if it's configured with CEF switching.

The workaround is to turn off CEF switching, **no ip cef**.

Wide-Area Networking

- CSCdm12648

All platforms running MLP may potentially encounter a transient error condition where no links are assigned to a multi-link bundle.

- CSCdm46683

Occasionally a VIP card may not respond to a RSP boards request for a DBUS transaction. When this occurs the RSP will reset the VIP interface and perform a cbus complex restart (to re-allocate MEMD).

We do have a workaround for this problem now. Please refer to the workaround enclosure.

- CSCdm91170

Callback configured on the dialer interface does not work and a work around is to use the ISDN caller command which has the same functionality...

- CSCdp01547
A NAS which is unable to allocate a resource (such as a modem) for an incoming voice call will send an ALERTING to the switch. This can cause the switch to stop from hunting to the next available trunk. There is no workaround.
- CSCdp01840
While making multiple digital calls to an isdn PRI router, excessive CPU utilization will be given to the Dialer software component. These CPU HOGS will cause an rsp4 with 10 busy PRI's to become unusable.
- CSCdp08283
In 12.0(5)T release of IOS software, LANE clients may use an incorrect value as a SDU size in their setup message to the LES. This can prevent the client from coming up. This would happen only if the mtu on the sub-interface is non-default(greater than 1500). The workaround is to use an MTU of 1500 on those sub-interfaces until this problem is resolved in the next release of IOS software.

Resolved Caveats—Release 12.0(4)XJ

There are no caveats as 12.0(4)XJ is the base release.

Related Documentation

The following sections describe the documentation available for the Cisco AS5300 series universal access servers. 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 only available online on CCO and on the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 23
- Platform-Specific Documents, page 24
- Feature Modules, page 25
- 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:

Service & Support: Technical Documents: Cisco Product Documentation: 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:

Service & Support: Technical Documents

- *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS 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(4)XJ.

On CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: 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 **Service & Support: Online Technical Support: Software Bug Toolkit**, or at <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

These documents are available for the Cisco AS5300 series universal access servers on CCO and the Documentation CD-ROM:

- *Cisco AS5300 Chassis Installation Guide*
- *Cisco AS5300 Module Installation Guide*
- *Cisco AS5300 Software Configuration Guide*
- *Cisco AS5300 Quick Start Guide (with Fast Step)*
Cisco AS5300 Universal Access Server Install and Configure
- *Configuring Cisco IOS Software Features*
- *Dial Case Study*
- Modem Information—Firmware/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

You can reach Cisco AS5300 documentation from the CCO home page by clicking on:

Service & Support: Technical Documents: Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300

You can reach Cisco AS5300 documentation on the Documentation CD-ROM by clicking on:

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

Feature Modules

Feature modules describe new features supported by Release 12.0(4)XJ 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:

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation

Cisco IOS Software Documentation Set

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

Service & Support: Technical Documents: Cisco Product Documentation: 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:

Service & Support: Technical Documents: Cisco Product Documentation: 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"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> 	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

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

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> 	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"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP Overview IP Addressing and Services IP Routing Protocols
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Security Configuration Guide</i> • <i>Security Command Reference</i> 	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"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB

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

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Voice, Video, and Home Applications Configuration Guide</i> • <i>Voice, Video, and Home Applications Command Reference</i> 	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"> • <i>Quality of Service Solutions Configuration Guide</i> • <i>Quality of Service Solutions Command Reference</i> 	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"> • <i>Cisco IOS Software Command Summary</i> • <i>Dial Solutions Quick Configuration Guide</i> • <i>System Error Messages</i> • <i>Debug Command Reference</i> 	

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/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>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.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. For additional information, contact 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. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or 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>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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, Any to Any, AtmDirector, CCDA, CCDE, CDDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, GigaStack, IGX, Internet Quotient, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, Secure Script, ServiceWay, SlideCast, SMARTnet, *The Cell*, TrafficDirector, TransPath, ViewRunner, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9909R)

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