



Text Part Number: 78-6121-06 Rev. -C0

# Release Notes for Cisco AS5300 Universal Access Servers for Cisco IOS Release 12.0 T

---

**May 8, 2001**

These release notes for Cisco AS5300 universal access servers support Cisco IOS Release 12.0 T, up to and including Release 12.0(7)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 12.0 T, see the *Caveats for Cisco IOS Release 12.0 T* document that accompanies these release notes. This caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM. For more information, refer to the "Caveats" on page 39 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 discuss the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 14
- Limitations and Restrictions, page 32
- Important Notes, page 33
- Caveats, page 39
- Related Documentation, page 39
- Service and Support, page 44
- Cisco Connection Online, page 45
- Documentation CD-ROM, page 45

---

### Corporate Headquarters

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

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

# Introduction

This section contains information about the Cisco AS5300 universal access servers and Early Deployment (ED) releases for the Cisco AS5300.

---

**Note** The AS5300/Voice Gateway is primarily supported with voice specific IOS releases, namely 12.0(2)XH and 12.0(4)XH. The first planned General Deployment (GD) release for these key Voice over IP (VoIP) features is 12.0(6)T.

---

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

- Remote Access Server
- Voice Gateway

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

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

For information on new features and Cisco IOS commands supported by Release 12.0(7)T, refer to the "New and Changed Information" on page 14 and the "Related Documentation" on page 39.

## System Requirements

This section describes the system requirements for Release 12.0 T and includes the following topics:

- Memory Requirements, page 3
- Hardware Supported, page 3
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4
- Microcode and Modem Code Software, page 4
- Feature Set Table, page 5

## Memory Requirements

Table 1 describes the DRAM and Flash memory requirements for the Cisco AS5300 for Release 12.0(7)T.

**Table 1** Memory Requirements for Cisco AS5300 Series

Feature Set	Image Name	Required Flash	Required DRAM	Runs From
IP	c5300-i-mz	8 MB	32 MB	RAM
IP Plus	c5300-is-mz	16 MB	64 MB	RAM
IP Plus 40	c5300-is40-mz	16 MB	64 MB	RAM
IP Plus IPsec 56	c5300-is56i-mz	16 MB	64 MB	RAM
IP Plus IPsec 3DES	c5300-ik2s-mz	16 MB	64 MB	RAM
IP/IPX/AT/DEC	c5300-d-mz	8 MB	32 MB	RAM
IP/IPX/AT/DEC Plus	c5300-ds-mz	16 MB	64 MB	RAM
Enterprise	c5300-j-mz	8 MB	32 MB	RAM
Enterprise Plus	c5300-js-mz	16 MB	64 MB	RAM
Enterprise Plus 40	c5300-js40-mz	16 MB	64 MB	RAM
Enterprise Plus IPsec 56	c5300-js56i-mz	16 MB	64 MB	RAM
Enterprise Plus IPsec 3DES	c5300-jk2s-mz	16 MB	64 MB	RAM

## Hardware Supported

Table 2 lists the interface and modem cards supported by the Cisco AS5300 using Cisco IOS Release 12.0 T.

For detailed descriptions of new hardware features, see the "New and Changed Information" on page 14.

**Table 2** Supported Interfaces for the Cisco AS5300 Series

Interface Cards	Modem Cards
Ethernet RJ-45 (included w/ unit)	MICA modems
Ethernet/Fast Ethernet (RJ-45) (included w/ unit)	Microcom 56K modems
ISDN PRI	
E1-G.703/G.704	
Channelized T1 (4 ports) without serial support	
Channelized T1 (4 ports) with 4 serial ports	
Channelized T1 (8 ports) with 4 serial ports	
Channelized E1 (4 ports) without serial support	
Channelized E1 (4 ports) with 4 serial ports	
Channelized E1 (8 ports) with 4 serial ports	
HMM/48 channel	MICA
HMM/60 channel	MICA
DMM/96 channel	MICA

**Table 2 Supported Interfaces for the Cisco AS5300 Series (continued)**

Interface Cards	Modem Cards
DMM/120 channel	MICA
48 Channel, TI C549-based VoIP feature card (Uses High Density AS53-VOXD DSP modules)	
60 Channel, TI C549-based VoIP feature card (Uses High Density AS53-VOXD DSP modules)	
24 Channel, TI C542-based VoIP feature card (First generation, uses AS53-6VOX DSP modules)	
48 Channel, TI C542-based VoIP feature card (First generation, uses AS53-6VOX DSP modules)	

## Determining the Software Version

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

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) AS5300 Software (c5300-i-mz), Version 12.0(7)T, 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)**.

## Microcode and Modem Code Software

Microcode and modem code software images are bundled with the Cisco IOS software image—with the exception of the Channel Interface Processor (CIP) microcode. Bundling eliminates the need to store separate microcode and modem code images. When the Cisco AS5300 is powered on, the system software unpacks the modem code software bundle and loads the proper software on all the interface processor boards. Table 3 lists the current versions of modem firmware and portware supported by the Cisco AS5300 for the Microcom 12-port and MICA 6-port and 12-port modem cards.

---

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

To understand how Cisco IOS software uses Microcom modem code, see the section “Modem Code” in the *Installing 56K 12-Port Modem Modules in Cisco AS5300 Universal Access Servers* publication. To understand how Cisco IOS software uses MICA modem code, see the section “Modem Code” in the *Installing 6-Port Modules and Carrier Cards in Cisco AS5300 Universal Access Servers* publication.

---

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 Service & Support area menu, 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**

On the Documentation CD-ROM at:

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

**Table 3 Current Modem Code Versions for the Cisco AS5300**

Modem Module	Bundled Modem Code Version	Cisco IOS Software Releases
Microcom modems	Microcom version 5.1.20	12.0(5)T and later
MICA modems	MICA portware version 2.7.1.0	12.0(5)T and and later

## 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.

Table 4 lists the software features and feature sets available for the Cisco AS5300 in Cisco IOS Release 12.0 T, up to and including Release 12.0(7)T. Table 4 uses the following conventions:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.
- In —The “In” column lists the Cisco IOS release that first introduced the feature. For example, (7) means a feature is introduced in 12.0(7)T. If a cell is empty in this column, the feature had been previously included in the initial base release.

**Note** This feature set table contains only a selected list of features. This table is not a cumulative or complete list of all the features in each image.

**Table 4 Selected Features Supported by the Cisco AS5300 Feature Sets**

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES <sup>1</sup>	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus IPsec 56	Enter-prise Plus IPsec 56 3DES <sup>2</sup>
<b>IBM Support</b>													
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

## System Requirements

**Table 4 Selected Features Supported by the Cisco AS5300 Feature Sets (continued)**

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPSec 56	IP Plus IPSec 3DES <sup>1</sup>	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus IPSec 56	Enter-prise Plus IPSec 56 3DES <sup>2</sup>
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: — Bisync 3780 Support — BSC Extended Addressing — Block Serial Tunneling (BSTUN) over Frame Relay		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Cisco MultiPath Channel (CMPC)		No	No	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	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Selected Features Supported by the Cisco AS5300 Feature Sets (continued)

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPSec 56	IP Plus IPSec 3DES <sup>1</sup>	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus IPSec 56	Enter-prise Plus IPSec 56 3DES <sup>2</sup>
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
<b>Internet</b>													
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
Store and Forward Fax	5	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes
<b>IP Routing</b>													
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

Table 4 Selected Features Supported by the Cisco AS5300 Feature Sets (continued)

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPSec 56	IP Plus IPSec 3DES <sup>1</sup>	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus IPSec 56	Enter-prise Plus IPSec 56 3DES <sup>2</sup>
TCP Enhancements: — TCP Selective Acknowledgment — TCP Timestamp		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>LAN Support</b>													
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
Subnetwork Bandwidth Manager	5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Management</b>													
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
CNS Client for Cisco IOS Software	4	No	No	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes
CNS client for IOS 12.05(t) (aka IPSec Policy Agent II)	5	No	No	No	No	No	No	No	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
OS_IFSS Featurette	1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
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
VPDN MIB and Syslog Facility		No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Selected Features Supported by the Cisco AS5300 Feature Sets (continued)

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES <sup>1</sup>	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus IPsec 56	Enter-prise Plus IPsec 56 3DES <sup>2</sup>
<b>Multimedia</b>													
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
<b>Quality of Service</b>													
CLI String Search	1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multicast Routing Monitor	5	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
TDM Hairpinning	4	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes
<b>Security</b>													
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
Parse Bookmarks	1	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

## System Requirements

**Table 4 Selected Features Supported by the Cisco AS5300 Feature Sets (continued)**

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES <sup>1</sup>	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus IPsec 56	Enter-prise Plus IPsec 56 3DES <sup>2</sup>
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
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
<b>Switching</b>													
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
<b>Terminal Services</b>													
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
<b>Voice Technologies</b>													
Voice over IP	3	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes

Table 4 Selected Features Supported by the Cisco AS5300 Feature Sets (continued)

Feature	Feature Set													
	In	IP	IP Plus	IP Plus 40	IP Plus IPSec 56	IP Plus IPSec 3DES <sup>1</sup>	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus IPSec 56	Enter-prise Plus IPSec 56 3DES <sup>2</sup>	
High-Density Voice over IP for Cisco AS5300/Voice Gateway	5	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	
<b>WAN Optimization</b>														
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	
<b>WAN Services</b>														
Always On/Dynamic ISDN (AO/DI)		No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	
Async over UDP	5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	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	
E1 R2 Country Support <sup>3</sup>		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
E1 R1 Support for only Taiwan <sup>4</sup>		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	
L2TP Dial-Out	5	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	

## System Requirements

**Table 4 Selected Features Supported by the Cisco AS5300 Feature Sets (continued)**

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPSec 56	IP Plus IPSec 3DES <sup>1</sup>	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus IPSec 56	Enter-prise Plus IPSec 56 3DES <sup>2</sup>
Modem Management Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
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
SS7	4	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes
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
<b>Miscellaneous</b>													
H.323 Version 2 Support	5	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes
Resource Pool Manager	5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Service Provider 1.0 Features	3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>New</b>													
Cisco H.323 Multizone Enhancements	7	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes
Configuring RADIUS for Multiple User Datagram Protocol Ports	7	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Debit Card Accounting and New RADIUS Attributes for IP Telephony	7	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes
Dynamic Multiple Encaps for Dial-in over ISDN	7	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interactive Voice Response for Cisco Access	7	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes

**Table 4 Selected Features Supported by the Cisco AS5300 Feature Sets (continued)**

Feature	Feature Set												
	In	IP	IP Plus	IP Plus 40	IP Plus IPSec 56	IP Plus IPSec 3DES <sup>1</sup>	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus IPSec 56	Enter-prise Plus IPSec 56 3DES <sup>2</sup>
Open Settlements Protocol (OSP) for IP Telephony	7	No	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes
Resource Pool Management Server	7	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resource Pool Management with Direct Remote Services	7	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Selecting AAA Server Groups Based on DNIS	7	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Voice over IP Q.SIG Network Transparency for Cisco AS5300	7	No	Yes	Yes	Yes	Yes	No	Yes	No	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.

## Encryption Images Added to Cisco IOS Release 12.0(2)T and Later

Table 5 lists two new Triple-DES encryption images available in Cisco IOS Release 12.0(2)T and later 12.0 T releases; they are not available in Release 12.0(1)T.

**Table 5 Encryption Images in Cisco IOS Release 12.0(2)T and Later**

Image Name	Feature Set Name	Description
c5300-ik2s-mz	IP Plus IPSec 3DES	Based on the IP Plus image with 56-bit encryption. Includes Triple-DES, the IPSec standard for high-security encryption.
c5300-jk2s-mz	Enterprise Plus IPSec 3DES	Based on the Enterprise Plus image with 56-bit encryption. Includes Triple-DES, the IPSec standard for high-security encryption.



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

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5300 universal access servers for Release 12.0 T:

### New Hardware Features in Release 12.0(7)T

The following new hardware features are supported by the Cisco AS5300 for Release 12.0(7)T:

#### High-Density Voice Support with DSPM-549

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

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

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

The benefits of high-density voice features include:

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

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

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

The benefits of voice features include:

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

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

## New Features in Release 12.0(7)T

The following new hardware features are supported by the Cisco AS5300 universal access servers for Release 12.0(7)T:

### Cisco H.233 Accounting and Security Enhancements for Cisco Gateways

The Cisco H.323 gateway now supports the use of CryptoH323Tokens for authentication. The CryptoH323Token is defined in H.225 Version 2 and is used in a “password-with-hashing” security scheme described in section 10.3.3 of the H.235 specification.

A cryptoToken can be included in any RAS message and is used to authenticate the sender of the message. You can use a separate database for user ID and password verification.

With this release, Cisco H.323 gateways support three levels of authentication:

- **Endpoint**—The RAS channel used for gateway-to-gatekeeper signaling is not a secure channel. To ensure secure communications, H.235 allows gateways to include an authentication key in their RAS messages. This key is used by the gatekeeper to authenticate the source of the messages. At the endpoint level, validation is performed on all messages from the gateway. The cryptoTokens are validated using the password configured for the gateway.
- **Per-Call**—When the gateway receives a call over the telephony leg, it prompts the user for an account number and personal identification number (PIN). These two numbers are included in certain RAS messages sent from the endpoint and are used to authenticate the originator of the call.
- **All**—This option is a combination of the other two. With this option, the validation of cryptoTokens in ARQ messages is based on the account number and PIN of the user making a call and the validation of cryptoTokens sent in all the other RAS messages is based on the password configured for the gateway.

You can configure the level of authentication for the gateway using the Cisco IOS software command line interface.

CryptoTokens for registration requests (RRQ), unregistration request (URQ), disengage request (DRQ) and the terminating side of admission request (ARQ) messages contain information about the gateway that generated the token, including the gateway ID (which is the H.323 ID configured on the gateway) and the gateway password. CryptoTokens for the originating side ARQ messages contain information about the user that is placing the call, including the user ID and personal identification number (PIN).

### Cisco H.323 Multizone Enhancements

Cisco H.323 Multizone enhancements allow a Cisco gateway to provide information to the gatekeeper with additional fields in the RAS (registration, admission, and status) messages.

Previously, the source gateway attempted to set up a call to a destination IP address as provided by the gatekeeper in an Admission Confirm (ACF) message. If the gatekeeper was unable to resolve the destination E.164 phone number to an IP address, the incoming call was terminated.

This version of the H.323 software adds support to allow a gatekeeper to provide additional destination information and modify the destinationInfo field in the ACF. The gateway will include the canMapAlias associated destination information in setting up the call to the destination gateway.

In conjunction with the canMapAlias functionality, this version includes support for the gatekeeper to indicate to the gateway that the call should be destined to a new E.164 number. The gatekeeper indicates this by sending an Admission Confirm message with an IP address of 0.0.0.0 in the destCallSignalAddress field and the new destination E.164 phone number in the destinationInfo field.

The gateway receiving such an ACF will fall back to routing the call based on this new E.164 address and performing a new lookup of the gateway's configured dial plan. This may result in the call being routed back to the PSTN or to an H.323 endpoint.

### Configuring RADIUS for Multiple User Datagram Protocol Ports

In past Cisco IOS releases, RADIUS hosts were uniquely identified by their IP addresses; therefore, only one definition of a RADIUS server for each IP address was allowed. The Configuring RADIUS for Multiple UDP Ports feature expands RADIUS implementation so that RADIUS security servers are identified by their IP addresses and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

The Configuring RADIUS for Multiple UDP Ports feature also applies to RADIUS server groups—server groups can now include multiple service definitions for host entries for the same server, as long as each entry has a unique identifier.

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

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

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

### Dynamic Multiple Encapsulations for Dial-In over ISDN

The Dynamic Multiple Encapsulations feature allows incoming calls over ISDN to be assigned an encapsulation type such as Frame Relay, PPP, and X.25 based on calling line identification (CLID) or DNIS. It also allows various encapsulation types and per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID (caller ID) or DNIS to ensure that only incoming calls with authorization and valid user profiles are accepted. When PPP is used, authentication and profile binding can also be done by PPP name.

In addition, a large set of user profiles can be stored in dialer profiles locally or on a remote AAA server. (For large scale dial-in, storing user-specific configurations on a remote server becomes necessary for enhancing expandability and local memory efficiency.) However, whether stored locally or on a remote AAA server, the user-specific encapsulation and configuration can be applied to individual B channels dynamically and independently.

Dynamic multiple encapsulation is especially important in Europe where ISDN is relatively inexpensive and maximum use of all 30 B channels on the same ISDN link is desirable. Further, the feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

### Gateway Support for Alternate Gatekeeper (CSCdp04549)

The Alternate Gatekeeper feature provides redundancy for a gatekeeper in a system where gatekeepers are used. This enhancement allows a gateway to use up to two alternate gatekeepers as a backup in the case of a primary gatekeeper failure.

A gatekeeper manages H.323 endpoints in a consistent manner, allowing them to register with the gateway and to locate another gatekeeper. The gatekeeper provides logic variables for proxies or gateways in a call path, to provide connectivity with the public switched telephone network (PSTN), to improve Quality of Service (QoS), and to enforce security policies. Multiple gatekeepers may be configured to communicate with one another, either by integrating their addressing into Domain Naming System (DNS) or using Cisco IOS configuration options.

### Interactive Voice Response for Cisco Access

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

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

- Play customized prompts.
- Collect account numbers and PINs.
- Collect destination phone numbers.
- Perform Authentication, Authorization, and Accounting (AAA) tasks interacting with a variety of servers.

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

Internet voice telephony is often used for toll bypass by routing through an existing data network or the Internet instead of PSTN trunks. Calls of this nature require originating and terminating gateways. When the originating and terminating voice gateways are owned by two different carriers, settlement between these carriers is required. The Settlement for Packet Voice feature implements a standardized settlement protocol that can be implemented between different vendors' gateways and voice settlement servers.

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

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

### Redundant Link Manager

Part of the Cisco SS7 Dial Access Solution (DAS), the Cisco Redundant Link Manager (RLM) provides link management over multiple IP networks, so that your Cisco SS7 DAS can tolerate a single point of failure.

By using the RLM functionality, the Q.931 signaling protocol and other proprietary protocols are transported on top of multiple redundant links between a telephony controller and the media gateways (MGWs).

A feature enhancement to RLM for this Cisco SS7 DAS release is redundancy at the link and telephony-controller level. When each RLM group has multiple telephony controllers associated with a MGW, a telephony-controller priority and a link priority are examined by the RLM client during failover, ensuring improved control handling. The RLM client is an MGW running RLM software.

The RLM client on the MGW supports both versions of RLM functionality:

- Multiple redundant links between a single telephony-controller and the MGWs (Version 1)
- Multiple redundant links between multiple telephony-controllers and the MGWs (Version 2)

After installation, the RLM client defaults to Version 2; however, you can choose a different version by using a command line interface (CLI) configuration command. Once an RLM version is selected, all RLM groups on a given MGW use the selected version's functionality.

---

**Note** The RLM feature is backwards compatible on the telephony-controller, but only one version of the RLM client can run on a given MGW.

---

## Resource Pool Management Server

Part of the Cisco SS7 Dial Access Solution (DAS), the Cisco Resource Pool Manager Server (RPMS) communicates with the RPM component of the MGWs to enable telephone companies and ISPs to count, control, bill, and manage resources centrally for wholesale and retail dial network services. RPM is configured across multiple MGW stacks using one or more external RPMS.

The Cisco RPMS provides the following:

- Customer shared-resource management
- Advanced wholesale (VPDN) services for enterprise accounts and ISPs
- Efficient use of resources to offer different oversubscription ratios and dial-service agreements
- Combination of retail and wholesale services on the same MGWs

Cisco RPMS offers three major functions:

- Resource management uses the call type and dialed number identification service (DNIS) information to accept or reject the call based on the customer profile session limits associated with the DNIS information. If the call is accepted, the call is assigned to an MGW resource.
- Dial services determines how the call is handled after it is answered. The call can be authenticated locally or sent to a home gateway through a VPDN tunnel (using the DNIS information or a domain name).
- Call discrimination is used to prevent unapproved call types from accessing MGW resources. When a call is placed, the MGW sends the call type and dialed number information service (DNIS) information to the Cisco RPMS. The Cisco RPMS compares this combination to the call discrimination table. If the call type-DNIS combination appears in the table, the call is rejected.

## Resource Pool Management with Direct Remote Services

Cisco Resource Pool Manager (RPM) enables telephone companies and ISPs to share dial resources for wholesale and retail dial network services in a single network access server (NAS) or across multiple NAS stacks. With Cisco RPM, service providers can count, control, and manage dial resources and provide accounting for shared resources when implementing different service-level agreements.

Cisco RPM can be configured in one or more standalone Cisco NASs, or, optionally, across multiple NAS stacks by using one or more external Cisco Resource Pool Manager Servers (RPMSs).

The Cisco RPM is ideal for combining retail and wholesale dial services using Cisco AS5200, AS5300, and AS5800 network access servers. Call management and call discrimination can be configured to occur before the call is answered. Dial customers are differentiated by the use of configurable customer profiles that are based on the Dialed Number Information Service (DNIS) and the call type determined at the time of an incoming call. When a call arrives at the NAS, the DNIS and call type are matched against a table of disallowed calls. If the DNIS and call type match an entry in this table, the call is rejected. Call discrimination can be used to manage the billing of calls to different types of resources.

When management by virtual private dialup network (VPDN) is configured, a VPDN group includes the information needed to set up or reject a VPDN session. VPDN setup can be based on the DNIS received during call setup, or on the domain name after the call is answered. Load balancing is used to achieve full usage of VPDN tunnels. The VPDN group can also serve as the “customer profile” when all calls are answered and sessions are identified and limited by domain name instead of DNIS.

To support data over voice bearer service (DoVBS), service providers use DNIS to direct calls to the appropriate resource. When a digital call arrives at the NAS through the voice network, it terminates on a High-Level Data Link Control (HDLC) controller rather than on a modem.

Direct remote services is an enhancement to Cisco resource pool management (RPM) implemented in Cisco IOS Release 12.0(7)T that enables service providers to implement wholesale dial services without using VPDN tunnels. A customer profile that has been preconfigured with a PPP template to define the unique PPP services for the wholesale dial customer is selected by the incoming DNIS and call type. At the same time, the DNIS is used to select AAA server groups for authentication/authorization and for accounting for the customer.

### Selecting AAA Server Groups Based on DNIS

In past Cisco IOS releases, authentication and accounting services (otherwise referred to as AAA services) have been implemented in one of the following methods:

- Globally—meaning that AAA services were defined using global configuration access list commands and applied in general to all interfaces on a specific network access server
- Per Interface—meaning that AAA services were defined using interface configuration commands and applied specifically to the interface being configured on a specific network access server
- Using the AAA DNIS Map feature as described in the Cisco IOS Release 12.0(2)T *Selecting AAA Servers Using DNIS Numbers* feature module—meaning that you could use DNIS to specify one AAA server to supply AAA services

With Cisco IOS Release 12.0(7)T, you can now select an AAA server group to which authentication and accounting requests will be sent by using DNIS. With this new Selecting AAA Server Groups Based on DNIS feature, you can specify the same server group for AAA services or a separate server group for each AAA service. You can now configure authentication and accounting on different physical devices and provide failover backup support.

This feature obsoletes the previous Cisco IOS Release 12.0(2)T AAA DNIS Map feature.

### SPE and Firmware Download Enhancements

The **spe** configuration command enables you to download firmware into your modems. When the access server is booted, the **spe** command controls the location from where the firmware image is downloaded to the service processing element (SPE). An SPE unit is defined as the smallest software downloadable unit. For Microcom, an SPE is an individual modem; for MICA an SPE is either 6 or 12 modems, depending on whether the MICA module is single or double density.

### TCLWare

The Debit Card for Packet Telephony on Cisco Access Platforms feature requires the use of both Audio Files and TCL Scripts. Unzip and download the files to your TFTP server.

In addition, download the audio files and TCL scripts from the Access Products Service and Support site on CCO at the following “TCLWare” location:

<http://www.cisco.com/kobayashi/sw-center/sw-access.shtml>

### Voice over IP Q.SIG Network Transparency for Cisco AS5300

QSIG Private Network Transparency provides the Cisco AS5300 the capability to relay QSIG messages transparently across H.323 VoIP networks for inter-PBX/KTS signaling. The feature also provides the ability for internetworking between non-QSIG signaling (for example, E&M, R2, Q.931) and QSIG signaling for basic calls.

QSIG Transparency provides support for ISDN supplementary features such as call waiting and caller identification delivery. The feature supports ISDN supplementary services defined ECMA-141, QSIG Data Link Layer and Standard-142, and QSIG Basic Call Control by providing network feature transparency.

## New Features in Release 12.0(5)T

The following new hardware features are supported by the Cisco AS5300 universal access servers for Release 12.0(5)T:

### Asynchronous Serial Traffic over UDP

The Asynchronous Serial Traffic over UDP feature provides the ability to encapsulate asynchronous data into UDP packets, and then unreliably send this data without needing to establish a connection with a receiving device.

You load the data you want to send through an asynchronous port, and then send it, optionally, as a multicast or a broadcast. The receiving device(s) can then receive the data whenever it wants. If the receiver ends reception, the transmission is unaffected.

This process is referred to as UDP Telnet (UDPTN), although it does not (and cannot) use the Telnet protocol. UDPTN is similar to Telnet in that both are used to send data, but UDPTN is unique in that it does not require that a connection be established with a receiving device.

### Cisco Resource Pool Manager

The Cisco Resource Pool Manager (RPM) feature enables telephone companies and Internet service providers (ISPs) to share dial resources for wholesale and retail dial network services. With RPM, telcos and ISPs can count, control, and manage dial resources and provide accounting for shared resources when implementing different service-level agreements. Resource pool management can be configured in a single, standalone Cisco network access server using RPM or, optionally, across multiple network access server stacks using one or more external Cisco Resource Pool Manager Servers.

### Cisco Store and Forward Fax

Cisco Store and Forward Fax 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 will be delivered as an e-mail attachment.
- Create and send a standard e-mail message that will 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 product to provide confirmed delivery using existing SMTP mechanisms (such as Extended Simple Mail Transfer Protocol (ESMTP)) for those features.

### CNS Client for Cisco IOS Software

Cisco Networking Services (CNS) Client feature for Cisco IOS software enables authenticated directory access. CNS Client for Cisco IOS software includes the following components:

- Lightweight Directing Access Protocol (LDAP) V.3 client
- Support to use Kerberos V.5 as security protocol for LDAP V.3 client
- CNS Event Services Client
- CNS Locator Services Client
- CNS IP Security (IPSec) virtual private network (VPN) Provisioning Agent
- CNS Configuration Change Notification Agent
- CNS Provisioning Agent

LDAP V.3 client functionality enables Cisco IOS software-based applications to securely authenticate to a CNS for Active Directory (CNS/AD) server using Kerberos V.5 as security protocol to retrieve or store information such as policy and configuration data. Cisco IOS software-based applications publish or subscribe to events using CNS event services client, enabling external applications using the application programming interface (API) features of CNS to receive events or publish events to the Cisco IOS device. This Cisco IOS software-based device will use CNS locator services client to locate the nearest directory server using Domain Name System. The administrator need not configure the device to locate the nearest directory server.

All the above-mentioned functionality is intended for use by internal Cisco IOS application developers. CNS IPSec VPN provisioning agent enables the router to retrieve IPSec policies stored in the CNS/AD server and configure itself, automating the provisioning of customer premises equipment devices for IPSec VPN. CNS provisioning agent enables Cisco IOS device to be provisioned using CNS event services.

### H.323 Version 2 Support

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

DTMF is the tone generated on a touch-tone phone when you press keypad digits. The tones are compressed into a single stream at one end of a call and decompressed at the other end by using H.245 messages. However, this compression and decompression can lead to distortion, depending upon the codec used. Thus, the DTMF-relay is used to configure one of three methods to transport DTMF tones generated after the call is established out-of-band. The three methods are:

- The standard H.323 out-of-band method uses H.245 to send digits as audible DTMF tones along with voice (the “h245-signal” option).
- The H.245 “alphanumeric” method (the “h245-alphanumeric” option) uses User Input Indication as part of a control channel, and is another standard H.245 transmission method.
- The “cisco-rtsp” method sends the voice stream but with an identifier indicating that the DTMF tones are added.

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

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

H.323 Version 2 GateKeeper selects a destination gateway by choosing from among all gateways registered in a zone by allowing you to assign selection priorities to these gateways based on the dialed prefix. Gateway resource reporting allows the gateway to notify the gatekeeper when H.323 resources are getting low. The gatekeeper uses this information to determine which gateway it will use to complete a call. The gatekeeper maintains a separate gateway list, ordered by priority, for each of its zone-prefixes.

### High-Density Voice over IP Support for the Cisco AS5300 Gateway

The High-Density Voice over IP Support for the Cisco AS5300 Gateway feature implements high-density voice support on the Cisco AS5300 by using DSPM-549 digital signal processor modules. When equipped with Voice Feature Cards and voice-enabled Cisco IOS software, the AS5300/Voice Gateway supports carrier-class VoIP and fax over IP services.

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

A fully configured voice-capable Cisco AS5300 router includes two voice carrier cards, each capable of supporting 60 concurrent sessions.

### Layer 2 Tunneling Protocol Dial-out

The Layer 2 Tunneling Protocol (L2TP) Dial-Out feature enables L2TP Network Servers (LNSs) to tunnel dial-out VPDN calls using L2TP as the tunneling protocol. This feature enables a centralized network to efficiently and inexpensively establish a virtual point-to-point connection with any number of remote offices.

Using the L2TP Dial-Out feature, Cisco routers can carry both dial-in and dial-out calls in the same L2TP tunnels.

Previously, only dial-in VPDN calls were supported.

L2TP dial-out involves two devices: an LNS and an L2TP Access Concentrator (LAC). When the LNS wants to perform L2TP dial-out, it negotiates an L2TP tunnel with the LAC. The LAC then places a PPP call to the client(s) the LNS wants to dial-out to.

### Service Assurance Agent

The Service Assurance (SA) Agent is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to monitor network performance by measuring key Service Level Agreement metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance.

With Cisco IOS Release 12.0(5)T, the SA Agent provides new capabilities that enable you to:

- Monitor the Domain Name Server, DHCP Server, and DLSw peer stack and tunnel performance. Thresholds can be used to trigger additional collection of time delay statistics.
- Monitor network one-way delay variance (jitter) and packet loss.
- Monitor web server response time.

### Subnetwork Bandwidth Manager

Resource Reservation Protocol (RSVP) is a signalling mechanism that supports request of specific levels of service such as reserved bandwidth from the network. RSVP and its service class definitions are largely independent of the underlying network technologies. This independence requires that a user define the mapping of RSVP onto subnetwork technologies.

The Subnetwork Bandwidth Manager (SBM) feature answers this requirement for RSVP in relation to IEEE 802-based networks. SBM specifies a signalling method and protocol for LAN-based admission control for RSVP flows. SBM allows RSVP-enabled routers and Layer 2 and Layer 3 devices to support reservation of LAN resources for RSVP-enabled data flows. The SBM signalling method is similar to that of RSVP itself. SBM protocol entities have the following features:

- Reside in Layer 2 or Layer 3 devices.
- Can manage resources on a segment. A segment is a Layer 2 physical segment shared by one or more senders, such as a shared Ethernet or Token Ring wire.
- Can become candidates in a dynamic election process that designates one SBM as the segment manager. The elected candidate is called the Designated Subnetwork Bandwidth Manager (DSBM). The elected DSBM is responsible for exercising admission control over requests for resource reservations on a managed segment.

### Voice over IP Enhancements for the Cisco AS5300/Gateway

The Voice over IP Enhancements for the Cisco AS5300/Gateway feature implements voice support on the Cisco AS5300 using DSPM-542 digital signal processor modules.

## New Software Features in Release 12.0(4)T

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

### ISDN LAPB-TA

To carry asynchronous traffic over ISDN, you need a terminal adapter to convert that traffic and forward it over synchronous connections. This is normally implemented by the V.120 protocol, which carries asynchronous traffic over ISDN. However, several countries in Europe (Germany, Switzerland, and some Eastern European countries) use Link Access Procedure, Balanced (LAPB) as the protocol to forward their asynchronous traffic over synchronous connections.

The Cisco AS5300 access server therefore needs to be able to recognize and accept calls from these asynchronous/synchronous conversion devices. The Link Access Procedure, Balanced-Terminal Adapter (LAPB-TA) feature makes this possible. (LAPB is sometimes referred to as “X.75,” because LAPB is the link layer specified in the ITU-T X.75 recommendation for carrying asynchronous traffic over ISDN.)

ISDN LAPB-TA allows a user with an ISDN terminal adapter that supports asynchronous traffic over LAPB to call into the router and establish an asynchronous Point-to-Point Protocol (PPP) session. LAPB supports both local Challenge Handshake Authentication Protocol (CHAP) authentication and external RADIUS authorization on the authentication, authorization, and accounting (AAA) server.

### Dynamic Multiple Encapsulations for Dial-In over ISDN

This feature allows incoming calls over Integrated Services Digital Network (ISDN) to be assigned an encapsulation type such as PPP, X.25, and ISDN LAPB-TA based on calling line identification (CLID) or Dialed Number Identification Service (DNIS). It also allows various encapsulation types as well as per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID or DNIS to make sure that only incoming calls with authorization and valid user profiles are accepted. If the protocol is PPP, authentication and profile binding can also be done by PPP name.

Dynamic multiple encapsulations are especially important in Europe where ISDN is relatively inexpensive and where it is desirable to allow maximum use of all B channels on the same ISDN link, especially for large scale dial-in. This feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

In addition to enhancing large scale dial-in functionality, dynamic multiple encapsulations also work well in smaller scale dial-in situations and for modem calls.

### Time-Division Multiplex Hairpinning

Time-division multiplex (TDM) hairpinning is supported for voice calls on the Cisco AS5300. TDM hairpinning is the connection of an incoming and an outgoing voice call on the same Cisco AS5300 via the TDM bus. The current hairpinning functionality requires converting calls to and from packet form with a pair of digital signal processors (DSPs).

The advantages of TDM hairpinning over conventional DSP-based hairpinning are:

- DSPs are freed as soon as the Cisco AS5300 finds that the call can be handled directly in the TDM bus (or hairpinned)
- Voice quality is improved because TDM hairpinning avoids tandem encoding/compression
- Freeing up DSPs improves the performance of the Cisco AS5300

This new capability is transparent to users because the TDM code handles the hairpinning process. As a result of this internal processing, there are no new or changed CLI commands.

## New Features in Release 12.0(3)T

The following new features are supported by the Cisco AS5300 in Cisco IOS Release 12.0(3)T. To locate the online documentation about these features, refer to the "Platform-Specific Documents" on page 40.

### BERT/TDM

Cisco's bit-error-rate-testing (BERT) solution and time-division multiplexing (TDM) command enhancements have been implemented for the Cisco AS5300 in Cisco IOS Release 12.0(2)XD1 and 12.0(3)T1. This enhancement applies to T1 and E1 facilities. The BERT solution can be managed from remote command-line interface (CLI) and SNMP management platforms for any Cisco AS5300 in the network. A loopback LED on the Cisco AS5300 chassis blinks slowly to indicate that BERT is in progress; it blinks rapidly if the test fails. You can use bit error rate testing and loopbacks to aid in problem resolution as well as to test the quality of T1/E1 links. Early detection of poor quality links and fast problem isolation can result in improved quality of service and higher revenues.

The TDM subsystem troubleshooting commands are not used during normal system operation. Instead, the Cisco IOS commands show the current status and settings of the TDM backplane, enable debug output for display to a console when TDM programming occurs, and provide a set of test commands to test the functionality of the TDM path.

### Voice over IP

Voice over IP (VoIP) support for the Cisco AS5300 was added in Cisco IOS Release 11.3(2)NA. VoIP enables a Cisco AS5300 to carry live voice traffic (for example, telephone calls and faxes) over an IP network. VoIP on the Cisco AS5300 supports two primary applications:

- Central-site telephony termination facility for VoIP traffic from multiple voice-equipped remote office facilities
- Public Switched Telephone Network (PSTN) gateway for Internet telephone traffic

Used as a PSTN gateway, the VoIP feature leverages the standardized use of H.323-based Internet telephone client applications, such as:

- Toll bypass
- Remote PBX presence over WANs
- Unified voice/data trunking

Voice over IP is primarily a software feature. However, to use this feature on the Cisco AS5300, you must install the VoIP feature card (VFC). The VFC contains multiple digital signal processor (DSP) modules. The VFC uses the Cisco AS5300 quad T1/E1 PSTN interface and LAN or WAN routing capabilities to provide up to a 48- or 60-channel gateway for VoIP packetized voice traffic to/from T1/E1 time-division multiplexing (TDM) traffic.

## Service Provider Features for Voice over IP

The Cisco voice service provider features include enhancements to the functionality and configuration of both the gateway and the VoIP gatekeeper. The architecture of these features provides the quality of service (QoS), stability, and functionality necessary for carrier class, real-time IP communications services.

The service provider features offer security, billing, scaling, and reliability for the Cisco VoIP gateway. Supporting up to two T1/E1 digital channels, the gateway connects to existing telephones and fax machines through the PSTN, key systems, and PBXs, making the process of placing calls over the IP network transparent to users. The gateway capability allows the Cisco AS5300 to function as an H.323 endpoint, providing admission control, address lookup and translation, and accounting services.

The gatekeeper manages H.323 endpoints in a consistent manner, allowing them to register with the gatekeeper and to locate another gatekeeper. The gatekeeper provides logic variables for proxies or gateways in a call path to provide connectivity with the PSTN, to improve QoS, and to enforce security policies. Multiple gatekeepers can be configured to communicate with one another, either by integrating their addressing into Domain Naming System (DNS), or via Cisco IOS configuration options.

## SS7/CCS7 Dial Access Solution

The Cisco SS7/CCS7 Dial Access Solution (DAS) provides centralized functions for adding Signaling System 7 (SS7) interfaces to large dial points of presence (POPs). This Non-Facility Associated Signaling (NFAS) functionality provides a full integration of dial access capabilities within the circuit-switched network infrastructure and provides significant savings on switching interface costs while simultaneously reducing trunking costs. Using the NFAS functionality means that all your T1 and E1 channels are used for voice and data while the associated signaling is carried separately over the SS7 network. In addition, you can cost-effectively scale your network from a few hundred to thousands of ports because you do not need to add a D channel for every additional port.

The Cisco SS7/CCS7 DAS allows carrier customers to connect their Cisco AS5300 access servers to the PSTN directly, using SS7 signaling protocols. The SS7 signaling links terminate on a separate UNIX system called the Signaling Controller (SC2200). The SC2200 maps incoming calls, which are signaled via SS7, to bearers on the access servers. The access servers and SC2200 interact to set up and tear down calls using an extended Q.931 protocol over Q.921 and User Datagram Protocol (UDP). In this manner, the Cisco AS5300 access servers and the SC2200 form a system that emulates a terminating or originating end-office telephone switch in the PSTN.

This feature adds two capabilities to Cisco IOS software:

- The control protocol implementation (Q.931/Q.921 over UDP)
- Continuity Check (the ability to loop back a DS-0 and generate tones), which is a maintenance function used in some networks

## Large Scale Dialout

In previous dial-on-demand routing (DDR) networking strategies, only incoming calls could take advantage of features such as dialer and virtual profiles, Multichassis Multilink PPP (MMP) support, and the ability to use an authentication, authorization, and accounting (AAA) server to store attributes. MMP allows network access servers (NASes) to be stacked together and appear as a single NAS chassis so that if one NAS fails, another NAS in the stack can accept calls. MMP also provides stacked NASes access to a local Internet point of presence (POP) using a single telephone number. This allows for easy expansion and scalability as well as assured fault tolerance and redundancy. With large scale dialout, these features are now available for both outgoing and incoming calls.

Large scale dialout eliminates the need to configure dialer maps on every NAS for every destination. Instead, you create remote site profiles containing outgoing call attributes (telephone number, service type, and so on) on the AAA server. The profile is downloaded by the NAS when packet traffic requires a call to be placed to a remote site.

Additionally, large scale dialout addresses congestion management by seeking an uncongested, alternative NAS within the same POP when the designated primary NAS experiences port congestion.

As an added benefit, large scale dialout enables scalable dialout service to many remote sites across one or more Cisco NASes or Cisco routers. This is especially beneficial to both Internet service providers (ISPs) and large scale enterprise customers because it can simplify network configuration and management. Large scale dialout streamlines activities such as service maintenance and scheduled activities like application upgrades from a centralized location. Large enterprise networks such as those used by retail stores, supermarket chains, and franchise restaurants can use large scale dialout to easily update daily prices and inventory information from a central server to all branch locations in one process, using the same NASes they currently use for dial-in functions.

### CDP Additions for Cisco IOS Software

The Cisco Discovery Protocol (CDP) is a media-independent device discovery protocol that runs on all Cisco-manufactured equipment, including routers, bridges, access servers, and switches. Each device sends periodic messages to a multicast address. Each device listens to the periodic messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This process enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP), including local-area network (LAN), Frame Relay, and Asynchronous Transfer Mode (ATM) media. CDP runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

Each device configured for CDP sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information that indicates the time a receiving device should hold CDP information before discarding it.

Additions for Cisco Discovery Protocol (CDP) include the following:

- New syslog output for instances of mismatching native VLAN IDs (IEEE 802.1Q) on connecting ports and port duplex state values on connecting devices
- **cdp advertise-v2** command and new output from **show cdp** commands

### Cisco IOS SNMP v3

Cisco IOS Simple Network Management Protocol version 3 (SNMPv3) addresses issues related to the large scale deployment of SNMP for configuration, accounting, and fault management. SNMP is currently used predominantly for monitoring and performance management. SNMPv3 also facilitates remote configuration of the SNMP entities, which makes remote administration of SNMP entities a much simpler task. SNMPv3 builds on top of SNMPv1 and SNMPv2 to provide a secure environment for the management of systems and networks.

SNMPv3 provides an identification strategy for SNMP devices to facilitate communication only between known SNMP peers. Each SNMP device has an identifier called the SNMP EngineID. SNMP communication is possible only if an SNMP entity knows the identity of its peer SNMP device.

SNMPv3 also contains a security model or security strategy that exists between an SNMP user and the SNMP group to which the user belongs. A security model may define the security policy within an administrative domain or intranet. The SNMPv3 protocol consists of the specification for the User-Based Security Model (USM).

The goals of message authentication service include the following protection strategies:

- **Modification of Information**—Protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal.
- **Masquerade**—Protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations.
- **Message Stream Modification**—Protection against messages getting maliciously reordered, delayed or replayed in order to effect unauthorized management operations.
- **Disclosure**—Protection against eavesdropping on the exchanges between SNMP engines. The following types of communication mechanisms are available for this protection strategy:
  - Communication without authentication and privacy (NoAuthNoPriv).
  - Communication with authentication and without privacy (AuthNoPriv).
  - Communication with authentication and privacy (AuthPriv).

## CISCO-PROCESS-MIB

The CISCO-PROCESS-MIB contains MIB objects that define information displayed about active processes when using the **show processes** command. The addition of this MIB, along with changes to the CISCO-MEMORY-POOL-MIB, allows the retrieval and reporting of additional CPU and memory statistics by SNMP. The CISCO-PROCESS-MIB provides CPU statistics at 5-second, 1-minute, and 5-minute intervals. In addition, this MIB provides CPU utilization and memory allocation/deallocation statistics for each process on each CPU listed in the MIB.

The information defined includes the following objects:

- Process ID
- CPU time the process has used (in milliseconds)
- Number of times the process has been invoked
- CPU time used for each process invocation
- ID of the TTY terminal that controls the process
- Name of the process
- CPU utilization by task in the last five seconds, the last minute, and the last five minutes

The CISCO-PROCESS-MIB is enabled when the first SNMP command is configured. The background statistics collection for VIP cards and the master CPU occurs even if the SNMP subsystem is not initialized.

### New Features in Release 12.0(2)T

The following new features are available for the Cisco AS5300 in Cisco IOS Release 12.0(2)T. To locate the online documentation about these features, refer to the "Platform-Specific Documents" on page 40.

#### Triple-DES Encryption

The IPsec feature in the Cisco IOS now implements Triple-DES, the IPsec standard for high-security encryption, as described in the IETF draft specification *The ESP Triple DES Transform*, by N. Doraswamy, P. Metzger, and W.A. Simpson. This transform uses three independent DES keys to achieve security far greater than that of DES.

For more information, refer to the *Triple DES Encryption for IPsec* document. This document is available on Cisco Connection Online (CCO) and the Documentation CD-ROM.

#### Cisco DialOut Utility

This feature is now supported on the Cisco AS5300 when using MICA modem portware version 2.5.1.0. The Cisco DialOut Utility is a COM port redirector that utilizes a protocol defined in RFC 2217 for communications between the client PC and a dial network access server (NAS).

### New Features in Release 12.0(1)T

The following new features are available for the Cisco AS5300 in Cisco IOS Release 12.0(1)T. To locate the online documentation about these features, refer to the "Platform-Specific Documents" on page 40.

#### CLI String Search

The Command-Line Interface (CLI) String Search feature allows you to search or filter the output of any **show** or **more** command. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. CLI String Search also allows for searching and filtering at `--More--` paging prompts.

With the search function, you can begin unfiltered output at the first line that contains a regular expression you specify. You can specify a maximum of one filter per command to either include or exclude output lines that contain the specified regular expression. A regular expression is any word, phrase, number, or other type of information that appears in **show** or **more** command output.

#### Easy IP Phase 2-DHCP Server

With the introduction of Easy IP Phase 2, Cisco IOS software also supports Intelligent DHCP Relay functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers. A DHCP Relay Agent enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator using standard Cisco IOS IP helper-address functionality.

## ISDN MIB RFC 2127

The new ISDN MIB RFC 2127 has been designed to provide useful information in accordance with the IETF's new standard for the management of ISDN interfaces. It controls all aspects of ISDN interfaces. RFC 2127 provides information on the physical Basic Rate Interfaces (BRIs), control and statistical information for B (bearer) and D (signaling) channels, terminal endpoints, and directory numbers.

The ISDN MIB RFC 2127 controls all aspects of ISDN interfaces. It consists of five groups:

- ISDN Physical Interface Group
- B (Bearer) Channel Group
- D (Signaling) Channel Group
- Terminal Endpoint Group
- Directory Number Group (optional)

The ISDN MIB RFC 2127 enables you to use any commercial SNMP network management application to support ISDN call processing in Cisco IOS software. You can integrate management of dial access products using ISDN with your existing network management systems.

## Time-Based Access Lists

It is now possible to implement access lists based on the time of day. To do so, create a time range that defines specific times of the day and week. The time range is identified by a name, and then referenced by a function, so that those time restrictions are imposed on the function itself.

Currently, IP and IPX extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the permit or deny statements in the access list are in effect. Prior to this feature, access list statements were continuously in effect after they had been applied. Both named or numbered access lists can reference a time range.

## Limitations and Restrictions

### MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. Currently, OLD-CISCO-\* MIBs are being converted into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 6:

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

<b>Deprecated MIB</b>	<b>Replacement</b>
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	

## Important Notes

This section contains important information about Cisco IOS Release 12.0 T software that can apply to the Cisco AS5300 universal access server.

### Deferral of AS5300 Boot Image

The c5300-boot-mz image has been deferred in Cisco IOS Release 12.0(7)T because of a severe defect. This defect has been assigned Cisco Caveat ID CSCdu10569. The software solution for this defect is the c5300-boot-mz image in Cisco IOS Release 12.0(4)T1.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

**Caution** Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

### Last Maintenance Release of Cisco IOS Release 12.0 T

Cisco IOS Release 12.0(6)T has been renamed 12.0(7)T to align this release with the 12.0(7) mainline release. The closed caveats for Release 12.0(7)T are identical to the caveats closed in the 12.0(7) mainline release. There was no change in the feature content of the renamed release--the features in 12.0(6)T are the same as 12.0(7)T. Release 12.0(7)T is the last maintenance release of the 12.0 T release train.

Customers needing closure of caveats for the 12.0 T features should migrate to the 12.1 mainline release, which has the complete feature content of Release 12.0 T and will eventually reach General Deployment (GD). Release 12.0 T is a super set of the 12.0 mainline release, so all caveats closed in the 12.0 mainline are also closed in 12.0 T.

### Cisco IOS Syslog Failure

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

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

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

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

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

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

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

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

### Affected Devices and Software Versions

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

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the "Workarounds" on page 36 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have protects you against this attack.

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

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

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

The following Cisco devices are *not* affected:

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

This vulnerability has been assigned Cisco bug ID CSCdk77426.

## Solution

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

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

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

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

<http://www.cisco.com>

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

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

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

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

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

## Workarounds

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

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

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

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

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

```

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

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

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

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

```

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

## Software Versions and Fixes

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

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

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

---

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

---

## Important Notes

**Table 7 Affected and Repaired Software Versions**

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

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

## Caveats

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

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

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

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

---

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

---

## Related Documentation

The following sections describe the documentation available for the Cisco AS5300 universal access servers. 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 39
- Platform-Specific Documents, page 40
- Feature Modules, page 41
- Cisco IOS Software Documentation Set, page 41

## Release-Specific Documents

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

- *Release Notes for Cisco IOS Release 12.0 T*

You can reach *Cross-Platform Release Notes for Cisco IOS Release 12.0 T* from the CCO home page by clicking on:

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

You can reach *Cross-Platform Release Notes for Cisco IOS Release 12.0 T* on the Documentation CD-ROM by clicking on:

**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

You can reach these documents from the CCO home page at:

**Technical Documents: Product Bulletins**

- Caveat documents

See the *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T* documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.0 and Release 12.0 T.

You can reach the caveat documents from the CCO home page by clicking on:

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

You can reach the caveat documents on the Documentation CD-ROM by clicking on:

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

---

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

---

## Platform-Specific Documents

The documents listed below for the Cisco AS5300 are available on CCO and on 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 the Cisco AS5300 documentation on CCO at:

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

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

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

## Feature Modules

Feature modules describe new features supported by Cisco IOS 12.0 T releases 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, feature modules are only available online. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

You can access the feature modules on CCO at:

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

You can reach the feature modules 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:

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

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

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

Release 12.0 Documentation Set

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

---

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

---

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

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

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

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

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

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• <i>Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Configuration Fundamentals Command Reference</i></li> </ul>	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <li>• <i>Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Bridging and IBM Networking Command Reference</i></li> </ul>	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set
<ul style="list-style-type: none"> <li>• <i>Dial Solutions Configuration Guide</i></li> <li>• <i>Dial Solutions Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview

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

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 1</i></li> <li>• <i>Network Protocols Command Reference, Part 1</i></li> </ul>	IP Addressing IP Services IP Routing Protocols
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 2</i></li> <li>• <i>Network Protocols Command Reference, Part 2</i></li> </ul>	AppleTalk Novell IPX
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 3</i></li> <li>• <i>Network Protocols Command Reference, Part 3</i></li> </ul>	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> <li>• <i>Security Configuration Guide</i></li> <li>• <i>Security Command Reference</i></li> </ul>	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> <li>• <i>Wide-Area Networking Configuration Guide</i></li> <li>• <i>Wide-Area Networking Command Reference</i></li> </ul>	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> <li>• <i>Voice, Video, and Home Applications Configuration Guide</i></li> <li>• <i>Voice, Video, and Home Applications Command Reference</i></li> </ul>	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Video Support Universal Broadband Features
<ul style="list-style-type: none"> <li>• <i>Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Quality of Service Solutions Command Reference</i></li> </ul>	Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Command Summary</i></li> <li>• <i>Dial Solutions Quick Configuration Guide</i></li> <li>• <i>System Error Messages</i></li> <li>• <i>Debug Command Reference</i></li> </ul>	

---

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

---

## Service and Support

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

---

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

---

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

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

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

[http://www.cisco.com/kobayashi/serv\\_tips.shtml](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](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).

---

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

---

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which package that ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <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" on page 39.

Access Registrar, AccessPath, Any to Any, AtmDirector, Browse with Me, 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, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Service Node, Virtual Voice Line, VisionWay, VlanDirector, Voice LAN, WaRP, Wavelength Router, Wavelength Router Protocol, WebViewer, 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, Stratum, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. 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. (9912R)

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