



Text Part Number: 78-5209-10 Rev. -B0

Release Notes for Cisco AS5300 Universal Access Servers for Cisco IOS Release 11.3 T

August 2, 1999

These release notes for Cisco AS5300 universal access server support Cisco IOS Release 11.3 T, up to and including Release 11.3(11)T. 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 11.3(11)T, see the *Caveats for Cisco IOS Release 11.3 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.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 11.3* on CCO and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 11
- Important Notes, page 22
- Caveats, page 23
- Documentation Updates, page 23
- Related Documentation, page 24
- Service and Support, page 29
- Cisco Connection Online, page 30
- Documentation CD-ROM, page 31

Corporate Headquarters

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

Copyright © 1998–1999
Cisco Systems, Inc.
All rights reserved.

Introduction

The Cisco AS5300 universal access server is a versatile data communications platform that provides the functions of an access server, router, and digital modems in a single modular chassis. The access server is intended for Internet service providers (ISPs), telecommunications carriers, and other service providers that offer managed Internet connections, and also 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 to digital dial access services.

System Requirements

This section describes the system requirements for Release 11.3 T:

- Memory Requirements, page 2
- Hardware Supported, page 3
- Determining the Version of Your Software Release, page 3
- Upgrading to a New Software Release, page 3
- Microcode and Modem Code Software, page 3
- Feature Set Table, page 5
- Encryption Images Added to Cisco IOS Release 11.3(3)T and Later, page 11

Memory Requirements

Table 1 describes the memory requirements for the Cisco AS5300 feature sets for Release 11.3(11)T.

Table 1 Memory Requirements for the AS5300 Universal Access Server

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs From
IP	c5300-i-mz	8 MB	32 MB	RAM
IP Plus	c5300-is-mz	8 MB	32 MB	RAM
IP Plus 40	c5300-is40-mz	8 MB	32 MB	RAM
IP Plus IPSec 56	c5300-is56i-mz	8 MB	32 MB	RAM
Desktop	c5300-d-mz	8 MB	32 MB	RAM
Desktop Plus	c5300-ds-mz	8 MB	32 MB	RAM
Enterprise	c5300-j-mz	8 MB	32 MB	RAM
Enterprise Plus	c5300-js-mz	8 MB	32 MB	RAM
Enterprise Plus 40	c5300-js40-mz	8 MB	32 MB	RAM
Enterprise Plus IPSec56	c5300-js56i-mz	8 MB	32 MB	RAM

Note If you move to a Cisco IOS Release 12.x, the required DRAM memory will be 64 MB.

Hardware Supported

Cisco IOS Release 11.3(11)T supports the Cisco AS5300 universal access server. For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 11. Table 2 lists the interface and modem cards supported by the Cisco AS5300.

Table 2 Supported Hardware Interfaces for the AS5300 Universal Access Server

Interface Cards	Modem Cards
Ethernet RJ-45	MICA modems
Ethernet/Fast Ethernet (RJ-45)	Microcom 56K modems
ISDN PRI	
E1-G.703/G.704	
Channelized T1 (4 ports) without serial support	
Channelized E1 (4 ports) without serial support	
Voice over IP (VoIP) feature card (VFC)	

Determining the Version of Your Software Release

To determine the version of Cisco IOS software 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 11.3(11)T, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about upgrading to a new software release, see the *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification* product bulletin located on CCO at:

Service & Support: Technical Documents: Product Bulletins: Software

Under **Cisco IOS 11.3**, click **Cisco IOS Software Release 11.3 Upgrade Paths (#703: 12/97)**

This product bulletin does not contain information specific to Cisco IOS Release 11.3 but provides generic upgrade information that may apply to Cisco IOS Release 11.3.

Microcode and Modem Code Software

Table 3 lists the current microcode versions for the Cisco AS5300. Microcode software images are bundled with the system software image—with the exception of the Channel Interface Processor (CIP) microcode (all system software images). Bundling eliminates the need to store separate microcode images. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface processor boards.

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

Table 3 Modem Code and Cisco IOS 11.3 Software Compatibility Matrix

Modem Module	Bundled Modem Code	Cisco IOS 11.3 T Software	Cisco IOS 11.3 AA Software
Microcom modems	Microcom version 3.1.30	Starting with 11.3(2)T, up to 11.3(4)T	11.3(4)AA
Microcom modems	Microcom version 3.3.20	Starting with 11.3(5)T, up to 11.3(7)T	11.3(5)AA and 11.3(6)AA
Microcom modems	Microcom version 5.1.20	11.3(8)T, and later releases	11.3(7)AA, and later releases
MICA modems	MICA portware version 2.0.1.7	Starting with 11.3(2)T, up to 11.3(4)T	11.3(4)AA
MICA modems	MICA portware version 2.3.1.0	Starting with 11.3(5)T, up to 11.3(7)T	11.3(5)AA, up to 11.3(6)AA
MICA modems	MICA portware version 2.6.2.0	11.3(8)T, and later releases	11.3(7)AA, and later releases

Note Only one portware version may be bundled with each Cisco IOS release. At the time when a newer portware version becomes bundled, the older portware version is not bundled anymore.

The **show modemcap** 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 modemcap** command to help you decide if you need to update your modem code files.

The *Cisco IOS Software Upgrade Planner* on CCO contains information about downloading software. To access this document from CCO, click **Login** on the CCO home page to access all information. From the CCO home page, go to the Software Support area, click **Software Center**, then **Cisco IOS Software** or **IOS Upgrade Planner**.

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

- On CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: Access Servers and Access Routers: Firmware and Portware Information: Firmware/Portware Release Notes
- On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300: Modem Information: Firmware/Portware Release Notes

Feature Set Table

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 11.3 T supports the same feature sets as Release 11.3, but Release 11.3 T can include new features supported by the Cisco AS5300 universal access server

Table 4 Feature Sets Supported by the AS5300 Universal Access Server

Feature Set	Software Image Name	Feature Set Matrix Term	Image Name	Platforms
IP Standard	IP	Basic ¹	c5300-i-mz	Cisco AS5300
	IP Plus	Plus ²	c5300-is-mz	Cisco AS5300
	IP Plus 40	Plus, Plus 40 ³	c5300-is40-mz	Cisco AS5300
Desktop	IP Plus IPsec 56	Plus, IPsec 56 ⁴	c5300-is56i-mz	Cisco AS5300
	Desktop	Basic	c5300-d-mz	Cisco AS5300
	Desktop Plus	Plus	c5300-ds-mz	Cisco AS5300
Enterprise	Enterprise	Basic	c5300-j-mz	Cisco AS5300
	Enterprise Plus	Plus	c5300-js-mz	Cisco AS5300
	Enterprise Plus 40	Plus, Plus 40 ⁵	c5300-js40-mz	Cisco AS5300
	Enterprise Plus IPsec56	Plus, IPsec 56 ⁶	c5300-js56i-mz	Cisco AS5300

1 This feature set is offered in the basic feature set.

2 This feature set is offered in the Plus feature set.

3 This feature set is offered in the encryption feature sets, which consist of 40-bit (Plus 40) data encryption feature sets.

4 This feature set is offered in the encryption feature sets, which consist of IPsec 56-bit (Plus IPsec 56) data encryption feature sets.

5 This feature set is offered in the encryption feature sets, which consist of 40-bit (Plus 40) data encryption feature sets.

6 This feature set is offered in the encryption feature sets, which consist of IPsec 56-bit (Plus IPsec 56) data encryption feature sets.

Table 5 lists the features and feature sets supported by the Cisco AS5300 universal access server in Cisco IOS Release 11.3 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, (11) means a feature was introduced in 11.3(11)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.

System Requirements

Table 5 Selected Features and Feature Sets for the Cisco AS5300

Feature	In	Feature Set									
		IP	IP Plus	IP Plus 40 ¹	IP Plus IPsec 56 ²	Desk top	Desk top Plus	Enter prise	Enter prise Plus	Enter prise Plus 40 ³	Enter prise Plus IPsec 56 ⁴
IBM Support											
APPN High-Performance Routing		No	No	No	No	No	No	No	No	No	No
APPN MIB Enhancements		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
APPN Scalability Enhancements		No	No	No	No	No	No	No	No	No	No
Bisync Enhancements: — Bisync 3780 Support — BSC Extended Addressing — Block Serial Tunneling (BSTUN) over Frame Relay		No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Cisco MultiPath Channel (CMPC)		No	No	No	No	No	No	No	No	No	No
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	No	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	No	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+	(3)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
SRB over FDDI on Cisco 4000-M, 4500-M, and 4700-M Routers		No	No	No	No	No	No	No	No	No	No

Table 5 Selected Features and Feature Sets for the Cisco AS5300 (continued)

Feature	Feature Set										
	In	IP	IP Plus	IP Plus 40 ¹	IP Plus IPsec 56 ²	Desk top	Desk top Plus	Enterprise	Enterprise Plus	Enterprise Plus 40 ³	Enterprise Plus IPsec 56 ⁴
TN3270 LU Nailing		No	No	No	No	No	No	No	No	No	No
TN3270 Server Enhancements		No	No	No	No	No	No	No	No	No	No
Token Ring LANE		No	No	No	No	No	No	No	No	No	No
Tunneling of Asynchronous Security Protocols		No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Internet											
DRP Server Agent		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DRP Server Agent Enhancements	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Routing											
Easy IP (Phase 1)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
IP Enhanced IGRP Route Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM Version 2		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
LAN Support											
AppleTalk Access List Enhancements		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
DECnet Accounting		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
IPX Named Access Lists		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
IPX SAP-after-RIP		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
NLSP Enhancements		No	No	No	No	No	No	Yes	Yes	Yes	Yes
NLSP Multicast Support		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Management											
Cisco Call History MIB Command Line Interface		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS Internationalization		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB, Phase 1		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv2C		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Inform Requests	(1)	No	No	No	No	No	No	Yes	Yes	Yes	Yes

Table 5 Selected Features and Feature Sets for the Cisco AS5300 (continued)

Feature	Feature Set										Enterprise Plus IPsec 56 ⁴
	In	IP	IP Plus	IP Plus 40 ¹	IP Plus IPsec 56 ²	Desk top	Desk top Plus	Enterprise	Enterprise Plus	Enterprise Plus 40 ³	
Virtual Profiles		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB	(2)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
VPDN MIB and Syslog Facility	(3)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Multimedia											
IP Multicast Load Splitting across Equal-Cost Paths		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
PIM Version 2	(2)	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
Stub IP Multicast Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quality of Service											
RTP Header Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security											
Automated Double Authentication	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Certificate Authority Interoperability	(3)	No	No	No	Yes	No	No	No	No	No	Yes
Double Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encrypted Kerberized Telnet		No	No	No	No	No	No	No	No	No	Yes
HTTP Security		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Internet Key Exchange Security Protocol	(3)	No	No	No	Yes	No	No	No	No	No	Yes
IPsec Network Security	(3)	No	No	No	Yes	No	No	No	No	No	Yes
Message Banners for AAA Authentication	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS-CHAP Support	(3)	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Named Method Lists for AAA Authentication and Accounting	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Per-User Configuration		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reflexive Access Lists		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Intercept		No	No	No	No	No	No	Yes	Yes	Yes	Yes
Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Vendor-Proprietary RADIUS -Additional Attributes	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Selected Features and Feature Sets for the Cisco AS5300 (continued)

Feature	Feature Set										
	In	IP	IP Plus	IP Plus 40 ¹	IP Plus IPsec 56 ²	Desk top	Desk top Plus	Enter prise	Enter prise Plus	Enter prise Plus 40 ³	Enter prise Plus IPsec 56 ⁴
Switching											
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
CLNS and DECnet Fast Switching over PPP		No	No	No	No	No	No	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	Yes	Yes	No	No
Fast-Switched Policy Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs		No	No	No	No	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
Terminal Services											
Telnet Extensions for Dialout		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Templates for Protocol Translation		No	No	No	No	No	No	Yes	Yes	Yes	Yes
WAN Optimization											
ATM MIB Enhancements		No	No	No	No	No	No	No	No	No	No
PAD Enhancements		No	No	No	No	No	No	Yes	Yes	Yes	Yes
PAD Subaddressing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services											
Always On/Dynamic ISDN (AO/DI)	(3)	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Bandwidth Allocation Control Protocol		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
E1 R2 Country Support ⁵	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
E1 R1 Support for only Taiwan ⁶	(3)	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
Frame Relay Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay MIB Extensions		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Selected Features and Feature Sets for the Cisco AS5300 (continued)

Feature	Feature Set										
	In	IP	IP Plus	IP Plus 40 ¹	IP Plus IPsec 56 ²	Desk top	Desk top Plus	Enterprise	Enterprise Plus	Enterprise Plus 40 ³	Enterprise Plus IPsec 56 ⁴
Frame Relay Router ForeSight		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Advice of Charge		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Caller ID Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Forwarding—Fast Switching		No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Leased-Line ISDN at 128 kbps		No	No	No	No	No	No	No	No	No	No
Microsoft Point-to-Point Compression (MPPC)	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Modem Management Enhancements	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
National ISDN Switch Types for BRI and PRI Interfaces (NI2)	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP over ATM		No	No	No	No	No	No	No	No	No	No
Stackable Home Gateway	(3)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Switched 56K Digital Connections	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Telnet Extensions for Dialout	(2)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
X.25 Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 on ISDN		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
X.28 Emulation		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1 This image is not available in Releases 11.3(1)T and 11.3(2)T. It is available in Release 11.3(3)T and later 11.3 T releases.
 2 This image is not available in Releases 11.3(1)T and 11.3(2)T. It is available in Release 11.3(3)T and later 11.3 T releases.
 3 This image is not available in Releases 11.3(1)T and 11.3(2)T. It is available in Release 11.3(3)T and later 11.3 T releases.
 4 This image is not available in Releases 11.3(1)T and 11.3(2)T. It is available in Release 11.3(3)T and later 11.3 T releases.
 5 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.
 6 E1 R1 signaling support for Taiwan requires MICA portware version 2.3.1.0.

Encryption Images Added to Cisco IOS Release 11.3(3)T and Later

Table 6 lists the encryption images available in Cisco IOS Release 11.3(3)T and later 11.3 T releases; they are not available in Releases 11.3(1)T and 11.3(2)T.

Table 6 Encryption Images Supported by the AS5300 Universal Access Server

Image Name	Feature Set Name	Description
c5300-is40-mz	IP Plus 40	New image based on the IP Plus image, with 40-bit encryption.
c5300-is56i-mz	IP Plus IPsec 56	New image based on the IP Plus image, with 56-bit encryption and additional features including Certificate Authority Interoperability and Internet Key Exchange Security Protocol.
c5300-js40-mz	Enterprise Plus 40	New image based on the Enterprise Plus image, with 40-bit encryption.
c5300-js56i-mz	Enterprise Plus IPsec 56	New image based on the Enterprise Plus image, with 56-bit encryption, IP Security, and additional features including Certificate Authority Interoperability and Internet Key Exchange Security Protocol.



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.

New and Changed Information

This section lists new features available for the Cisco AS5300 for Release 11.3 T.

No New Features in Cisco IOS Release 11.3(9)T through 11.3(11)T

No new software features were introduced in Cisco IOS Release 11.3(9)T through 11.3(11)T for the Cisco AS5300.

No New Features in Cisco IOS Release 11.3(8)T

No new software features were introduced in Cisco IOS Release 11.3(8)T for the Cisco AS5300; however, the modem code that is bundled with the Cisco IOS software was upgraded as follows to support V.90:

- Microcom version 3.3.20 replaced by Microcom version 5.0.40
- MICA portware version 2.3.1.0 replaced by MICA portware version 2.5.1.0

No New Features in Cisco IOS Release 11.3(7)T

No new software features were introduced in Cisco IOS Release 11.3(7)T for the Cisco AS5300.

New Features in Cisco IOS Release 11.3(6)T

The following three new cas-custom commands are available for the Cisco AS5300 in Cisco IOS Release 11.3(6)T:

- **debounce-time**

- This command validates ABCD bit changes. If an ABCD bit value changes to shorter than the debounce time, then the bit changes are invalid. Currently this command is supported for E1 only. This value adds up to all timers. For example, in order to achieve 40 seizure-ack-time, you need to configure the debounce time to 20, and seizure-ack-time to 20.

- Default value is 40.

- Example:

```
as5300_1(config-ctrl-cas)# debounce-time?  
<16-40> Debounce Time in Milliseconds
```

- **seizure-ack-time**

- This command specifies the time difference between the seizure signal and seizure acknowledgment signal; that is, how long the router waits before transmitting a seizure acknowledgment signal after receiving a seizure signal. This is specific to R2 signaling only.

- Default value is 100.

- Example:

```
as5300_1(config-ctrl-cas)# seizure-ack-time?  
<2-100> Seizure to Acknowledge time in Milliseconds
```

- **release-guard-time**

- This command specifies the time difference between receive idle signal and transmit idle signal after the router receives clear forward (idle) signal. This disconnect request is for successful calls only. This is specific to R2 signaling only.

- The default value is 2000.

- Example:

```
as5300_1(config-ctrl-cas)# release-guard-time?  
<1-2000> Release Guard Time in Milliseconds
```

No New Features in Cisco IOS Release 11.3(5)T

No new software features were introduced in Cisco IOS Release 11.3(5)T for the Cisco AS5300.

New Features in Cisco IOS Release 11.3(4)T

The following new software features in Cisco IOS Release 11.3(4)T are available for the Cisco AS5300. For easy online access, feature modules that describe these new features are linked.

IP Type of Service and Precedence for GRE Tunnels

Prior to this feature, at generic route encapsulation-based tunnel endpoints, the type of service (ToS) bits (including precedence bits) were not copied to the tunnel or GRE IP header that encapsulates the inner packet. Instead, those bits were set to zero. This was not a problem unless the intermediate routers between two tunnel endpoints honored ToS or precedence bits, in which case those settings were ignored.

With the advent of virtual private network (VPN) and quality of service (QoS) applications, it is desirable to copy the ToS bits when the router encapsulates the packets using GRE. Thus, intermediate routers between tunnel endpoints can take advantage of the QoS features such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

Message Banners for AAA Authentication

The authentication, authorization, and accounting (AAA) suite of security services now supports the use of configurable, personalized login and failed-login banners. This feature lets you change the default message for login and failed-login. You can configure message banners that will be displayed when a user logs in to the system to be authenticated using AAA and when authentication, for whatever reason, fails.

New Features in Cisco IOS Release 11.3(3)T

The following new software features in Cisco IOS Release 11.3(3)T are available for the Cisco AS5300.

Always On/Dynamic ISDN

Always On/Dynamic ISDN (AO/DI) is an on-demand service that optimizes the use of an existing Integrated Services Digital Network (ISDN) signaling channel (D channel) to transport X.25 traffic. The X.25 D-channel call is placed from the subscriber to the packet data service provider. Multilink and TCP/IP Protocols are encapsulated within the X.25 logical circuit carried by the D channel. The bearer channels (B channels) use the Multilink Protocol without the standard Q.922 and X.25 encapsulations and invoke additional bandwidth as needed. AODI takes full advantage of existing packet handlers at the central office by using an existing D channel to transport the X.25 traffic. The link associated with the X.25 D-channel packet connection is used as the primary link of the Multilink Protocol. The D channel is a connectionless, packet-oriented link between the Customer Premises Equipment (CPE) and the central office. Because the D channel is always available, it is possible to offer *always available* services. On-demand functionality is achieved by using the B channels to temporarily boost data throughput and then disconnecting the B channels after use.

Multiple ISDN Switch Types

The Multiple ISDN Switch Types feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per-interface basis, thus extending the existing global **isdn switch-type** command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

The **isdn tei** command is also extended to the interface level. Terminal endpoint negotiation (TEI) determines when Layer 2 is activated (power up or first call).

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces introduce changes to ISDN switch types for Primary Rate Interfaces (PRIs) and Basic Rate Interfaces (BRIs) as follows:

- Adds a new switch type for PRI interfaces (**isdn switch-type primary-ni**).
- Changes the BRI basic-ni1 switch type to basic-ni (**isdn switch-type basic-ni**).
- Removes the ISDN vn2 switch type (**isdn switch-type vn2**) used in France. The existing vn3 switch type (**isdn switch-type vn3**) supports French vn2 switches.

- Removes the ISDN basic-nwnet3 switch type (**isdn switch-type basic-nwnet3**) used in Norway. The basic-net3 switch type (**isdn switch-type basic-net3**) supports Norway NET3 switches.
- Removes the ISDN basic-nznet3 switch type (**isdn switch-type basic-nznet3**) used by New Zealand NET3 switches. The ISDN basic-net3 switch type (**isdn switch-type basic-net3**) supports New Zealand NET3 switches.
- Adds the ability to configure outgoing PRI B-channel selection for the T1 controller in ascending order (channel 1 to channel 23) or descending order (channel 23 to channel 1). Previously, the router selected a B channel for outgoing calls from the highest free channel in descending order. The E1 controller channel selection for ascending order is channel 1 to 31, and 31 to 1 for descending order.

Note The command parser will still accept the following switch types: basic-nwnet3, vn2, and basic-net3; however, when viewing the NVRAM configuration using either the **show running configuration** or **write terminal** command, the basic-net3 or vn3 switch types, respectively, are displayed.

Microsoft Point-to-Point Compression

Microsoft Point-to-Point Compression (MPPC) is a scheme used to compress Point-to-Point Protocol (PPP) packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize processor and bandwidth utilization in order to support multiple simultaneous connections. The MPPC algorithm uses a Lempel-Ziv (LZ) based algorithm with a continuous history buffer called a dictionary.

VPDN MIB and Syslog Facility

The Virtual Private Dial-Up Network (VPDN) Management Information Base (MIB) feature is intended to support all tables and objects defined in “Cisco VPDN Management MIB” for the user sessions of the VPDN features. There are a number of commands that provide information and statistics through the command-line interface (CLI) but not Simple Network Management Protocol (SNMP); the Cisco VPDN MIB has been created to satisfy the need to provide information and statistics through SNMP.

RIF Passthru in DLSw+

By default, DLSw+ terminates the routing information field (RIF) for Token Ring, terminates the LLC for all media types, and forwards only data across a WAN with DLSw+ and TCP/IP headers. The RIF is a field in source-route bridged frames that indicates the SRB path the frame should take when traversing a Token Ring network. In the case of an explorer packet, the RIF is a field of the source-route bridged frame that indicates the SRB path that the SRB explorer has traversed so far. The RIF is limited to 7 hop counts by the IBM standards. Because DLSw+ terminates the RIF at the virtual ring, the network’s scalability increases because the hop count of the packet starts over, and the packet can traverse 7 additional hops. Also, RIF termination simplifies network design because ring numbers no longer have to be unique throughout an entire enterprise.

However, some environments do not function properly if the RIF is terminated. For that reason, DLSw+ now supports the RIF-passthru feature, in which the entire source-route bridged path appears in the RIF.

Certificate Authority Interoperability

Certificate Authority (CA) interoperability is provided in support of the IP Security (IPSec) standard. CA interoperability permits devices running Cisco IOS software and CA devices to communicate so that devices running Cisco IOS software can obtain and use digital certificates from the CA. Although IPSec can be implemented in your network without the use of a CA, using a CA provides manageability and scalability for IPSec.

For background and configuration information for IPSec, see the *IPSec Network Security* feature documentation.

IPSec Network Security

IPSec is a security feature that provides robust authentication and encryption of IP packets. IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF).

IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”) such as Cisco routers. IPSec enables applications such as virtual private networks (VPNs), extranets, and remote user access.

IPSec provides the following network security services:

- Privacy—IPSec can encrypt packets before transmitting them across a network.
- Integrity—IPSec authenticates packets at the destination peer to ensure that the data has not been altered during transmission.
- Authentication—Peers authenticate the source of all IPSec-protected packets.
- Anti-replay protection—Prevents capture and replay of packets; helps protect against denial-of-service attacks.

IPSec services are similar to those provided by Cisco Encryption Technology, a proprietary security solution introduced in Cisco IOS Software Release 11.2. (The IPSec standard was not yet available at Release 11.2.) However, IPSec provides a more robust security solution, and is standards-based.

Internet Key Exchange Security Protocol

ISAKMP/Oakley is a key management protocol used in conjunction with the IPSec standard. IPSec can be configured without ISAKMP/Oakley, but ISAKMP/Oakley enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

ISAKMP/Oakley is a hybrid protocol that implements the Oakley key exchange inside the ISAKMP framework.

Automated Double Authentication

The automated double authentication feature enhances the existing double authentication feature.

Previously, with the existing double authentication feature, a second level of user authentication was achieved when the user established a Telnet connection to the network access server or router and entered a username and password. Now, with automated double authentication, the user does not have to Telnet anywhere, but instead responds to a dialog box that requests a username and password or PIN.

(For information about the existing double authentication feature, refer to the “Configuring Authentication” chapter of the Cisco IOS Release 11.3 *Security Configuration Guide*.)

Named Method Lists for AAA Authorization and Accounting

In earlier Cisco IOS releases, only named authentication method lists were supported under Cisco's authentication, authorization, and accounting (AAA) network security services. With Cisco IOS Release 11.3(3)T, AAA has been extended to support both authorization and accounting named method lists. Named method lists for authorization and accounting function the same way as those for authentication; they allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis.

MS-CHAP Support

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server (NAS).

MS-CHAP differs from the standard CHAP as follows:

- MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.
- The MS-CHAP Response packet is in a format designed to be compatible with Microsoft Windows NT 3.5 and 3.51, Microsoft Windows 95, and Microsoft LAN Manager 2.x. This format does not require the authenticator to store a clear or reversibly encrypted password.
- MS-CHAP provides an authenticator-controlled authentication retry mechanism.
- MS-CHAP provides an authenticator-controlled change password mechanism.
- MS-CHAP defines a set a "reason-for failure" codes returned in the Failure packet message field.

Depending on the security protocols you have implemented, PPP authentication using MS-CHAP can be used with or without authentication, authorization and accounting (AAA) security services. If you have enabled AAA, PPP authentication using MS-CHAP can be used in conjunction with both TACACS+ and RADIUS.

Additional Vendor-Proprietary RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) is an access server authentication, authorization, and accounting protocol originally developed by Lucent Technologies Remote Access Business Unit (formerly Livingston, Inc.). Although an Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. In this release, Cisco IOS software introduces support for additional vendor-proprietary RADIUS attributes. Users who have implemented security solutions using a vendor-proprietary implementation of RADIUS can now integrate Cisco access servers into their networks more easily.

R1 Modified Signaling

Note R1 modified signaling for Taiwan requires MICA portware version 2.3.1.0.

Enabling R1 modified signaling allows a Cisco AS5200 or Cisco AS5300 universal access server to talk to central office trunks that also use R1 modified signaling. R1 Signaling is an international signaling standard that is common to channelized T1/E1 networks; however, this feature is only available in Taiwan. You can configure a channelized T1/E1 interface to support different types of R1 modified signaling, which is used in older analog telephone networks.

Note This type of signaling is not the same as ITU R1 signaling; it is R1 signaling modified specifically for Taiwan.

New Features in Cisco IOS Release 11.3(2)T

The following new software features in Cisco IOS Release 11.3(2)T are available for the Cisco AS5300.

Support for Cisco AS5300

This is the first Cisco IOS 11.3 T release to include support for the Cisco AS5300.

Dialer Watch

Dialer Watch is a backup feature that integrates dial backup with routing capabilities. Prior dial backup implementations used the following conditions to trigger backup:

- Interesting packets were defined at central and remote routers using dial-on-demand routing (DDR).
- Connection loss occurred on a primary interface using a backup interface with floating static routes.
- Traffic thresholds were exceeded using a dialer load threshold.

Prior backup implementations might not have supplied optimum performance on some networks, such as those using Frame Relay multipoint subinterfaces or Frame Relay connections that do not support end-to-end LMI (Local Management Interface).

Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Dialer Watch uses the convergence times and characteristics of dynamic routing protocols. Integrating backup and routing features enables Dialer Watch to monitor every deleted route. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted. Monitoring the watched routes is done in the following sequence:

- 1 Whenever a watched route is deleted, Dialer Watch checks to see if there is at least one valid route for any of the watched IP addresses defined.
- 2 If there is no valid route, the primary link is considered down and unusable.
- 3 If there is a valid route for at least one of the defined watched IP addresses, and if the route is pointing to an interface other than the backup interface configured for Dialer Watch, the primary link is considered up.

- 4 In the event that the primary link goes down, Dialer Watch is immediately notified by the routing protocol and the secondary link is brought up.
- 5 When the secondary link is up, at the expiration of each idle timeout, the primary link is rechecked.
- 6 If the primary link remains down, the idle timer is indefinitely reset.
- 7 If the primary link is up, the secondary backup link is disconnected. Additionally, a disable timer can be set to create a delay for the secondary link to disconnect after the primary link is reestablished.

MS Callback

The MS Callback feature provides client-server callback services for Microsoft Windows 95 and Microsoft Windows NT clients. MS Callback supports the Microsoft Callback Control Protocol (MSCB). MSCB is a Microsoft proprietary protocol used by Windows 95 and Windows NT clients. MS Callback supports negotiated PPP Link Control Protocol (LCP) extensions initiated and agreed to by the Microsoft client. MS Callback is added to existing PPP Callback functionality. Therefore, if you configure your Cisco AS5300 to perform PPP Callback using Cisco IOS Release 11.3(2)T or later, MS Callback is automatically available.

MS Callback supports AAA security models using a local database or AAA server.

MSCB uses LCP callback options with suboption type 6. The Cisco MS Callback feature supports clients with a user-specified callback number and server-specified (preconfigured) callback number.

MS Callback does not affect non-Microsoft machines that implement standard PPP LCP extensions as described in RFC 1570. In this scenario, MS Callback is transparent.

PIM Version 2

Protocol-Independent Multicast (PIM) Version 2 includes the following improvements over PIM Version 1:

- A single, active rendezvous point (RP) exists per multicast group, with multiple backup RPs. This compares to multiple active RPs for the same group in PIM Version 1.
- A bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism. Thus, routers dynamically learn the group-to-RP mappings.
- Sparse mode and dense mode are properties of a group, as opposed to an interface. Cisco strongly recommends sparse-dense mode as opposed to either sparse mode or dense mode only.
- PIM Join and Prune messages have more flexible encodings for multiple address families.
- A more flexible Hello packet format replaces the Query packet to encode current and future capability options.
- Register messages to an RP indicate whether they were sent by a border router or a designated router.
- PIM packets are no longer inside IGMP (Internet Group Management Protocol) packets; they are standalone packets.

PIM Version 1, together with the Auto-RP feature, can perform the same tasks as the PIM Version 2 BSR. However, Auto-RP is a standalone protocol, separate from PIM Version 1, and is Cisco proprietary. PIM Version 2 is a standards track protocol in the Internet Engineering Task Force (IETF).

Cisco's PIM Version 2 implementation allows good interoperability and transition between Version 1 and Version 2. You can upgrade to PIM Version 2 incrementally. PIM Versions 1 and 2 can be configured on different routers within one network. Internally, all routers on a shared media network must run the same PIM version. Therefore, if a PIM Version 2 router detects a PIM Version 1 router, the Version 2 router downgrades itself to Version 1 until all Version 1 routers have been shut down or upgraded.

PIM uses the BSR to discover and announce RP-set information for each group prefix to all the routers in a PIM domain. This is the same function accomplished by Auto-RP, but the BSR is part of the PIM Version 2 specification. The BSR mechanism interoperates with Auto-RP.

To avoid a single point of failure, you can configure several candidate BSRs in a PIM domain. A BSR is elected among the candidate BSRs automatically; they use bootstrap messages to discover which BSR has the highest priority. This router then announces to all PIM routers in the PIM domain that it is the BSR.

Routers that are configured as candidate RPs then unicast to the BSR the group range for which they are responsible. The BSR includes this information in its bootstrap messages and disseminates it to all PIM routers in the domain. Based on this information, all routers will be able to map multicast groups to specific RPs. As long as a router is receiving the bootstrap message, it has a current RP map.

DRP Server Agent Enhancements

The Director Response Protocol (DRP) Server Agent enhancements are as follows:

- Distributed Director can use Border Gateway Protocol (BGP) Multi-Exit Discriminators in traffic redirection decisions.
- The DRP Server can measure client-to-server link latency (roundtrip time) for use in traffic redirection decisions.

VPDN MIB

For VPDN (Virtual Private Dial-Up Network) sessions, information on active tunnels and sessions are retrievable through Simple Network Management Protocol (SNMP) from the VPDN Management Information Base (MIB). The VPDN MIB feature is intended to support all the tables and objects defined in "Cisco VPDN Management MIB" for the user sessions of the VPDN features. There are a number of commands that provide information and statistics through the command-line interface (CLI) but not SNMP; the Cisco VPDN MIB has been created to satisfy the need to provide information and statistics through SNMP.

Switched 56K Digital Connections over Channelized T1 and Channel Associated Signaling

Internet service providers can provide switched 56-kbps access to their customers using a Cisco AS5300 and an ISDN PRI or a CT1 RBS connection:

- Using ISDN PRI, the access server uses the bearer capability to determine the type of service.
- Using a CT1 RBS connection, the DS0s of the access server can be configured to provide either modem or 56-kbps data service.

The dial-in user can access a 56-kbps data connection to the ISP using either an ISDN BRI connection or a 2- or 4-wire switched 56-kbps connection. The telco to which the access server connects must configure its switches to route 56-kbps data calls and voice (modem) calls to the appropriate DS0 (digital signal level 0). Similarly, an enterprise can provide switched 56-kbps digital dial-in services to its full-time telecommuters or small remote offices using ISDN PRI or a CT1 RBS connection.

E1 R2 Country Support

New country support for E1 R2 signaling and modem management enhancements is added to Cisco IOS Release 11.3(2)T and later for the Cisco AS5300 access server. Only MICA modems support the R2 functionality.

Cisco Systems' R2 signaling default is ITU, which supports the following countries: Denmark, Finland, Germany, Russia (ITU variant), Hong Kong (ITU variant), and South Africa (ITU variant). The "ITU variant" means there are multiple R2 signaling types in the specified country, but Cisco supports the ITU variant. Cisco Systems also supports specific local variants of E1 R2 signaling in the following regions, countries, and corporations.

Note Country names and regions followed by an asterisk (*) are first supported in Release 11.3(2)T.

- Argentina *
- Australia
- Brazil
- China
- Columbia
- Costa Rica
- East Europe (includes Croatia, Russia, and Slovak Republic) *
- Ecuador ITU *
- Ecuador LME *
- Greece
- Guatemala *
- Hong Kong (uses the China variant) *
- Indonesia
- Israel
- Korea
- Malaysia
- New Zealand
- Paraguay
- Peru *
- Philippines

- Saudi Arabia *
- Singapore
- South Africa (Panaftel variant) *
- Telmex (a telephone corporation in Mexico)
- Telnor (a telephone corporation in Norway)
- Thailand
- Uruguay
- Venezuela
- Vietnam *

Modem Management Enhancement

This modem management enhancement is available for Cisco AS5300 access servers using MICA modems.

You can display a snapshot of all the firmware versions running on all modems in the access server by entering the **show modemcap** command. This command also shows the source location of each version of firmware (for example, running out of Flash memory, boot Flash memory, or bundled with Cisco IOS software). This command is useful for managing and monitoring multiple versions of modem firmware running in an access server.

Telnet Extensions for Dialout

- CSCdj07687—This feature is associated with the Add Telnet Com Port Extensions featurette.

New Features in Cisco IOS Release 11.3(1)T

The following software feature was first introduced in Cisco IOS Release 11.3(1)T.

SNMP Inform Requests

The SNMP Inform Requests feature allows routers to send inform requests to SNMP managers.

Routers can send notifications to SNMP managers when particular events occur. For example, an agent router might send a message to a manager when the agent router experiences an error condition. SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

Because inform requests are more reliable, they consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform request might be retried several times.

The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources. If it is important that the SNMP manager receives every notification, use inform requests. However, if you are concerned about traffic on your network or memory in the router and you do not need to receive every notification, use traps.

Important Notes

This section contains important notes concerning Cisco IOS Release 11.3 T software that apply to the Cisco AS5300.

New TACACS+ Attribute-Value Pair

A new authorization feature that allows you to separately configure and authorize Multilink PPP was added in Cisco IOS Release 11.3(1). This feature can cause MLP authorization to fail in Terminal Access Controller Access Control System (TACACS+) servers that do not include authorization permissions in the configuration.

For TACACS+, add the following attribute-value (AV) pair for all users who are allowed to negotiate Multilink PPP:

```
service = ppp protocol = multilink {
```

Bridge Group Multicast-Source Command

As of Cisco IOS Release 11.3(2)T, the **bridge group multicast-source** command is no longer available. This command was removed to comply with the source-route-transparent (SRT) bridging implementation.

Missing Source-Route Bridging Commands

Because of a production problem, many source-route bridging commands were omitted from the printed version of *Cisco IOS Software Command Summary (78-4746-XX)*. For documentation of all source-route bridging commands, see the *Bridging and IBM Networking Command Reference (78-4743-XX)*. You can also obtain the most current documentation on CCO or on the Documentation CD-ROM.

Image Deferral, Cisco IOS Release 11.3(8)T

Cisco IOS Release 11.3(8)T was deferred to Release 11.3(8)T1 on all software images to incorporate corrections to the following caveats:

- CSCdk86294—The D channel is always in the shutdown state when nonfacility associated signaling is configured.
- CSCdk80809—Enhanced Interior Gateway Routing Protocol (EIGRP) has difficulty converging on certain routes.

For more information on these caveats, refer to Bug Navigator II. Bug Navigator II is available at <http://www.cisco.com/support/bugtools>. On CCO, log in and click this path:

Service & Support: Online Technical Support: Software Bug Toolkit: Bug Navigator II.

Cisco IOS Release 11.3, 11.3 NA, and 11.3 T End of Sales and End of Engineering

End of Engineering (EOE) means that there are no more regularly scheduled maintenance releases. The last maintenance release scheduled on the EOE date is only available through CCO and Field Service Operations—not through manufacturing.

- Cisco IOS Releases 11.3, 11.3 NA, and 11.3 T are scheduled to reach End of Sales (EOS) status with maintenance Releases 11.3(10), 11.3(10)NA, 11.3(10)T.
- Cisco IOS Releases 11.3, 11.3 NA, and 11.3 T are scheduled to reach End of Engineering (EOE) with Releases 11.3(11), 11.3(11)NA, and 11.3(11)T.

EOS and EOE releases are subject to change. For the most up-to-date information on the status of EOS or EOE, see the *End of Sales and End of Engineering for Cisco IOS Software Releases* product bulletins located on CCO.

Ongoing support for functionality in Releases 11.3, 11.3 NA, and 11.3 T is available in Cisco IOS Release 12.0(3)T and later maintenance releases of Cisco IOS Release 12.0 on CCO at:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click **End of Sales and End of Engineering for Cisco IOS Software Releases 11.3 and 11.3 T (#847: 12/98)** or **Cisco IOS Software 11.3 NA EoS and EoE (#849:12/98)**

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. For information on caveats in Cisco IOS Release 11.3 T, refer to the *Caveats for Cisco IOS Release 11.3 T* document which is located on CCO and the Documentation CD-ROM.

All caveats in Release 11.3 are also in Release 11.3 T.

For information on caveats in Cisco IOS Release 11.3, refer to the “Important Notes and Caveats for Release 11.3” section in the cross-platform *Release Notes for Cisco IOS Release 11.3* document which is located on CCO and the Documentation CD-ROM. These release notes list severity 1 and 2 caveats affecting all maintenance releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

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**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Documentation Updates

Due to a production problem, many source-route bridging commands were omitted from the printed version of the *Cisco IOS Software Command Summary* (part number 78-4746-01). For complete documentation of all source-route bridging commands, refer to the *Bridging and IBM Networking Command Reference* (part number 78-4743-01). You can also obtain the most current documentation on the Documentation CD-ROM or Cisco Connection Online (CCO).

Related Documentation

The following sections describe the documentation available for the Cisco AS5300 universal access server. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents.

Use these release notes with these documents:

- Release-Specific Documents, page 24
- Platform-Specific Documents, page 25
- Feature Modules, page 25
- Cisco IOS Software Documentation Set, page 26

Release-Specific Documents

The following documents are specific to Release 11.3 and are located on CCO and the Documentation CD-ROM.

- *Release Notes for Cisco IOS Release 11.3*

You can reach *Cross-Platform Release Notes for Cisco IOS Release 11.3* on CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3

You can reach *Cross-Platform Release Notes for Cisco IOS Release 11.3* on the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3

- Product bulletins, field notices, and other release-specific documents

You can reach these documents on CCO at:

Service & Support: Technical Documents

- Caveats document

As a supplement to the caveats listed in the “Caveats” section in these release notes, see the *Caveats for Cisco IOS Release 11.3 T* document, which contains caveats applicable to all platforms for all maintenance releases of Release 11.3 T.

You can reach the caveats document on CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

You can reach the caveats document on the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

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

The following Cisco AS5300 documents are available:

- *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

The above documentation can be found on CCO and on the Documentation CD-ROM:

- On Cisco Connection Online (CCO) at:
Service & Support: Technical Documents: Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300
- On the Documentation CD at:
Access Servers and Access Routers: Access Servers: Cisco AS5300

Feature Modules

Feature modules describe new features supported by Release 11.3 T 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.

You can reach the feature modules on CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3: New Features in Release 11.3

You can reach the feature modules on the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3: New Features in Release 11.3

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 11.3: Cisco IOS Release 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index

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

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index

Release 11.3 Documentation Set

Table 7 describes the contents of the Cisco IOS Release 11.3 software documentation set, which is available in electronic form and also 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 paper documents were printed.

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

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3

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

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3

Table 7 Cisco IOS Software Release 11.3 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>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP Addressing IP 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> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	ATM Frame Relay SMDS X.25 and LAPB
<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 Interface Configuration Guide</i> • <i>Cisco IOS Interface Configuration Guide</i> 	Interface Configurations
<ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> 	Dial-In Port Setup Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions ISDN X.25 over ISDN VPDN Dial Business Solutions and Examples
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing

Table 7 Cisco IOS Software Release 11.3 Documentation Set (continued)

Books	Chapter Topics
<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
<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 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> 	Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols
<ul style="list-style-type: none"> • <i>Configuration Guide Master Index</i> • <i>Command Reference Master Index</i> 	
<ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> • <i>Cisco IOS System Error Messages</i> • <i>Debug Command Reference</i> • <i>Dial Solutions Quick Configuration Guide</i> 	

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco 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 24.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, 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 Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, *The Cell*, TrafficDirector, TransPath, ViewRunner, VirtualStream, 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, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. 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. (9907R)

Copyright © 1998-1999, Cisco Systems, Inc.
All rights reserved.

