



Text Part Number: 78-5490-09 Rev.-B0

# Release Notes for Cisco AS5200 and Cisco AS5300 Universal Access Servers for Cisco IOS Release 11.3 AA

---

**February 16, 2002**

These release notes for Cisco AS5200 and Cisco AS5300 universal access servers support Cisco IOS Release 11.3 AA, 11.3(9)AA1a and up to and including Release 11.3(11a)AA. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 11.3(11a)AA, see the “Caveats” section on page 26 and *Caveats for Cisco IOS Release 11.3 T*. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

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

## Contents

These release notes discuss the following topics:

- System Requirements, page 2
- New and Changed Information, page 18
- Important Notes, page 24
- Caveats, page 26
- Related Documentation, page 36
- Service and Support, page 42
- Cisco Connection Online, page 43
- Documentation CD-ROM, page 44

---

### Corporate Headquarters

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

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

## Introduction

For information on new features and Cisco IOS commands supported by Release 11.3 AA, refer to the “New and Changed Information” section on page 18 and the “Related Documentation” section on page 36.

## Early Deployment Releases

These release notes describe the Cisco AS5200 and Cisco AS5300 universal access servers for Release 11.3(11a)AA. Release 11.3 AA is an Early Deployment (ED) release based on Release 11.3 and announces fixes to software caveats and support for new Cisco hardware.

For information about features in Release 11.3, see *Cross-Platform Release Notes for Cisco IOS Release 11.3* located on CCO and the Documentation CD-ROM. For information about features in other ED releases, see Table 1.

For information about features in other platforms, see the product-specific release notes which are located on CCO and the Documentation CD-ROM.

**Table 1 Early Deployment Releases for the Cisco AS5200 and Cisco AS5300**

ED Release	Maintenance Release	Platforms Supported	Additional Software Features	Additional Hardware Features	Availability
Release 11.3 AA	(11a)	Cisco AS5200, Cisco AS5300	None	None	Now
Release 11.3 NA	(11)	Cisco AS5300	None	None	Now
Release 11.3 T	(11)	Cisco AS5200	None	None	Now

## System Requirements

This section describes the system requirements for Release 11.3(11a)AA:

- Memory Requirements, page 3
- Hardware Supported, page 4
- Determining the Software Version, page 5
- Upgrading to a New Software Release, page 5
- Modem Code, page 5
- Feature Set Tables, page 7

## Memory Requirements

### Cisco AS5200

For Cisco access servers to take advantage of features in the current release, you must upgrade the code or main system memory as listed in Table 2. Some platforms have specific chip or architecture requirements that affect what can be upgraded and in what increments.

No encryption images are currently available. The image runs from Flash memory.

**Table 2 Cisco AS5200 Memory Requirements**

Feature Sets	Image Name	Software Image	Required Flash Memory	Minimum DRAM Memory	Runs From
Desktop Standard Feature Set	Desktop	c5200-d-l	8 MB	8 MB	Flash
	Desktop Plus	c5200-ds-l	8 MB	8 MB	Flash
IP Standard Feature Set	IP	c5200-i-l	8 MB	8 MB	Flash
	IP Plus	c5200-is-l	8 MB	8 MB	Flash
Enterprise Standard Feature Set	Enterprise	c5200-j-l	16 MB	8 MB	Flash
	Enterprise Plus	c5200-js-l	16 MB	8 MB	Flash

### Cisco AS5300

Flash memory is optional for the Cisco AS5300 images. The images run from RAM. Encryption images first appeared in Cisco IOS Release 11.3(3)T.

**Table 3 Cisco AS5300 Memory Requirements for Images Including Encryption Images**

Feature Sets	Image Name	Software Image	Required Flash Memory	Minimum DRAM Memory	Runs From	Encryption Image Based on:
Desktop Standard Feature Set	Desktop	c5300-d-mz	8 MB	32 MB	RAM	Not available
	Desktop Plus	c5300-ds-mz	8 MB	32 MB	RAM	Not available
IP Standard Feature Set	IP	c5300-i-mz	8 MB	32 MB	RAM	Not available
	IP Plus	c5300-is-mz	8 MB	32 MB	RAM	Not available
	IP Plus 40	c5300-is40-mz	8 MB	32 MB	RAM	IP Plus image with 40-bit encryption
	IP Plus IPSec 56	c5300-is56i-mz	8 MB	32 MB	RAM	IP Plus image with 56-bit encryption

**Table 3 Cisco AS5300 Memory Requirements for Images Including Encryption Images (continued)**

<b>Feature Sets</b>	<b>Image Name</b>	<b>Software Image</b>	<b>Required Flash Memory</b>	<b>Minimum DRAM Memory</b>	<b>Runs From</b>	<b>Encryption Image Based on:</b>
<b>Enterprise Standard Feature Set</b>	Enterprise	c5300-j-mz	8 MB	32 MB	RAM	Not available
	Enterprise Plus	c5300-js-mz	8 MB	32 MB	RAM	Not available
	Enterprise Plus 40	c5300-js40-mz	8 MB	32 MB	RAM	Enterprise Plus image with 40-bit encryption
	Enterprise Plus IPSec56	c5300-js56i-mz	8 MB	32 MB	RAM	Enterprise Plus image with 56-bit encryption

## Hardware Supported

### Cisco AS5200

The Cisco AS5200 universal access server is supported in Release 11.3 AA. The following LAN interfaces are supported on the Cisco AS5200:

- Ethernet (AUI)
- MultiChannel Interface (Channelized E1/T1)

The following WAN data rates are supported on the Cisco AS5200:

- 48/56/64 kbps
- 1.544/2.048 Mbps

The following WAN interfaces are supported on the Cisco AS5200:

- EIA/TIA-232
- X.21
- V.35
- EIA/TIA-449
- EIA-530
- ISDN PRI
- E1-G.703/G.704
- Channelized T1
- Channelized E1
- Serial

## Cisco AS5300

The Cisco AS5300 universal access server is supported in Release 11.3 AA. The following LAN and WAN interfaces are supported on the Cisco AS5300:

- Ethernet RJ-45
- Ethernet/Fast Ethernet (RJ-45)
- ISDN PRI
- E1-G.703/G.704
- Channelized T1
- Channelized E1
- Dual Redundant Internal Power Supplies

The following modem cards are supported on the Cisco AS5300:

- MICA modems
- Microcom 56K modems

## Determining the Software Version

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

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (c5300-js-mz), Version 11.3(11a)AA.....
```

## Upgrading to a New Software Release

For information about upgrading to a new software release, see *Cisco IOS Software Release Upgrade Paths and Packaging Simplification product bulletin #703* located on CCO at:

### Technical Documents: Product Bulletins: Software

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

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

## Modem Code

Cisco IOS Release 11.3(2)T and later releases includes bundled modem code, which is the firmware or portware that runs on the Microcom 12-port and MICA 6-port modem cards. Modem code is bundled with the Cisco IOS software image to eliminate the need to store separate modem code. When the access server starts, the Cisco IOS software unpacks the modem code and loads the proper code on the modem cards.

- For Microcom modems, see Table 4.
- For MICA modems, see Table 5.

Cisco IOS Release 11.3(11a)AA also supports all the features in MICA portware Release 2.5.1.0. The features include V.90 and Fax and Data Dial Out.

## System Requirements

---

When used with Cisco SS7/C7 Dial Access Solution System, portware Release 2.6.0.6 is supported, but needs to be downloaded.

---

**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.

---

**Table 4 Microcom Modem Code for Cisco IOS Release 11.3 AA for the Cisco AS5200 and AS5300**

Access Server	Bundled Modem Code	Cisco IOS Release 11.3 AA
Cisco AS5200 and AS5300	3.1.30	11.3(4)AA and later releases
Cisco AS5200 and AS5300	3.3.20	11.3(5)AA and later releases
Cisco AS5200 and AS5300	5.0.20	Upgrade to Cisco Release 5.0.40
Cisco AS5200 and AS5300	5.0.40	11.3(4)AA and later releases

For more information on Microcom modem compatibility, go to:

<http://www.cisco.com/kobayashi/sw-center/access/as5200-56k.html>

**Table 5 Mica Modem Code for Cisco IOS Release 11.3 AA for the Cisco AS5200 and AS5300**

Bundled Code Version	Portware Code	Access Server	Cisco IOS 11.3 AA
2.0.1.7 initial V.34	2.3.1.0 initial V.34	Cisco AS5200 and AS5300	11.3(4)AA and later releases
2.3.1.0 R1 Support & Maint.	None	Cisco AS5200 and AS5300	11.3(5)AA and later releases
	2.6.0.6—V.90, Fax and Data Dial out	Used on Cisco AS5200 and AS5300 for Cisco SS7/C7 Dial Access Solution System <sup>1</sup>	11.3(8)AA
	2.6.1.0—V.90, Fax and Data Dial out	Cisco AS5200 and AS5300	11.3(8)AA and later releases

<sup>1</sup> You may need to download this portware using the **firmware** command.

For more information on Mica modem compatibility, go to:

<http://www.cisco.com/kobayashi/sw-center/access/as5300-mica.shtml>

### Determining the Version Number of Your Modem Code

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

## Feature Set Tables

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

This section describes the feature sets for the Cisco AS5200 and Cisco AS5300. Feature sets are groupings of features that are provided in the different images available in a given Cisco IOS release. Feature set groups are further divided into optional variations of the basic group.

**Table 6 Feature Set Groups and Feature Sets for the AS5200 and Cisco AS5300 Universal Access Servers**

Feature Set Groups	Standard Feature Sets	Encryption Feature Sets
Desktop	Basic, Plus	Not available
IP	Basic, Plus	Plus 40, Plus IPsec56 <sup>1</sup>
Enterprise	Basic, Plus	Plus 40, Plus IPsec56

<sup>1</sup> IPsec is an abbreviation for IP Security



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

Table 7 and Table 8 list the features and feature sets supported by the Cisco AS5200 and Cisco AS5300 in Cisco IOS Release 11.3(11a)AA. The tables use the following conventions to identify features:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (11) means a feature was introduced in 11.3(11)T. If a cell in this column is empty, the feature was included in the initial base release.

---

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

---

## System Requirements

### Cisco IOS Feature Sets for the Cisco AS5200 Access Servers

Table 7 lists the features for all releases up to the current release.

**Table 7 Cisco IOS Software Feature Sets for the Cisco AS5200 Access Server**

Feature	Feature Set						
	In <sup>1</sup>	IP	IP Plus	Desktop	Desktop Plus	Enterprise	Enterprise Plus
<b>IBM Support</b>							
APPN High-Performance Routing		No	No	No	No	No	No
APPN MIB Enhancements		No	No	No	No	No	No
APPN over Ethernet LAN Emulation		No	No	No	No	No	No
APPN Scalability Enhancements		No	No	No	No	No	No
Bisync Enhancements include: • Bisync 3780 Support • BSC Extended Addressing • Block Serial Tunneling (BSTUN) over Frame Relay		No	No	No	No	Yes	Yes
Cisco MultiPath Channel (CMPC)		No	No	No	No	No	No
DLSw+ Enhancements include: • 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	No	No	No	Yes	Yes
FRAS Enhancements include: • FRAS Boundary Network Node Enhancement • FRAS Dial Backup over DLSw+ • FRAS DLCI Backup • FRAS Host • FRAS MIB • SRB over Frame Relay		No	No	No	No	Yes	Yes
SRB over FDDI on Cisco 4000, 4500, and 4700 Series Routers		No	No	No	No	No	No
RIF Passthru in DLSw+	(3)	No	No	No	No	Yes	Yes
TN3270 LU Nailing		No	No	No	No	No	No
TN3270 Server Enhancements		No	No	No	No	No	No
Token Ring LANE		No	No	No	No	No	No
Tunneling of Asynchronous Security Protocols		No	No	No	No	Yes	Yes

**Table 7 Cisco IOS Software Feature Sets for the Cisco AS5200 Access Server (continued)**

Feature	Feature Set						
	In <sup>1</sup>	IP	IP Plus	Desktop	Desktop Plus	Enterprise	Enterprise Plus
<b>Internet</b>							
DRP Server Agent		Yes	Yes	Yes	Yes	Yes	Yes
DRP Server Agent Enhancements	(2)	Yes	Yes	Yes	Yes	Yes	Yes
L2TP Optimal Fastswitching Support	(8)	Yes	Yes	Yes	Yes	Yes	Yes
<b>IP Routing</b>							
Easy IP (Phase 1)		No	Yes	No	Yes	No	Yes
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations		No	No	No	No	No	No
IP Enhanced IGRP Route Authentication		Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels	(4)T	Yes	Yes	Yes	Yes	Yes	Yes
TCP Enhancements: • TCP Selective Acknowledgment • TCP Timestamp		Yes	Yes	Yes	Yes	Yes	Yes
<b>LAN Support</b>							
AppleTalk Access List Enhancements		No	No	Yes	Yes	Yes	Yes
DECnet Accounting		No	No	Yes	Yes	Yes	Yes
IPX Named Access Lists		No	No	Yes	Yes	Yes	Yes
IPX SAP-after-RIP		No	No	Yes	Yes	Yes	Yes
NLSP Enhancements		No	No	No	No	Yes	Yes
NLSP Multicast Support		No	No	Yes	Yes	Yes	Yes
Token Ring LAN Emulation Services	(8)	Yes	Yes	Yes	Yes	Yes	Yes
<b>Management</b>							
Cisco Call History MIB Command Line Interface		Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS Internationalization		Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB, Phase 1		Yes	Yes	Yes	Yes	Yes	Yes
Show Caller	(5)	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv2C		Yes	Yes	Yes	Yes	Yes	Yes
Virtual Profiles		Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB and Syslog Facility	(3)	No	Yes	No	Yes	Yes	Yes
VPDN Per User Config	(9)	No	Yes	No	Yes	Yes	Yes
Cisco IOS File System (IFS)	(4)AA	Yes	Yes	Yes	Yes	Yes	Yes
<b>Multimedia</b>							
IP Multicast Load Splitting across Equal-Cost Paths		Yes	Yes	Yes	Yes	Yes	Yes

## System Requirements

**Table 7 Cisco IOS Software Feature Sets for the Cisco AS5200 Access Server (continued)**

Feature	Feature Set						
	In <sup>1</sup>	IP	IP Plus	Desktop	Desktop Plus	Enterprise	Enterprise Plus
IP Multicast over ATM Point-to-Multipoint Virtual Circuits		No	No	No	No	No	No
IP Multicast over Token Ring LANs		No	No	No	No	No	No
PIM Version 2		Yes	Yes	Yes	Yes	Yes	Yes
Stub IP Multicast Routing		Yes	Yes	Yes	Yes	Yes	Yes
<b>Quality of Service</b>							
RTP Header Compression		Yes	Yes	Yes	Yes	Yes	Yes
<b>Security</b>							
Named Method Lists for AAA Authorization and Accounting	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Additional Vendor-Proprietary RADIUS Attributes	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Automated-Double Authentication	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Configuring Key, Timeout, Retransmission per Radius Server	(8)	Yes	Yes	Yes	Yes	Yes	Yes
DNS Server Request Support in AAA (Per User DNS)	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Double Authentication		Yes	Yes	Yes	Yes	Yes	Yes
Encrypted-Kerberized Telnet		No	No	No	No	No	No
HTTP Security		Yes	Yes	Yes	Yes	Yes	Yes
MS-CHAP Support	(3)	No	No	No	No	Yes	Yes
Per-User Configuration		Yes	Yes	Yes	Yes	Yes	Yes
Reflexive Access Lists		Yes	Yes	Yes	Yes	Yes	Yes
TCP Intercept		No	No	No	No	Yes	Yes
Vendor-Proprietary RADIUS Attributes		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	No
CLNS and DECnet Fast Switching over PPP		No	No	No	No	Yes	Yes
DECnet/VINES/XNS over ISL, includes: <ul style="list-style-type: none"> <li>• Banyan VINES Routing over ISL Virtual LANs</li> <li>• DECnet Routing over ISL Virtual LANs</li> <li>• XNS Routing over ISL Virtual LANs</li> </ul>		No	No	No	No	Yes	Yes
Fast-Switched Policy Routing		Yes	Yes	Yes	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs		No	No	No	No	No	No

**Table 7 Cisco IOS Software Feature Sets for the Cisco AS5200 Access Server (continued)**

Feature	Feature Set						
	In <sup>1</sup>	IP	IP Plus	Desktop	Desktop Plus	Enterprise	Enterprise Plus
VIP Distributed Switching Support for IP Encapsulated in ISL		No	No	No	No	No	No
<b>Terminal Services</b>							
Telnet Extensions to Dialout <sup>2</sup>		Yes	Yes	Yes	Yes	Yes	Yes
Virtual Templates for Protocol Translation		No	Yes	No	Yes	Yes	Yes
<b>WAN Optimization</b>							
ATM MIB Enhancements		No	No	No	No	No	No
PAD Enhancements		No	Yes	No	Yes	Yes	Yes
PAD Subaddressing		Yes	Yes	Yes	Yes	Yes	Yes
<b>WAN Services</b>							
Configurable SLIP/PPP Timeout Message	(8)	Yes	Yes	Yes	Yes	Yes	Yes
SS7/C7 Continuity Testing for Network Access Servers	(5)	No	Yes	No	Yes	No	Yes
Redundant Link Manager (RLM)	(7)	Yes	Yes	Yes	Yes	Yes	Yes
Continuity Testing (COT)	(7)	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Module	(7)	Yes	Yes	Yes	Yes	Yes	Yes
Always On/Dynamic ISDN (AO/DI)	(3)	No	No	No	No	Yes	Yes
Bandwidth Allocation Control Protocol		Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch	(2)	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Enhancements		Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay MIB Extensions		Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Router ForeSight		Yes	Yes	Yes	Yes	Yes	Yes
ISDN Advice of Charge		Yes	Yes	Yes	Yes	Yes	Yes
ISDN Caller ID Callback		Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS		Yes	Yes	Yes	Yes	Yes	Yes
Layer Two Tunneling Protocol (L2TP)	(5)	No	Yes	No	Yes	Yes	Yes
Layer 2 Forwarding—Fast Switching		No	Yes	No	Yes	Yes	Yes
Leased Line ISDN at 128 kbps		No	No	No	No	No	No
MS Callback	(2)	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Point-to-Point Compression (MPPC)	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types	(3)	Yes	Yes	Yes	Yes	Yes	Yes
National ISDN Switch Types for BRI and PRI Interfaces (NI2)	(3)	Yes	Yes	Yes	Yes	Yes	Yes
PPP over ATM		No	No	No	No	No	No
Stackable Home Gateway	(3)	No	Yes	No	Yes	Yes	Yes

## System Requirements

**Table 7 Cisco IOS Software Feature Sets for the Cisco AS5200 Access Server (continued)**

Feature	Feature Set						
	In <sup>1</sup>	IP	IP Plus	Desktop	Desktop Plus	Enterprise	Enterprise Plus
Telnet Extensions for Dialout		Yes	Yes	Yes	Yes	Yes	Yes
User-Configurable SLIP/PPP Banner with Parameter Insertion	(8)	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Enhancements		Yes	Yes	Yes	Yes	Yes	Yes
X.25 on ISDN		Yes	Yes	Yes	Yes	Yes	Yes
X.25 Switching between PVCs and SVCs		Yes	Yes	Yes	Yes	Yes	Yes
X.28 Emulation		Yes	Yes	Yes	Yes	Yes	Yes

1 The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, (6) means a feature was introduced in Cisco IOS Release 11.3(6)AA. If a cell in this column is empty, the feature was included in the initial base release.

2 All platforms with integrated MICA modems will support dialout in future releases.

### Cisco IOS Feature Sets for the Cisco AS5300 Access Servers

Table 8 lists the features for all releases up to the current release.

**Table 8 Cisco IOS Software Feature Sets for the Cisco AS5300 Access Server**

Feature	Feature Set										
	In <sup>1</sup>	IP	IP Plus	IP Plus 40 <sup>2</sup>	IP Plus IPsec 56	Desktop	Desktop Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56
<b>IBM Support</b>											
APPN High-Performance Routing		No	No	No	No	No	No	No	No	No	No
APPN MIB Enhancements		No	No	No	No	No	No	No	No	No	No
APPN over Ethernet LAN Emulation		No	No	No	No	No	No	No	No	No	No
APPN Scalability Enhancements		No	No	No	No	No	No	No	No	No	No
Bisync Enhancements: • Bisync 3780 Support • BSC Extended Addressing • Block Serial Tunneling (BSTUN) over Frame Relay		No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Cisco MultiPath Channel (CMPC)		No	No	No	No	No	No	No	No	No	No

**Table 8 Cisco IOS Software Feature Sets for the Cisco AS5300 Access Server (continued)**

Feature	Feature Set										
	In <sup>1</sup>	IP	IP Plus	IP Plus 40 <sup>2</sup>	IP Plus IPsec 56	Desk-top	Desk-top Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56
DLSw+ Enhancements: <ul style="list-style-type: none"> <li>• Backup Peer Extensions for Encapsulation Types</li> <li>• DLSw+ Border Peer Caching</li> <li>• DLSw+ MIB Enhancements</li> <li>• DLSw+ SNA Type of Service</li> <li>• LLC2-to-SDLC Conversion between PU4 Devices</li> <li>• NetBIOS Dial-on-Demand Routing</li> <li>• UDP Unicast Enhancement</li> </ul>		No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
FRAS Enhancements: <ul style="list-style-type: none"> <li>• FRAS Boundary Network Node Enhancement</li> <li>• FRAS Dial Backup over DLSw+</li> <li>• FRAS DLCI Backup</li> <li>• FRAS Host</li> <li>• FRAS MIB</li> <li>• SRB over Frame Relay</li> </ul>		No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+	(3)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
SRB over FDDI on Cisco 4000-M, 4500-M, and 4700-M Routers		No	No	No	No	No	No	No	No	No	No
TN3270 LU Nailing		No	No	No	No	No	No	No	No	No	No
TN3270 Server Enhancements		No	No	No	No	No	No	No	No	No	No
Token Ring LANE		No	No	No	No	No	No	No	No	No	No
Tunneling of Asynchronous Security Protocols		No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
<b>Internet</b>											
DRP Server Agent		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DRP Server Agent Enhancements	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
L2TP Optimal Fastswitching Support	(8)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>IP Routing</b>											
Easy IP (Phase 1)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes

## System Requirements

**Table 8 Cisco IOS Software Feature Sets for the Cisco AS5300 Access Server (continued)**

Feature	Feature Set										
	In <sup>1</sup>	IP	IP Plus	IP Plus 40 <sup>2</sup>	IP Plus IPsec 56	Desk-top	Desk-top Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56
IP Enhanced IGRP Route Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Enhancements: <ul style="list-style-type: none"> <li>• TCP Selective Acknowledgment</li> <li>• TCP Timestamp</li> </ul>		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>LAN Support</b>											
AppleTalk Access List Enhancements		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
DECnet Accounting		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
IPX Named Access Lists		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
IPX SAP-after-RIP		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
NLSP Enhancements		No	No	No	No	No	No	Yes	Yes	Yes	Yes
NLSP Multicast Support		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
<b>Management</b>											
Cisco Call History MIB Command Line Interface		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS Internationalization		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB, Phase 1		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Show Caller	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv2C		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Inform Requests	(1)	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Virtual Profiles		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB	(2)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
VPDN MIB and Syslog Facility	(3)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
VPDN Per User Config	(9)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Cisco IOS File System (IFS)	(4) AA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dual Redundant Internal Power Supplies SNMP	(6) <sup>3</sup>	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Multimedia</b>											
IP Multicast Load Splitting across Equal-Cost Paths		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 8 Cisco IOS Software Feature Sets for the Cisco AS5300 Access Server (continued)

Feature	Feature Set										
	In <sup>1</sup>	IP	IP Plus	IP Plus 40 <sup>2</sup>	IP Plus IPsec 56	Desk-top	Desk-top Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56
IP Multicast over ATM Point-to-Multipoint Virtual Circuits		No	No	No	No	No	No	No	No	No	No
PIM Version 2	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast over Token Ring LANs		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stub IP Multicast Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Quality of Service</b>											
RTP Header Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Security</b>											
Automated Double Authentication	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Certificate Authority Interoperability	(3)	No	No	No	Yes	No	No	No	No	No	Yes
Configuring Key, Timeout, Retransmission per Radius Server	(8)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNS Server Request Support in AAA (Per User DNS)	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Double Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encrypted Kerberized Telnet		No	No	No	No	No	No	No	No	No	Yes
HTTP Security		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Internet Key Exchange Security Protocol	(3)	No	No	No	Yes	No	No	No	No	No	Yes
IPsec Network Security	(3)	No	No	No	Yes	No	No	No	No	No	Yes
Message Banners for AAA Authentication	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS-CHAP Support	(3)	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Named Method Lists for AAA Authentication and Accounting	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Per-DNIS AAA Server Selection	(6)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Per-User Configuration		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reflexive Access Lists		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Intercept		No	No	No	No	No	No	Yes	Yes	Yes	Yes
Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Vendor-Proprietary RADIUS —Additional Attributes	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

**Table 8 Cisco IOS Software Feature Sets for the Cisco AS5300 Access Server (continued)**

Feature	Feature Set										
	In <sup>1</sup>	IP	IP Plus	IP Plus 40 <sup>2</sup>	IP Plus IPsec 56	Desk-top	Desk-top Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56
<b>Switching</b>											
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
CLNS and DECnet Fast Switching over PPP		No	No	No	No	No	No	Yes	Yes	Yes	Yes
DECnet/VINES/XNS over ISL: <ul style="list-style-type: none"> <li>• Banyan VINES Routing over ISL Virtual LANs</li> <li>• DECnet Routing over ISL Virtual LANs</li> <li>• XNS Routing over ISL Virtual LANs</li> </ul>		No	No	No	No	No	No	Yes	Yes	No	No
Fast-Switched Policy Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
VIP Distributed Switching Support for IP Encapsulated in ISL		No	No	No	No	No	No	No	No	No	No
<b>Terminal Services</b>											
Telnet Extensions for Dialout		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Templates for Protocol Translation		No	No	No	No	No	No	Yes	Yes	Yes	Yes
<b>WAN Optimization</b>											
ATM MIB Enhancements		No	No	No	No	No	No	No	No	No	No
PAD Enhancements		No	No	No	No	No	No	Yes	Yes	Yes	Yes
PAD Subaddressing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>WAN Services</b>											
Configurable SLIP/PPP Timeout Message	(8)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SS7/C7 Continuity Testing for Network Access Servers	(5)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Redundant Link Manager (RLM)	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Continuity Testing (COT)	(7)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
ISDN Module	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Always On/Dynamic ISDN (AO/DI)	(3)	No	No	No	No	No	No	Yes	Yes	Yes	Yes
E1 R2 Country Support	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
E1 R1 Support for only Taiwan <sup>4</sup>	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

**Table 8 Cisco IOS Software Feature Sets for the Cisco AS5300 Access Server (continued)**

Feature	Feature Set										
	In <sup>1</sup>	IP	IP Plus	IP Plus 40 <sup>2</sup>	IP Plus IPsec 56	Desk-top	Desk-top Plus	Enterprise	Enterprise Plus	Enterprise Plus 40	Enterprise Plus IPsec 56
Enhanced Local Management Interface (ELMI)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay MIB Extensions		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Router ForeSight		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Advice of Charge		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Caller ID Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer Two Tunneling Protocol (L2TP)	(5)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Layer 2 Forwarding—Fast Switching		No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Leased-Line ISDN at 128 kbps		No	No	No	No	No	No	No	No	No	No
Microsoft Point-to-Point Compression (MPPC)	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Modem Management Enhancements	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
National ISDN Switch Types for BRI and PRI Interfaces (NI2)	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP over ATM		No	No	No	No	No	No	No	No	No	No
Stackable Home Gateway	(3)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Switched 56K Digital Connections	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Telnet Extensions for Dialout	(2)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
User-Configurable SLIP/PPP Banner with Parameter Insertion	(8)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 on ISDN		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Switching between PVCs and SVCs		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.28 Emulation		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1 The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, (6) means a feature was introduced in Cisco IOS Release 11.3(6)AA. If a cell in this column is empty, the feature was included in the initial base release.

2 Encryption images are not available in Cisco IOS Releases 11.3(1)T and 11.3(2)T. They are available in Release 11.3(3)T and later 11.3 T releases.

3 Dual Redundant Independent Power Supply was also introduced in Cisco IOS Release 11.3(6)T and 12.0(1)T.

4 E1 R1 signaling support for Taiwan requires MICA portware Version 2.3.1.0.

## New and Changed Information

This section describes the new features supported by the Cisco AS5200 and the Cisco AS5300 in Cisco IOS Release 11.3 AA.

### No New Features in Release 11.3(11a)AA

There are no new features supported by the Cisco AS5200 and Cisco AS5300 universal access servers in Cisco IOS Release 11.3(11a)AA.

### New Software Features in Cisco IOS Release 11.3(9)AA

The following new software enhancement is supported by the Cisco AS5200 and Cisco AS5300 universal access servers for Release 11.3(9)AA.

#### VPDN Per User Config

Previously, Cisco IOS sent domain name or DNS requests for VPDN tunnel attribute information. Then, if no VPDN tunnel attributes were returned, Cisco IOS again tried to send the entire username string for regular PPP termination. Because of this behavior, it was not possible to support per-user tunnel granularity. It also limited the types of connections that are possible in a Radius Proxy VPDN roaming environment.

The VPDN Per User Config feature sends the entire structured username to the AAA server the first time. This allows the Cisco IOS to form a VPDN tunnel or terminate PPP locally depending on the returned attributes.

### New Software Features in Cisco IOS Release 11.3(8)AA

The following new software enhancements are supported by the Cisco AS5200 and Cisco AS5300 universal access servers for Release 11.3(8)AA.

#### L2TP Optimal Fastswitching Support

L2TP Optimal Fastswitching Support is a user transparent performance enhancement that allows L2TP to have the same switching functionality as L2F (Layer2 Forwarding Protocol). This capability was added to L2F as part of the optimal fastswitching support for VPDN in Cisco IOS Release 11.3. This L2TP fastswitching support for LES (LAN emulation server) platforms, even on the LNS (L2TP Network Server), allows L2TP to scale to the large numbers of interfaces that L2F can support (1000+ sessions).

In this implementation, two route cache lookups are used to forward a packet: one to switch to the virtual access interface and the other to switch from the virtual access interface to the output physical interface. This process has been reduced to one. This is accomplished by caching the complete IP/UDP/L2TP/PPP header, which is prepended to the packet that is to be tunneled, so that when a packet is received on the input physical interface, the route cache lookup returns the output physical interface missing out of the virtual interface. The cached header is then prepended to the packet, and the appropriate reformatings are performed before the packet is switched as normal.

This feature is implemented in this way only for Cisco IOS release 11.3 AA. In other releases, the scalability is provided by the FIB.

### Configuring Key, Timeout, and Retransmission per Radius Server

This security feature, also called Per-Radius-server for key, timeout, and retransmit, adds per-server parameters to three global commands that apply to all RADIUS servers:

**radius-server timeout m**

**radius-server retransmit n**

**radius-server key xyz**

The parameters on a per-server basis define the “global” commands for each specified server. For example:

```
radius-server host 1.1.1.1 timeout n retransmit m key abc
radius-server host 2.2.2.2 timeout k retransmit l key def
```

If the user does not define the per-server value, a “global” commands value is used. Anytime the per-server options are used, they override the “global” value. If neither global, nor per-server values are defined, the defaults are used: timeout (5 seconds), retransmit (3 retries), and no key (respectively).

The **radius-server host** is specified by using additional keywords of the three changed command syntax.

### Configurable SLIP/PPP Timeout Message

Configurable SLIP/PPP timeout message is an enhancement to the exec login process whereby the prompt string can be set to some value that does not contain the prompt, thereby keeping the user scripts from becoming confused. When the username or password prompt times out, the prompt string is included as part of the timeout message. The presence of the prompt string in the timeout message can be confused with the login prompt by some scripts. A new command is added that can set the prompt string contained in the timeout message to a different value. This feature is similar and related to the feature User-Configurable SLIP/PPP Banner with Parameter Insertion.

### User-Configurable SLIP/PPP Banner with Parameter Insertion

This feature is a compatibility enhancement that provides a Cisco IOS customizable SLIP command line parser for support of third party vendor equipment that is used to dial into a Cisco access router or server. This feature allows scripts designed to work with SLIP support on third party vendor equipment, such as Netcruiser negotiated parameters syntax, to negotiate compatibly when dialing into a Cisco access router or server.

## New Software Features in Cisco IOS Release 11.3(7)AA

The following new software enhancements are supported by the Cisco AS5200 and Cisco AS5300 universal access servers for Release 11.3(7)AA.

### Cisco SS7/C7 Dial Access Solution System Features

The three new features described in this section support the Cisco SS7/C7 Dial Access Solution System, a product which runs on the following access servers in conjunction with the Cisco Signaling Controller (CSC) and the Network Access Server (NAS):

- Cisco AS5200
- Cisco AS5300

- Cisco AS5800

These features further enhance the capabilities of the Cisco SS7/C7 Dial Access Solution System, which was first introduced with Cisco IOS release 11.3(5)AA. (See the section, “New Features in Cisco IOS Release 11.3(5)AA.”) The new features introduced with the current release are:

- Redundant Link Manager (RLM)
- Continuity Testing (COT)
- ISDN Module

These features provide support for IP connection to SS7/C7 Signaling Controller and associated continuity testing (COT). This support allows carrier customers to connect their access servers to the Public Switch Telephone Network (PSTN) directly, by using Signaling System #7 (SS7/C7) signaling protocols. The SS7/C7 signaling links terminate on a separate UNIX system called the Cisco Signaling Controller (Cisco SC2200). The Cisco SC2200 maps incoming calls, which are signaled via SS7/C7, to bearers on the access servers. The access servers and Cisco SC2200 interact to set up and tear down calls using an extended Q.931 protocol over Q.921 and UDP. In this manner, the access servers and Cisco SC2200 form a system that emulates an end-office switch in the PSTN.

The Cisco SS7/C7 Dial Access Solution System uses the ISDN Q.931 and Q.921 protocols over a Redundant Link Manager (RLM) module. RLM makes use of the UDP protocol to transfer information from the NAS to the CSC and vice versa. The ISDN module works in conjunction with the RLM.

For more information on the Cisco SS7/C7 Dial Access Solution System, see the, “Related Documentation” section on page 36.

### Redundant Link Manager (RLM)

The goal of Redundant Link Manager (RLM) is to primarily provide a virtual link management over multiple IP networks so that the Q.931 signaling protocol and other proprietary protocols can be transported on top of multiple redundant links between the Cisco Signaling Controller (CSC) and the Network Access Server (NAS). In addition to this, RLM opens, maintains, and closes multiple links, manages buffers of queued signaling messages, and monitors whether links are active for link failover and Signaling Controller failover. The user can create more than one IP connection between the CSC and the NAS.

The RLM goes beyond Q.921, because it allows for future use of different upper layers, and more importantly, allows for multiple, redundant paths to be treated as one path by upper layers.

### Continuity Testing (COT)

The Continuity Test (COT) subsystem supports the Continuity Test, which is required by the SS7 network to conduct loopback and NAS-generated tone check testing on the path before a circuit is established. COT will detect any failure of DS0 channels. It is required for North American SS7 compliance.

This feature is an enhancement to the COT feature introduced in Cisco IOS release 11.3(6)AA. See “SS7/C7 Continuity Testing for Network Access Servers” subsection.

## ISDN Module

The ISDN module ensures that the ISDN protocol stack functions properly while the D-channel information (Q.931 and the Q.921 frames) are transported over possibly multiple IP networks via UDP across links managed by the Redundant Link Manager (RLM).

For more information about RLM, see the “Redundant Link Manager (RLM)” subsection.

## New Features in Cisco IOS Release 11.3(6)AA

The following new software enhancements are supported by the Cisco AS5200 and Cisco AS5300 universal access servers for Release 11.3(6)AA.

### Per DNIS AAA Server Selection

You can now authenticate users to a particular AAA server based on the session’s Dialed Number Identification Service (DNIS) number. RADIUS directed-request support has been implemented to support this capability.

Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS allows you to know which customer is calling when you answer.

Cisco routers with either ISDN or internal modems can receive the DNIS number. This functionality allows users to assign different RADIUS servers for different customers (that is, different RADIUS servers for different DNIS numbers).

The DNIS number identifies which number is called to reach you. This capability shows you the calling party number when you answer. You can also assign specific RADIUS servers to different DNIS numbers. In other words, you can assign specific RADIUS servers to individual users dialing into the network.

### Dual Redundant Internal Power Supplies for the Cisco AS5300

The dual redundant power supply feature for the Cisco AS5300 provides optional DC or AC dual internally redundant power supplies for the Cisco AS5300 chassis. This feature provides higher reliability and load balancing. Two versions are available:

- Dual AC input dual 300-watt
  - The dual redundant AC power supply for the Cisco AS5300 has separate power cords.
- Dual DC input dual 300-watt

New and changed Cisco IOS software commands manage the power supply, providing the following capability:

- Designate SNMP trap (message) addresses
- Enable/disable sending SNMP traps
- Send SNMP traps and alarms when a failure or recovery from the unit is detected
- Display of the SNMP environment monitor statistics

For more information, see the online documentation.

### Token Ring LAN Emulation Services

Token Ring LANE allows Token Ring LAN users to take advantage of ATM's benefits without modifying end-station hardware or software. ATM uses connection-oriented service with point-to-point signaling or multicast signaling between source and destination devices. However, Token Ring LANs use connectionless service. Messages are broadcast to all devices on the network. With Token Ring LANE, routers and switches emulate the connectionless service of a Token Ring LAN for the end stations.

By using Token Ring LANE, you can scale your networks to larger sizes while preserving your investment in LAN technology.

For more information, see CCO at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed\\_cr/switch\\_c/xclane.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/switch_c/xclane.htm)

## New Features in Cisco IOS Release 11.3(5)AA

The following new software enhancements are supported by the Cisco AS5200 and Cisco AS5300 universal access servers for Release 11.3(5)AA.

### SS7/C7 Continuity Testing for Network Access Servers

Either the Cisco AS5200 or the Cisco AS5300 universal access server can function as the access server component in a Cisco SS7/C7 dial network access system. For more information on these systems, see the "Related Documentation" section.

This feature allows you to set up continuity testing for Signaling System 7 (SS7/C7) on a network access server (NAS), in which the NAS generates the tone. Continuity testing reduces the call-failure rate by detecting failed DS0s (B channels) on the NAS before setting up a call. Calls can be circuit-switched data calls or analog modem calls. Because the Cisco Signaling Controller SC2200 does not directly control the bearer channels on an access server, the access server must perform the loopbacks and tone generation or tone detection required for continuity testing. Continuity testing is required for North American SS7/C7 compliance.

### Layer Two Tunneling Protocol (L2TP)

On the Cisco AS5200 and Cisco AS5300 universal access servers, Layer Two Tunneling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer Two Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for Access Virtual Private Networks (VPNs). Access VPNs allow mobile users to connect to their corporate intranets or extranets, thus improving flexibility and reducing costs.

### The **show caller** Command Feature

On the Cisco AS5200 and Cisco AS5300 universal access servers, the **show caller** command is a network management feature that applies to dial protocols. It might apply to both private and public networks, both ISP and corporate networks.

Previously, display of login user information was scattered in various **show** commands. It was very time-consuming to debug and track caller information, especially for some high-end access platforms that could potentially have thousands of interfaces up at the same time.

The **show caller** command is a user interface command that displays various information about a particular connection. Its output and usage look similar to the current output of **show user**, but with more options and more information.

The **show caller** command supports both ISDN and asynchronous modem connections. Information is displayed for both incoming and outgoing directions. Interfaces include serial, asynchronous, ISDN, dialer and virtual interfaces (bundle, 'v-access' interfaces).

The **show caller** command is supported for PPP, Multilink PPP, and SLIP. It also includes all NCPs running on PPP, including IP, IPX and Appletalk.

## New Features in Cisco IOS Release 11.3(4)AA

The following new software enhancements are supported by the Cisco AS5200 and Cisco AS5300 universal access servers for Release 11.3(4)AA.

### DNS Server Request Support in AAA (Per User DNS)

On the Cisco AS5200 and Cisco AS5300 universal access servers, Microsoft Point-to-Point Protocol (PPP) clients have the ability to request either a primary or secondary domain naming system (DNS) server from NAS during IP Control Protocol (IPCP) negotiation. To support this functionality using authentication, authorization, and accounting (AAA) security services, two new TACACS+ attribute-value (AV) pairs and two new vendor-proprietary RADIUS attributes have been added.

### Cisco IOS File System (IFS)

The IFS feature provides a single interface to all file systems the Cisco IOS uses:

- Flash memory file systems
- Network file systems (TFTP, rcp, and FTP)
- Any other endpoint for reading or writing data (such as NVRAM, the running configuration, ROM, raw system memory, system bundled microcode, Xmodem, Flash load helper log, modems, and BRI MUX interfaces).

IFS provides the following benefits:

- File viewing and classification
- Platform-independent commands
- Minimal prompting for commands
- Directory navigation and creation

---

**Note** Beginning with this release, Flash memory file commands now use the Cisco IOS File System (IFS). You can no longer use the previous version of these commands.

---

For more information on IFS, see the online documentation under the title *Cisco IOS File System* on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS Software Release 11.3: Cisco IOS 11.3 AA New Features: 11.3(2)AA New Features: Features on All 11.3 AA Platforms: Cisco IOS File System**

You can reach this topic on the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS Software Release 11.3: Cisco IOS 11.3 AA New Features: 11.3(2)AA New Features: Features on All 11.3 AA Platforms: Cisco IOS File System**

## New Features in Cisco IOS Release 11.3 T and Other Releases

These release notes contain features that are specific to Release 11.3(11a)AA only.

Release 11.3(11a)AA is based on Release 11.3. For additional information about the releases which support the Cisco AS5200 and Cisco AS5300 universal access servers, see the “Early Deployment Releases” section on page 2.

## Important Notes

The following sections contain important notes about Cisco IOS Release 11.3 and can apply to the Cisco AS5200 and Cisco AS5300 universal access servers.

### ATM Multipoint Signaling

Prior to Cisco IOS Release 11.1(13) and 11.2(8), the **atm multipoint-signaling** command was used on the main interface and affected all subinterfaces. For Release 11.1(13), 11.2(8), and later releases (including Release 11.3), explicit configuration on each subinterface is required to obtain the same functionality. Refer to caveat CSCdj20944, which is described as follows:

The **atm multipoint-signaling** interface command is currently only available on the main ATM interface. The effect is that signaling behavior (point-to-point or point-to-multipoint) for all clients on all subinterfaces is determined by the command on the main interface.

Clients on different subinterfaces can have different behavior. Specifically, 1577 requires point-to-point, and PIM allows point-to-multipoint. The command should be on a per subinterface basis.

Enable the **atm multipoint-signaling** command on all subinterfaces that require it. Previously, you only needed to enable the command on the main interface.

### Enabling IPX Routing

Whenever IPX routing is enabled, the Token Ring interface resets.

### Forwarding of Locally Sourced AppleTalk Packets

Cisco’s implementation of AppleTalk does not forward packets with local-source and destination network addresses. This behavior does not conform to the definition of AppleTalk in Apple Computer’s *Inside AppleTalk* publication. However, this behavior is designed to prevent any possible corruption of the AppleTalk Address Resolution Protocol (ARP) table in any AppleTalk node that collects MAC-addresses.

## Missing Source-Route Bridging Commands

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

## New TACACS+ Attribute-Value Pair

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

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

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

## Using LAN Emulation

Note the following information regarding the LAN Emulation (LANE) feature in Cisco IOS Release 11.3:

- LANE is available for use with Cisco 4500 and Cisco 4700 series routers, and Cisco 7000 and Cisco 7500 series routers connected to either an LS100 or LS1010 switch. LANE requires at least Version 3.1(2) of the LS100 software, which requires a CPU upgrade if you are currently running software earlier than Version 2.5.
- Do not use the LS2020 for LANE because it does not support UNI 3.0 and point-to-multipoint SVCs.
- Routing of IP, IPX, AppleTalk, DECnet, VINES, and XNS is supported.
- Hot Standby Router Protocol (HSRP) is supported.
- LANE does not support Connectionless Network Service (CLNS) or LANE over Permanent Virtual Circuits (PVCs).
- Do not route AppleTalk Phase 1 to AppleTalk Phase 2 by using LANE.

## 40-bit Encryption Images Are Unavailable in Release 11.3(1)

Cisco is conducting an internal review of the build and distribution processes associated with its 40-bit Cisco IOS cryptographic products. To provide seamless access to Cisco IOS 40-bit encryption capability, Cisco will provide access to the most current 40-bit encryption images, beginning with Cisco IOS Release 1.2 (12), 11.2(12)P, and 11.3(2).

The following 40-bit encryption images are unavailable indefinitely:

- 11.2(1)–11.2(11.2)
- 11.2(2)P–11.2(11.1)P
- 11.2(1)F–11.2(4)F
- 11.3(1)

This review is not related to any new or previously unreported caveats. The information gathered in the review will be used to implement new automated development and order-processing applications.

## Caveats

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

This section contains open and resolved caveats.

All caveats in Release 11.3 and Release 11.3 T are also in Release 11.3(11a)AA.

For information on caveats in Cisco IOS Release 11.3, see “Important Notes and Caveats for Release 11.3” in *Cross-Platform Release Notes for Cisco IOS Release 11.3* on CCO and the Documentation CD-ROM. These release notes list severity 1 and 2 caveats affecting all maintenance releases.

For information on caveats in Cisco IOS Release 11.3 T, see *Caveats for Cisco IOS Release 11.3 T* on CCO and the Documentation CD-ROM.

---

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

---

## Open Caveats—Release 11.3(11a)AA

This section describes possibly unexpected behavior by Release 11.3(11a)AA and describes only severity 1 and 2 caveats.

### Basic System Services

- CSCdp28929  
Router crashes when reference is done to a gone TTY/Telnet session.

### Miscellaneous

- CSCdm74142  
Router crashes with bus error, reason unknown. No workaround at this moment.
- CSCdm77004  
Erratic disconnect of layer 2, the debug ISDN q921 shows bad sequencing, some PRI seem to have a layer 2 looped.
- CSCdm94072  
Router is showing error message, probably connected to Radius.  
  
%SCHED-3-UNEXPECTEDEVENT: Process received unknown event (maj 80, min 0).  
-Process= "Virtual Exec", ipl= 0, pid= 125 -Traceback= 60605B58 606057F0 602446C8  
6025D59C 6025DC50 60285AE0 602C2E2C 602C2E18

- CSCdp08987  
Memory corruption crash ( Software forced crash) .
- CSCdp15792  
Ds0's get stuck in l\_wait\_connect0 state, while trunk state shows that the far end is onhook. Suspected problem with state machine handling a remote disconnect during call setup. Analysis of debugs is necessary to confirm this theory.
- CSCdp60101  
The Kerberos Client functionality on Cisco products, when configured to provide access control, will fail in a "deny" state when the expiration of the credentials is in January or February of leap years, thus denying any Kerberos-authenticated access. A workaround for the problem is to choose an alternate form of authentication such as TACACS+ or RADIUS.

#### Protocol Translation

- CSCdm91167  
Router restarted by software forced crash due to a memory corruption :  
%SYS-3-OVERRUN: Block overrun at 64741B58 (red zone 00000000)

#### TCP/IP Host-Mode Services

- CSCdp39987  
Customers AS5300s running 11.3 AA crash randomly but consistently with System was restarted by error - a Software forced crash, PC 0x60201340.

#### Wide-Area Networking

- CSCdk80734  
The router will reload when the XOT task attempts to exit, which is programmed to occur when it has been idle (i.e. no connections outstanding) for 60 seconds.
- CSCdm05357  
L2TP gets stuck parsing an invalid control message with a zero-length AVP.
- CSCdm19521  
When trying to establish a multichassis multilink connection for a user which is configured for the **ppp dnis** command, SGBP and MMPPP will fail. There is no workaround. SGBP and MMPPP will work for a user who has authenticated "normally" without using the **ppp dnis** command.
- CSCdp30306  
On AS5300, MICA modem calls being placed are failing with "Failed Dial." While this is happening, ISCN CCBs are being allocated (always to B-channel 0) and the calls fail with:  
01:21:14: ISDN Se0:23: Ux\_BadMsg(): Invalid Message for call state 4, call id 0x A0D0, call ref 0x102, event 0x80  
(call state not consistent)
- CSCdp32161  
Executing busyout /no busyout on RLM circuits crash the router.

- CSCdp40171  
Removal of the RLM GROUP from configuration will cause the serial interface to be removed.
- CSCdp40864  
SABMEs may be ignored by the router for extended periods of time after a link failure. (When debug isdn event or debug isdn q931 are active, a Syncing discards message will be displayed for each SABME.)

## Caveats for Release 11.3(1) through 11.3(10)AA and 11.3(9)AA1a.

Unless otherwise noted, these caveats apply to all 11.3 releases up to and including 11.3(10)AA and 11.3(9)AA1a. For additional caveats applicable to Release 11.3(10)AA, see the caveats sections for newer 11.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 11.3(11a)AA and 11.3(9)AA1a.

### Access Server

- CSCdm50856  
The **sh modem** command on an AS5200 router has different results from snmpwalk of the cmInitialLineConnections variable defined in CISCO-MODEM-MGMT-MIB. The IOS is 11.3(8)T1.

### Basic System Services

- CSCdw65903  
An error can occur with management protocol processing. Please use the following URL for further information:  
<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903>
- CSCdk80230  
Certain Internetwork Status Monitor (ISM) NetView users can issue non-enable mode commands without router authentication. Users accessing the router through NetView must be authenticated through NetView's security methods, which may include RACF and SAF. Mainframe users can be restricted from issuing any router commands through the restriction of the RUNCMD within NetView. Users issuing enable mode commands must be authorized to issue this level of command through ISM, and must possess the ENABLE mode password. If the router is controlled by TACACS+, the ISM user must have a TACACS+ User ID and Password to issue enable level commands.  
**show user** : Command has been modified; the user field is filled up by the host name.  
Two options have been added to the following commands : **sna host** and **dspu host**. The options are: no-enable and high-security. These options have to be configured with focalpoint.
  - no-enable : When set does not allow enable command from the host
  - high-security : When set allows the following commands in USER mode. (PRIVILEGE mode is not affected by this option.) All these commands have to be entered in full else the command will not be allowed (i.e "sh versi" is not allowed for **show version**)

ENABLE or EN QUIT EXIT SHOW ? SHOW APPN SHOW VERSION SHOW  
CONTROLLER SHOW EXTENDED SHOW DSPU SHOW SNA SHOW TECH SHOW  
MEMORY SHOW PROCESS SHOW INTERFACE SHOW ENVIRONMENT SHOW  
PROTOCOL

- CSCdm44772

If **sh run** or **wr t** are issued at exactly the same time from two different VTY , one session may finish before the other and trash a variable that still need to be used by the 1st session which causes a router crash.

Workaround: Don't do **sh run** at the same time from 2 VTY's.

### DECnet

- CSCdk23805

When Decnet accounting is implemented, it's possible for the router to crash depending on the amount of connections.

- CSCdm28939

During configuration of Decnet on a router, it is possible to specify an ATG ( Address Translation Gateway ) network number in the range 0 to 3. If the *ATG-network-number* is specified incorrectly while configuring an interface, it will cause the router to reload.

If *ATG-network-number* is not required it does not need to be specified, and the problem will not occur.

If *ATG-network-number* is required then a workaround is to ensure that the *ATG-network-number* specified when enabling an interface matches that specified when Decnet routing is enabled globally, for example:

```
decnet 1 routing 2.3 interface ethernet 0/0 decnet 1 cost 5
```

### EXEC and Configuration Parser

- CSCdm39355

Router crashes while command completion, if the length of the entire command after completion exceeds PARSEBUF.

Fix: Dont allow the "command completion" if it exceeds PARSEBUF .

### IBM Connectivity

- CSCdm39124

Console message flooding may occur when an XID3 loop occurs with APPN in the router. The following messages are repeated for each iteration of the loop.

```
%APPN-3-logcsCS_XXXXIP11_LOGMSG_01: CS - Sending Alert to MS, sense_code =  
83E0001, proc_name = XXXXIP32, port_name = HMAC04, ls_name = @LS00289  
%APPN-3-logcsCS_XXXXIP11_LOGMSG_03: CS - Associated outbound XID data in alert  
(length >= 29): %APPN-3-Error:  
32730770000000000000F7C1000000008000010B51000500000000007000E11F4C4C5C2E5D  
4E4F0F04BD5D5C3C9D7F0F110380037110C0804F1F2F0F0F0F00908F0F0F0F0F014  
06C3C9E2C3D640C1D7D7D540D5D561C4D3E4D90F0FC3C9E2C3D640C1D7D7D540D5  
D52207000000083E0001 %APPN-3-logcsCS_XXXXIP11_LOGMSG_05: CS - Associated  
inbound XID data in alert (length >= 29): %APPN-3-Error:  
326705D56F010000B0081000000000000010B410005B800000000070010370023110C0804  
F0F3F0F0F0F006D4E240E2D5C140E2C5D9E5C5D90908F0F0F0F0F0F013110310001  
0F0F0F0F0F0F0F0F0F0F0F0F00E0FF4C4C5C2E5D4E4F0F04BC3E3F5F6C6
```

Customer bypass is to avoid console logging.

- CSCdm49573  
The router crashes with bus error when executing a **show dlsw circuit** command and there is a circuit with a local rif of 18 bytes.  
This is a regression introduced by CSCdk83294.
- CSCdm50361  
There is a problem whereby DLSw Lite peers leak CLS connect request buffers. If possible, the customer can try using a different peer type. This patch will free an outstanding connect request if additional requests are received while the first is still pending.
- CSCdm51010  
The APPN router may run out of memory due to unnecessary lfsid table expansion for some dlur links to downstream PU2.0s. This problem can occur after dlur takeover or if the dlur-pu had previously received a dactpu not final use from the dlus.
- CSCdm59430  
In a rare situation, router might crash in the TCPD routines or managed timer. There is no workaround for it.

## Interfaces and Bridging

- CSCdk10376  
SYMPTOM Crash in frf9\_preComp()  
CONDITION Mostly frequently will occur during times when router traffic is heavy which causes memory usage to increase and a possible low memory condition to occur.  
WORKAROUND Disable compression or use a different type.  
MISC Since this problem is aggravated by a low memory condition tuning the memory tuning can help prevent it from occurring but will not guarantee it can not happen.
- CSCdm38825  
Under certain conditions, source route bridging using a pa-4r-dtr token ring card may result in frames occasionally being bridged out of order. For protocols which are sensitive to the sequence order of frames, such as LLC2, intermittent session loss may occur.  
There are no known workarounds.
- CSCdm40975  
Under certain conditions, Cisco routers corrupt IP packets when using fancy switching (fast, CEF,...) from a ATM PVC using bridging encapsulation and BVI interface. It happens only if the sending bridge preserves the original CRC in the packet (i.e. uses PID 0x0001, see RFC 1483 page 7).  
Workaround: disable fancy switching
- CSCdm41644  
This is caused by an over-write issue in bss area with FDDI modules equipped which has potential to cause serious problem such as crash in 12.0T.

- CSCdm46735

A PA-4R-DTR port may reset under the following circumstances:

1) A high rate of traffic is traversing the port. (200 pps or better) 2) The PA-4R-DTR port is the Active monitor of the physical ring. 3) A event on the ring occurs that forces the active monitor to purge the ring.

When this problem occurs, the PA-4R-DTR port will reset, and the ring will experience a beacon.

Workaround: Make sure the DTR port is not the active monitor on the ring. This can be done by ensuring that the mac-address of the DTR card is not the highest mac-address on the physical ring.

### IP Routing Protocols

- CSCdm20483

IP access lists fail to block pings on interfaces configured for policy routing with IP route-cache policy.

- CSCdm44957

Some IP fragments may be incorrectly filtered out by access lists.

- CSCdm45873

If you are redistributing OSPF routes into any other routing protocol, it does not include NSSA External routes. There is no work-around.

- CSCdm53317

DNS replies passing from "inside" to "outside" via NAT are not NAT translated correctly in many cases. There is no workaround.

### ISO CLNS

- CSCdm45667

Under certain circumstances, Cisco routers running Cisco IOS Release 11.3(9)T can stop receiving packets on interfaces. This happens when CLNS packets with an N-selector of 0x20 (the DECnet NSP protocol selector) are received by the router and **decnet conversion** has not been enabled or configured correctly.

If this happens, the **show interface** command displays a full input queue and a number of dropped packets. For example: input queue 76/75, 122 drops

When the input queue is full and the interface stops receiving packets, the only course of action is to reload the router.

### LAT

- CSCdm82005

The following line commands are not supported in Cisco IOS Release 12.0(5.5) through 12.0(6): the **session-limit** command, the **absolute-timeout** command, and online help for the **lat** command. There is no workaround.

## Miscellaneous

- CSCdk45491
 

Symptom : The NM-1FE-TX fails to autonegotiate properly when connected through an SMF connector.

Analysis : Setting the speed to 100 manually solves the problem. An interface speed command with the following syntax is being added to overcome this. The default behavior would be to autonegotiate.

```
[no] speed {10 | 100 | auto}
```
- CSCdm04861
 

This was a race condition between the processes that tried to get connection status information (and dropped packet information in the 11-2 version) from the VIP. We put in a semaphore to prevent multiple processes from accessing the globals used at the same time
- CSCdm18910
 

When port info is passed from LAC and **vpdn aaa attribute nas-port vpdn-nas** is configured, it should be mapped to correct NAS-Port-Type value.
- CSCdm22032
 

Configuring PPP encapsulation on an interface and the making that interface a member of a bridge group gives tracebacks and fair-queue not initialized properly messages. Remove bridging from the interface or turning off fair queue makes the messages disappear.

```
00:06:39: -Traceback= 601C9C58 602015E0 60556558 60553958 6021D034 6021D020
00:06:39: Fair Queue:packet not initialized properly: 0, 0 , 38 00:06:39: -Traceback= 601C9C58
602015E0 60556558 60553958 6021D034 6021D020 00:06:39: Fair Queue:packet not
initialized properly: 0, 0 , 38 00:06:39: -Traceback= 601C9C58 602015E0 60556558 60553958
6021D034 6021D020 00:06:40: Fair Queue:packet not initialized properly: 0, 0 , 38 00:06:40:
-Traceback= 601C9C58 602015E0 60556558 60553958 6021D034 6021D020 00:06:40: Fair
Queue:packet not initialized properly: 0, 0 , 38 00:06:40: -Traceback= 601C9C58 602015E0
60556558 60553958 6021D034 6021D020 00:06:40: Fair Queue:packet not initialized properly:
0, 0 , 38 00:06:40: -Traceback= 601C9C58 602015E0 60556558 60553958 6021D034
6021D020 00:06:40: Fair Queue:packet not initialized properly: 0, 0 , 38 00:06:40: -Traceback=
601C9C58 602015E0 60556558 60553958 6021D034 6021D020 00:06:40: Fair Queue:packet
not initialized properly: 0, 0 , 38 00:06:40: -Traceback= 601C9C58 602015E0 60556558
60553958 6021D034 6021D020
```
- CSCdm33429
 

AS5300 will get bus error when under heavy load caused by outgoing modem calls. Have tested with IOS 11.3(9)T and 11.3(8.5)T with same results.

Problem is reproducible within minutes.
- CSCdm33707
 

After a Cisco router is reloaded, the Encryption Service Adapter (ESA) cannot reestablish an active crypto connection.

Workaround: Remove the crypto map, reload the router, and reapply the crypto map.
- CSCdm44726
 

11.3AA images don't support OIR correctly for ATM PAs. OIR the atm PA more than once will hang the box.

- CSCdm52552  
E1 R2 line signalling problem in Fiji to Ericsson switch.
- CSCdm54169  
You cannot change the MTU size of a tunnel interface in code after 11.3(9.2). CSCdk15279 permitted this ability to exceed the MTU size (of the physical interface - 24).  
Workarounds:
  - 1) Use images between 11.3(5.1)T and 11.3(9.3) or 12.0(0.16) and 12.0(4.2). Basically after DDTS# CSCdk15279 and before DDTS# CSCdm06422.
  - 2) Configure **ip mtu** on tunnel interface before **tunnel destination**. If tunnel destination is already configured, then unconfigure the destination, configure **ip mtu**, then reconfigure the destination.  
You will need to wait about 5 seconds after removing the tunnel destination before issuing the **ip mtu** command.  
Once the work-around is issued, there should be no problems in the event of a router reboot as the **ip mtu** command is parsed before the tunnel destination.
- CSCdm58776  
If a router running CET encryption has many connection setup attempts happening at once, some may time out prematurely. Also, some connection setup attempts may not setup properly.
- CSCdm68773  
A Cisco router might reload when the Cisco Service Manager (CSM) tries to allocate modems from a different pool. There is no workaround.
- CSCdm84682  
If you shut down a PA-A2 circuit emulation service (CES) circuit, you will bring down OAM-managed data PVCs that are defined on the same card. There is no workaround.
- CSCdm90336  
Switch/NAS can get out of sync due to IDLE being sent by NAS to switch prior to being ready to accept the next call and a call comes in.  
This results in Switch no longer sending calls to this particular DS0 until NAS sends IDLE back to switch.
- CSCdp13385  
An extra network start accounting

### Novell IPX, XNS, and Apollo Domain

- CSCdk04507  
Routers running IPX and EIGRP at IOS version 11.2 or greater can experience crashes when there is a high frequency of interface up/down transitions, especially with dial-up interfaces.  
Work-around: disable IPX-EIGRP.

## Wide-Area Networking

- CSCdk37517
 

DDR with **dialer dtr** does not reset DTR to a down state after an unsuccessful call attempt. Unsuccessful in this case means that DDR is triggered, DTR is raised, but the modem/TA attached to the serial port never connects so that DCD does not come up.

This can be verified by viewing **show dialer** to ensure that the dialer state is idle, and then **show interface serial x** to check the state of DTR.

This problem does not seem to occur in 11.1 release of software.
- CSCdm01618
 

When the router is functioning as X.28 pad, it should send a X-on to the DTE as soon as it enters the data transfer mode if parameter 5 is set to 1. The pad does not.
- CSCdm28510
 

Adding the **dialer isdn short-hold** command to the **map-class dialer** command to optimize ISDN costs based on AOC-D messages might break the "dialer idle-timeout" configuration. The idle timer resets to 4294966 seconds when expiring, and does not disconnect the ISDN call. The short-hold timer gets incremented on receipt of an AOC-D message, and never disconnects the ISDN call.

Workaround: Remove the **dialer isdn short-hold** command from the **map-class dialer** command.
- CSCdm30090
 

When the router is operating as an X.25 switch, and forwards an X.25 call containing certain facilities not interpreted by the router, the facility values may be corrupted. The problem is most likely to occur when the call cannot be forwarded immediately (i.e., when using X25-over-TCP) with heavy traffic; the affected facilities include any local facilities and the Charging Information facility.
- CSCdm33448
 

A router performing X.25 switching may reload when clearing many calls simultaneously during heavy traffic.
- CSCdm36123
 

Customer is deterministically getting a crash (segV) when dialer rotor best is configured and 'deb dialer' is started once traffic triggers a call.
- CSCdm37153
 

Cisco AS5200 PRI never sends UAF respond to telcos switch in latest 11.3.
- CSCdm37653
 

Reliable PPP can cause an intermittent crash when used with WFQ. Workaround is to disable Reliable PPP or WFQ.
- CSCdm38291
 

Watched route on dialer watch if not installed in routing table when backup interface times out the router configured for dialer watch never dials back.
- CSCdm52736
 

RLM: When the E1 where nfas\_d primary is unplugged, even if the signaling on RLM should not be involved, a NL\_REL\_IND is sent to the ISDN module that stops speaking with the SC.

- CSCdm54100

Customer requires the autoselect functionality for their vty sessions. They are doing X.25 to async and failing PPP CHAP authentication, because of the removal of these commands. They were running an earlier version of 11.3(x) code, which had these commands, but now required an upgrade to 12.0(x) code.

Autocommand is not an option because that would force the vty lines to go into PPP mode and in certain instances, they require EXEC sessions.

BugID CSCdk52583 was the reason for the removal of these commands, identifying a memory leak associated with the autoselect functionality under the vty lines.

Removing these commands now breaks approximately 30,000 client users and an undetermined amount of Cisco routers that previously had this functionality.

- CSCdm61038

It is not possible to change the status of channel 31 (the 32nd channel) in an ISDN E1.

- CSCdm71874

A Cisco router might enter "TEI\_ASSIGNED" mode. In this case, a SABME poll is not answered by the router. There is no workaround.

## Related Documentation

The following sections describe the documentation available for the Cisco AS5200 and Cisco AS5300 universal access servers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

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

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents, page 36
- Platform-Specific Documents, page 37
- Feature Modules, page 38
- Cisco IOS Software Documentation Set, page 39

## Release-Specific Documents

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

- *Release Notes for Cisco IOS Release 11.3*

You can reach the cross-platform *Release Notes for Cisco IOS Release 11.3* on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3**

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

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

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

You can reach these documents on CCO at:

**Service & Support: Technical Document**

- Caveats document

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

You can reach the caveats document on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T**

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

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

---

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

---

## Platform-Specific Documents

These documents are available for the Cisco AS5200 and Cisco AS5300 universal access servers on CCO and the Documentation CD-ROM.

You can reach Cisco AS5200 and Cisco AS5300 documentation on CCO at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Access Servers: Cisco AS5200 and Cisco AS5300**

You can reach Cisco AS5200 and Cisco AS5300 documentation on the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5200 and Cisco AS5300**

### Cisco AS5200 and Cisco AS5300 Documentation

The following Cisco AS5200 documents are available:

- *Cisco AS5200 Universal Access Server Software Configuration Guides*
- *Cisco AS5200 Universal Access Server Installation Guide*
- *Cisco AS5200 Manager Guide*
- Modem/Terminal Adapter Information
- Regulatory Compliance And Safety Information
- Documentation for Spare Parts

The following Cisco AS5300 documents are available:

- *Cisco AS5300 Universal Access Server Chassis Installation Guide*
- *Cisco AS5300 Module Installation Guide*
- *Cisco AS5300 Universal Access Server Software Configuration Guide*
- *New and Changed Cisco IOS Commands for the Cisco AS5300*
- Modem Information
- Regulatory Compliance and Safety Information
- Documentation for Spare Parts

### Modem Code Documentation

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

You can reach modem information on CCO at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Access Servers: Cisco AS5200/Cisco AS5300: Modem Information/Terminal Adapter Information**

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

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

### Portware

Instructions for downloading portware are at the following URL:

**[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/5300/mod\\_info/5238.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/mod_info/5238.htm)**

You can reach the instructions for downloading portware on CCO at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Access Servers: Cisco AS5300: Modem Information: Downloading Modem Code**

You can reach the instructions for downloading portware on the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300: Modem Information: Downloading Modem Code**

## Feature Modules

Feature modules describe new features supported by Release 11.3 AA and are an update to the Cisco IOS documentation set. Feature modules consist of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the features modules are available online only. The feature module information is included in the next printing of the Cisco IOS documentation set.

You can reach more information on the Cisco SS7/C7 Dial Access Solution System on CCO at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Signaling Systems: Signaling Controller: Cisco SS7/C7 Dial Access Solution System Integration Guidelines**

You can reach the feature modules on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3: New Features in Release 11.3**

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

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

## Cisco IOS Software Documentation Set

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

You can reach these documents on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS Release 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index**

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

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

### Release 11.3 Documentation Set

Table 9 includes the contents of the Cisco IOS Release 11.3 software documentation set, which is available in electronic form, and also in printed form upon request.

---

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

---

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

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3**

## Related Documentation

---

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

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

**Table 9 Cisco IOS Software Release 11.3 Documentation Set**

<b>Books</b>	<b>Chapter Topics</b>
<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>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>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>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 Interface Configuration Guide</i></li><li>• <i>Cisco IOS Interface Configuration Guide</i></li></ul>	Interface Configurations
<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 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

**Table 9 Cisco IOS Software Release 11.3 Documentation Set (continued)**

Books	Chapter Topics
<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>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>Configuration Guide Master Index</i></li> <li>• <i>Command Reference Master Index</i></li> </ul>	
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Command Summary</i></li> <li>• <i>Cisco IOS System Error Messages</i></li> <li>• <i>Debug Command Reference</i></li> <li>• <i>Dial Solutions Quick Configuration Guide</i></li> </ul>	

---

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

---

## Service and Support

For service and support for a product purchased from a reseller, contact the reseller who offers a wide variety of Cisco service and support programs that are 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 documents mentioned in the "Related Documentation" section on page 36.

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 © 1999-2000, Cisco Systems, Inc.  
All rights reserved.