



Text Part Number: 78-5072-11

# Release Notes for the Cisco 3600 Series for Cisco IOS Release 11.3 T

---

**August 2, 1999**

These release notes for Cisco 3600 series routers support Cisco IOS Release 11.3 T, up to and including Release 11.3(11)T, which is based on Cisco IOS Release 11.3. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of software caveats that apply to Release 11.3(11)T, refer to the *Caveats for Cisco IOS Release 11.3 T* document that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

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

## Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 12
- Important Notes, page 22
- Caveats, page 24
- Related Documentation, page 24
- Service and Support, page 29
- Cisco Connection Online, page 30
- Documentation CD-ROM, page 30

---

### Corporate Headquarters

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

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

## Introduction

The Cisco 3600 series includes the Cisco 3620 and Cisco 3640 routers. As modular solutions, the Cisco 3600 series enables corporations to increase dial-up density and take advantage of current and emerging Cisco WAN technologies and networking capabilities. The Cisco 3600 series is fully supported by Cisco IOS software, which includes dial-up connectivity, LAN-to-LAN routing, data and access security, WAN optimization, and multimedia features.

## System Requirements

This section describes the system requirements for Release 11.3 T.

- Memory Requirements, page 2
- Hardware Supported, page 3
- Determining the Version of Your Software Release, page 4
- Upgrading to a New Software Release, page 5
- Feature Set Tables, page 5

## Memory Requirements

**Table 1** Memory Requirements for the Cisco 3600 Series

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs from	Status
IP	c3620-i-mz c3640-i-mz	4 MB	16 MB	RAM	
IP Plus	c3620-is-mz c3640-is-mz	8 MB	24 MB	RAM	
IP Plus IPsec 56	c3620-is56i-mz c3640-is56i-mz	8 MB	32 MB	RAM	IPsec 56 encryption image new in Release 11.3(4)T. Required DRAM memory is 24 MB for releases prior to Release 11.3(4)T.
IP/IPX/AT/DEC	c3620-d-mz c3640-d-mz	8 MB	24 MB	RAM	
IP/IPX/AT/DEC Plus	c3620-ds-mz c3640-ds-mz	8 MB	32 MB	RAM	
Enterprise Plus	c3620-js-mz c3640-js-mz	8 MB	32 MB	RAM	
Enterprise Plus IPsec 56	c3620-js56i-mz c3640-js56i-mz	8 MB	32 MB	RAM	IPsec 56 encryption image new in Release 11.3(4)T
Enterprise/APPN Plus	c3620-ajs-mz c3640-ajs-mz	8 MB	32 MB	RAM	

**Table 1** Memory Requirements for the Cisco 3600 Series (continued)

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs from	Status
Enterprise/APPN Plus IPSec 56	c3620-ajs56i-mz c3640-ajs56i-mz	8 MB	32 MB	RAM	IPSec 56 encryption image new in Release 11.3(4)T

## Hardware Supported

Cisco IOS Release 11.3 T supports the Cisco 3600 series:

- Cisco 3620
- Cisco 3640

For detailed descriptions of new hardware features, refer to the “New and Changed Information” section on page 12.

**Table 2** Supported Interfaces and Data Rates for the Cisco 3600 Series

Interface, Network Module, or Data Rate	Platforms Supported	
<b>Dial Access Network Modules</b>	16- and 32-port Asynchronous network module	All Cisco 3600 series platforms
	6- to 30-port Integrated Digital Modems network module	All Cisco 3600 series platforms
	8- or 16-port Integrated Analog network module	All Cisco 3600 series platforms
<b>LAN Interfaces</b>	1- and 4-port Ethernet (AUI and 10BaseT)	All Cisco 3600 series platforms
	4/16 Mbps Token Ring	All Cisco 3600 series platforms
	Fast Ethernet (100BaseTX and 100BaseFX)	All Cisco 3600 series platforms
<b>Mixed Media Network Modules</b>	Single port 10/100BaseTX with 1-port Channelized/PRI E1 balanced mode	All Cisco 3600 series platforms
	Single port 10/100BaseTX with 1-port Channelized/PRI E1 unbalanced mode	All Cisco 3600 series platforms
	Single port 10/100BaseTX with 1-port Channelized/PRI T1	All Cisco 3600 series platforms
	Single port 10/100BaseTX with 1-port Channelized/PRI T1 with CSU	All Cisco 3600 series platforms
	Single port 10/100BaseTX with 2-port Channelized/PRI E1 balanced mode	All Cisco 3600 series platforms
	Single port 10/100BaseTX with 2-port Channelized/PRI E1 unbalanced mode	All Cisco 3600 series platforms
	Single port 10/100BaseTX with 2-port Channelized/PRI T1	All Cisco 3600 series platforms
	Single port 10/100BaseTX with 2-port Channelized/PRI T1 with CSU	All Cisco 3600 series platforms

**Table 2 Supported Interfaces and Data Rates for the Cisco 3600 Series (continued)**

Interface, Network Module, or Data Rate	Platforms Supported	
<b>Voice/Fax Interfaces and Network Modules<sup>1</sup></b>	1- and 2-port Voice/Fax network module	All Cisco 3600 series platforms with Voice/Fax network module
	2-port E&M Voice interface card	All Cisco 3600 series platforms
	2-port FXO Voice interface card	All Cisco 3600 series platforms with Voice/Fax network module
	2-port FXS Voice interface card	All Cisco 3600 series platforms with Voice/Fax network module
<b>WAN Data Rates</b>	48/56/64 kbps	All Cisco 3600 series platforms
	1.544/2.048 Mbps	All Cisco 3600 series platforms
	Up to 8 Mbps on 4-port Serial network module	All Cisco 3600 series platforms
	52 Mbps max using High Speed Serial Interface (HSSI) network module	All Cisco 3600 series platforms
<b>WAN Interfaces and Network Modules<sup>2</sup></b>	1- and 2-port Channelized T1 and E1 network module	All Cisco 3600 series platforms
	1-port ATM-25 network modules for the Cisco 3600 series	All Cisco 3600 series platforms
	1-port BRI with NT or S/T WAN interface card	All Cisco 3600 series platforms
	1-Port High Speed Serial Interface (HSSI) network module	All Cisco 3600 series platforms
	4- and 8-port BRI network module with NT1	All Cisco 3600 series platforms
	4- and 8-port BRI network module with S/T interface	All Cisco 3600 series platforms
	4- and 8-port Synchronous/Asynchronous	All Cisco 3600 series platforms
	4-port Serial	All Cisco 3600 series platforms
	56/64 kbps DSU/CSU	All Cisco 3600 series platforms
	T1 WAN interface card for Cisco 3600, Cisco 2600, and Cisco 1600 series	All Cisco 3600 series platforms
T1 with Integrated DSU/CSU for the Cisco 3600, Cisco 2600, and Cisco 1600 series	All Cisco 3600 series platforms	

1 The Voice/Fax network modules require Cisco IOS Plus feature sets.

2 The ATM-25 network modules require Cisco IOS Plus feature sets.

## Determining the Version of Your Software Release

To determine the version of Cisco IOS software currently running on the Cisco 3600 series router, log in to the Cisco 3600 series router and enter the **show version EXEC** command.

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-AJS-MZ), Version 11.3(11)T, RELEASE SOFTWARE
```

## Upgrading to a New Software Release

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

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

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

This product bulletin does not include information specific to Cisco IOS Release 11.3 T, but provides general upgrade information that may apply to Cisco IOS Release 11.3 T.

## Microcode and Modem Code Software

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

---

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

---

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

You can reach the release notes and configuration information on CCO at:

**Service & Support: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers: Cisco 3600 Series: Analog Modem Firmware**

**Service & Support: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers: Cisco 3600 Series: Digital Modem Portware**

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

**Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 3600 Series: Analog Modem Firmware**

**Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 3600 Series: Digital Modem Portware**

## Feature Set Tables

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

**Table 3 Feature Sets Supported by the Cisco 3600 Series**

Feature Set	Feature Set Matrix Term	Software Image	Platforms
<b>IP Standard Feature Sets</b>			
IP	Basic <sup>1</sup>	c3620-i-mz	Cisco 3620
		c3640-i-mz	Cisco 3640

**Table 3 Feature Sets Supported by the Cisco 3600 Series**

Feature Set	Feature Set Matrix Term	Software Image	Platforms
IP Plus	Plus	c3620-is-mz	Cisco 3620
		,c3640-is-mz	Cisco 3640
IP Plus IPsec 56	Plus, Plus IPsec 56 <sup>2</sup>	c3620-is56i-mz	Cisco 3620
		c3640-is56i-mz	Cisco 3640
<b>Desktop Standard Feature Sets</b>			
Desktop (IP/IPX/AT/DEC)	Basic	c3620-d-mz	Cisco 3620
		c3640-d-mz	Cisco 3640
Desktop (IP/IPX/AT/DEC Plus)	Plus	c3620-ds-mz	Cisco 3620
		c3640-ds-mz	Cisco 3640
<b>Enterprise Feature Set</b>			
Enterprise Plus	Plus	c3620-js-mz	Cisco 3620
		c3640-js-mz	Cisco 3640
Enterprise Plus IPsec 56	Plus, Plus IPsec 56	c3620-js56i-mz	Cisco 3620
		c3640-js56i-mz	Cisco 3640
<b>Enterprise/APPN Feature Set</b>			
Enterprise/APPN Plus	Plus	c3620-ajs-mz	Cisco 3620
		c3640-ajs-mz	Cisco 3640
Enterprise/APPN Plus IPsec 56	Plus, Plus IPsec 56	c3620-ajs56i-mz	Cisco 3620
		c3640-ajs56i-mz	Cisco 3640

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



**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, you 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 4 lists the features and feature sets supported by the Cisco 3600 series in Cisco IOS Release 11.3 T. Table 4 uses the following conventions to identify features:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was first introduced. For example, a (2) means a feature is introduced in Release 11.3(2)T. If a cell is empty in this column, the feature was introduced in the initial base release.

---

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

---

Table 4 Feature List by Feature Set for the Cisco 3600 Series

Feature	In	Feature Set								
		IP	IP Plus	IP Plus IPsec 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise/ APPN Plus	Enterprise/ APPN Plus IPsec 56
<b>IBM Support</b>										
APPN High Performance Routing		No	No	No	No	No	No	No	Yes	Yes
APPN MIB Enhancements		No	No	No	No	No	No	No	Yes	Yes
APPN over Ethernet LAN Emulation		No	No	No	No	No	No	No	Yes	Yes
APPN Scalability Enhancements		No	No	No	No	No	No	No	Yes	Yes
Bisync Enhancements: — Bisync 3780 Support — BSC Extended Addressing — Block Serial Tunneling (BSTUN) over Frame Relay		No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Cisco MultiPath Channel (CMPC)		No	No	No	No	No	No	No	No	No
DLSw+ Enhancements: — Backup Peer Extensions for Encapsulation Types — DLSw+ Border Peer Caching — DLSw+ MIB Enhancements — DLSw+ SNA Type of Service — LLC2-to-SDLC Conversion between PU4 Devices — NetBIOS Dial-on-Demand Routing — UDP Unicast Enhancement		No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 3600 Series (continued)

Feature	In	Feature Set								
		IP	IP Plus	IP Plus IPsec 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise/ APPN Plus	Enterprise/ APPN Plus IPsec 56
FRAS Enhancements: — FRAS Boundary Network Node Enhancement — FRAS Dial Backup over DLSw+ — FRAS DLCI Backup — FRAS Host — FRAS MIB — SRB over Frame Relay		No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
RIF Passthrough in DLSw+	(3)	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
SRB over FDDI on Cisco 4000, 4500, and 4700 Series Routers		No	No	No	No	No	No	No	No	No
TN3270 LU Nailing		No	No	No	No	No	No	No	No	No
TN3270 Server Enhancements		No	No	No	No	No	No	No	No	No
Token Ring LANE		No	No	No	No	No	No	No	No	No
Tunneling of Asynchronous Security Protocols		No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
<b>Internet</b>										
DRP Server Agent		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DRP Server Agent Enhancements	(2)	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
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations		No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Enhanced IGRP Route Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels (CSCdj88415)	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 3600 Series (continued)

Feature	In	Feature Set								
		IP	IP Plus	IP Plus IPsec 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise/ APPN Plus	Enterprise/ APPN Plus IPsec 56
TCP Enhancements: — TCP Selective Acknowledgment — TCP Timestamp		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>LAN Support</b>										
AppleTalk Access List Enhancements		No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
DECnet Accounting		No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
IPX Named Access Lists		No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
IPX SAP-after-RIP		No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
NLSP Enhancements		No	No	No	No	No	Yes	Yes	Yes	Yes
NLSP Multicast Support		No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
<b>Management</b>										
Cisco Call History MIB Command Line Interface		No	No	No	No	No	No	No	No	No
Cisco IOS Internationalization		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB, Phase 1		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv2C		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Inform Requests		No	No	No	No	No	Yes	Yes	Yes	Yes
Virtual Profiles		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB and Syslog Facility	(3)	No	Yes	Yes	No	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
IP Multicast over ATM Point-to-Multipoint Virtual Circuits		No	No	No	No	No	No	No	No	No
IP Multicast over Token Ring LANs		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM Version 2	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stub IP Multicast Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Voice over IP		No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
<b>Quality of Service</b>										
RTP Header Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

**Table 4 Feature List by Feature Set for the Cisco 3600 Series (continued)**

Feature	In	Feature Set								
		IP	IP Plus	IP Plus IPsec 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise/ APPN Plus	Enterprise/ APPN Plus IPsec 56
<b>Security</b>										
Additional Vendor-Proprietary RADIUS Attributes	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automated Double Authentication	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Certificate Authority Interoperability	(3)	No	No	Yes	No	No	No	Yes	No	Yes
Double Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encrypted Kerberized Telnet		No	No	No	No	No	No	Yes	No	Yes
HTTP Security		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Internet Key Exchange Security Protocol	(3)	No	No	Yes	No	No	No	Yes	No	Yes
IPsec Network Security	(3)	No	No	Yes	No	No	No	Yes	No	Yes
MS-CHAP Support	(3)	No	No	No	No	No	Yes	Yes	Yes	Yes
Named Method Lists for AAA Authorization & Accounting	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Per-User Configuration		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reflexive Access Lists		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Intercept		No	No	No	No	No	Yes	Yes	Yes	Yes
Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Switching</b>										
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs		No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
CLNS and DECnet Fast Switching over PPP		No	No	No	No	No	Yes	Yes	Yes	Yes
DECnet/VINES/XNS over ISL, includes:		No	No	No	No	No	Yes	Yes	Yes	Yes
— Banyan VINES Routing over ISL Virtual LANs										
— DECnet Routing over ISL Virtual LANs										
— XNS Routing over ISL Virtual LANs										

Table 4 Feature List by Feature Set for the Cisco 3600 Series (continued)

Feature	In	Feature Set								
		IP	IP Plus	IP Plus IPsec 56	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise/APPN Plus	Enterprise/APPN Plus IPsec 56
Fast-Switched Policy Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs		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
<b>Terminal Services</b>										
Virtual Templates for Protocol Translation		No	No	No	No	No	Yes	Yes	Yes	Yes
<b>WAN Optimization</b>										
Always On/Dynamic ISDN (AO/DI)	(3)	No	No	No	No	No	Yes	Yes	Yes	Yes
ATM MIB Enhancements		No	No	No	No	No	No	No	No	No
PAD Enhancements		No	No	No	No	No	Yes	Yes	Yes	Yes
PAD Subaddressing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>WAN Services</b>										
Bandwidth Allocation Control Protocol		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced Local Management Interface (ELMI)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay MIB Extensions		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Router ForeSight		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Advice of Charge		No	No	No	No	No	No	No	No	No
ISDN Caller ID Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS		No	No	No	No	No	No	No	No	No
Layer 2 Forwarding—Fast Switching		No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Leased Line ISDN at 128 kbps		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MPPC (Microsoft Point-to-point Compression)	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

**Table 4 Feature List by Feature Set for the Cisco 3600 Series (continued)**

Feature	In	Feature Set								
		IP	IP Plus	IP Plus IPsec 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise/ APPN Plus	Enterprise/ APPN Plus IPsec 56
MS Callback	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types	(3)	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
PPP over ATM		No	No	No	No	No	No	No	No	No
Stackable Home Gateway		No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Telnet Extensions for Dialout		No	No	No	No	No	No	No	No	No
X.25 Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 on ISDN		No	No	No	No	No	No	No	No	No
X.25 over ISDN D-Channel	(3)	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
X.28 Emulation		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

## New and Changed Information

The following sections list the new features supported by the Cisco 3600 series in Cisco IOS Release 11.3 T. For more information about these features, see the “Related Documentation” section on page 24.

### New Features in Release 11.3(7)T through Release 11.3(11)T

There are no new hardware or software features supported by the Cisco 3600 series in Cisco IOS Release 11.3(7)T through Release 11.3(11)T.

### New Software Feature in Release 11.3(6)T

The following new software feature is supported by the Cisco 3600 series in Cisco IOS Release 11.3(6)T and later releases.

#### Cisco Dial-Out Client

The Cisco Dial-Out Client allows modems connected to a router to be used transparently for dial-out from a LAN users desktop (using Microsoft Windows). This feature allows users to call the Internet and bulletin board services from their desktop, and allows faxing from the PC, using programs such as Winfax Pro.

The first version of Cisco Dial-Out Client has been available for some time now, supporting the Cisco 3600 series with asynchronous and sync/async network modules, connected to external data/fax modems. Now, in tandem with MICA Portware 2.5.1.0, V2 of the Cisco Dial-Out Client is available, adding support for the Cisco 3600 series integrated MICA modems for both dial-out and fax-out applications. This support allows the Cisco 3600 series with digital modems (using Cisco IOS Release 11.3(6)T and later to act as a dial-out server for LAN-attached PCs in branch offices.

## New Software Feature in Release 11.3(5)T

The following new software feature is supported by the Cisco 3600 series in Cisco IOS Release 11.3(5)T and later releases.

### V.90

56-kbps modem firmware (V.90) is available for the Cisco 3600 series beginning in Cisco IOS Release 11.3(5)T. V.90 is the new standard for 56k modem communication, and is an evolution from the older K56Flex and X2 protocols. This firmware update will allow 56K-enabled client modems to archive the maximum connect speeds possible using this new technology. Benefits include faster Web access, faster file download, and improved multimedia support. This firmware version is 2.5.1.0.

## New Hardware Feature in Release 11.3(4)T

The following new hardware feature is supported by the Cisco 3600 series in Cisco IOS Release 11.3(4)T and later releases.

### Eight New Enhanced PRI Network Modules

The following eight Enhanced PRI network modules were added to the Cisco 3600 series:

- NM-1FE1CT1—One-port 10/100BaseTX Ethernet with one-port T1 PRI/Channelized
- NM-1FE1CT1-CSU—One-port 10/100BaseTX Ethernet with one-port T1 PRI/Channelized with integrated CSU
- NM-1FE2CT1—One-port 10/100BaseTX Ethernet with two-port T1 PRI/Channelized
- NM-1FE2CT1-CSU—One-port 10/100BaseTX Ethernet with two-port T1 PRI/Channelized with integrated CSU
- NM-1FE1CE1B—One-port 10/100BaseTX Ethernet with one-port E1 PRI/Channelized Balanced mode (120 ohm)
- NM-1FE1CE1U—One-port 10/100BaseTX Ethernet with one-port E1 PRI/Channelized Unbalanced mode (75 ohm)
- NM-1FE2CE1B—One-port 10/100BaseTX Ethernet with two-port E1 PRI/Channelized Balanced mode (120 ohm)
- NM-1FE2CE1U—One-port 10/100BaseTX Ethernet with two-port E1 PRI/Channelized Unbalanced mode (75 ohm)

The Cisco 3600 series team is pleased to announce new enhanced versions of PRI Network Modules, now available with a integrated 10/100BaseTX Ethernet port. These network modules provide greater versatility, allowing for better slot efficiency and increased port densities when utilized in the Cisco 3600 series with Cisco IOS Release 11.3(4)T and later.

These new network modules, when combined with the Digital Modem network modules, provide hybrid ISDN/Analog dial access capabilities for the first time on the Cisco 3620, lowering the entry price for 1 PRI with 24/30 Digital Modems solution.

This network module can also be utilized in a Cisco 3640, allowing support for up to 8 PRI in a 2RU chassis.

## New Hardware Features in Release 11.3(3)T

The following new hardware features are supported by the Cisco 3600 series in Cisco IOS Release 11.3(3)T and later releases.

### 1-Port ATM-25 Network Module for the Cisco 3600 Series

The 1-port asynchronous transfer mode (ATM-25) network module provides connectivity to an external asynchronous digital subscriber line (ADSL) modem for Cisco series 3600 routers. This network module provides ATM traffic shaping for use with ADSL uplink speeds and protocol support for permanent virtual circuit (PVC) environments. This network module provides full support for multiprotocol encapsulation over ATM Adaptive Layer 5(RFC 1483), classic IP over ATM encapsulation (RFC 1577), and Cisco Point-to-Point Protocol (PPP) over ATM.

In the online feature description, Figure 1 shows the 1-port ATM-25 network module in a typical ADSL application environment. In this example, the network module and the associated Cisco 3640 router provide ATM connectivity to the ADSL modem and provide traffic shaping and protocol encapsulation for the downstream LAN clients.

### 1-Port High Speed Serial Interface (HSSI) Network Module

The Cisco 3600 series 1-port high-speed serial interface (HSSI) network module provides full-duplex connectivity at Synchronous Optical Network (SONET) OC-1/STS-1 (51.840 Mhz), T3 (44.736 MHz), and E3 (34.368 MHz) rates in conformance with the EIA/TIA-612 and EIA/TIA-613 specifications. The actual rate of the interface depends on the external data service unit (DSU) and the type of service to which it is connected. This 1-port HSSI network module can reach speeds of up to 52 Mbps in unidirectional traffic with 1,548-byte packets and 4,250 packets per second. Asynchronous Transfer Mode (ATM), ATM with Data Exchange Interface (DXI), High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), Frame Relay, and Switched Multi-Megabit Data Service (SMDS) WAN services are all fully supported.

The 1-Port HSSI network module provides the following benefits:

- Supports speeds up to 52 Mbps
- Supports a range of connectivity options: ATM, ATM with DXI, HDLC, Frame Relay, PPP, and SMDS
- Supports EIA/TIA-612 and EIA/TIA-613 specifications at T3, E3, SONET OC1/STS-1 and NCT1 substrates

### T1 CAS Support for the Cisco 3640 Digital Modem Network Module

The Digital Modem Network Module for the Cisco 3640 is a high-density digital network module containing, 6, 12, 18, 24, or 30 digital (MICA) modems. These modems, along with the T1 (or E1) port module, provide a direct digital connection to an Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) channel. The T1 CAS feature enables these network modules to support voice call transmission using channelized T1 lines (CT1) with channel associated signaling (CAS).

CAS is a form of signaling used on a T1 line. With CAS, a signaling element is dedicated to each channel in the T1 frame. This type of signaling is sometimes called Robbed Bit Signaling (RBS) because a bit is taken out (or robbed) from the user's data stream to provide signaling information to and from the switch. The T1 CAS feature enables the modems on the Digital Network Modem Module to receive and transmit incoming and outgoing call signaling (such as on-hook and off-hook) through each T1 controller that is configured for a channelized T1 line.

## New Software Features in Release 11.3(3)T

The following new software features are supported by the Cisco 3600 series in Cisco IOS Release 11.3(3)T and later releases.

### IBM SUPPORT:

#### RIF Passthrough in DLSw+

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

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

### MANAGEMENT:

#### VPDN MIB and Sys Log Facility

The Virtual Private Dialup Network (VPDN) Management Information Base (MIB) feature is intended to support all the tables and objects defined in "Cisco VPDN Management MIB" for the user sessions of the VPDN features. There are a number of commands which provide information and statistics through the Command Line Interface (CLI) but not Simple Network Management Protocol (SNMP); the Cisco VPDN MIB has been created to satisfy the need to provide information and statistics through SNMP.

### SECURITY:

#### Additional Vendor-Proprietary RADIUS Attributes

Remote Authentication Dial-In User Server (RADIUS) is an access server authentication, authorization, and accounting protocol originally developed by Livingston, Inc. Although an Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for

communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. In this release, Cisco IOS software introduces support for additional vendor-proprietary RADIUS attributes.

Users who have implemented security solutions using a vendor-proprietary implementation of RADIUS can now integrate Cisco access routers into their networks more easily.

For a complete list of supported IETF and vendor-proprietary RADIUS attributes, refer to the “RADIUS Attributes” appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*.

### Automated Double Authentication

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

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

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

### Certificate Authority Interoperability

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

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

### IPSec Network Security

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF).

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

IPSec provides the following network security services:

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

With IPSec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as virtual private networks (VPNs), extranets, and remote user access.

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

## Internet Key Exchange Security Protocol

ISAKMP/Oakley is a key management protocol which is used with the IPsec standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets.

IPsec can be configured without ISAKMP/Oakley, but ISAKMP/Oakley enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.

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

## MS-CHAP Support

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

MS-CHAP differs from the standard CHAP as follows:

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

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

Two new vendor-specific RADIUS attributes (IETF Attribute 26) were added to enable RADIUS to support MS-CHAP. For a complete list of supported IETF and vendor-proprietary RADIUS attributes, refer to the “RADIUS Attributes” appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*.

## Named Method Lists for AAA Authorization and Accounting

In earlier Cisco IOS releases, only named authentication method lists were supported under Cisco’s Authentication, Authorization, and Accounting (AAA) network security services. With Cisco IOS Release 11.3(4)T, AAA has been extended to support both authorization and accounting named method lists. Named method lists for authorization and accounting function the same way as those for authentication. They allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis.

### WAN OPTIMIZATION:

#### Always On/Dynamic ISDN (AO/DI)

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

### WAN SERVICES:

#### Microsoft Point-to-Point Compression (MPPC)

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

#### Multiple ISDN Switch Types

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

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

#### National ISDN Switch Types for Basic Rate and Primary Rate Interfaces

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces introduces changes to ISDN switch types for Primary Rate Interfaces (PRI) and Basic Rate Interfaces (BRI) as follows:

- Adds a new switch type for PRI interfaces (**isdn switch-type primary-ni**).
- Changes the BRI basic-ni1 switch type to basic-ni (**isdn switch-type basic-ni**).
- Removes the ISDN vn2 switch type (**isdn switch-type vn2**) used in France. The existing vn3 switch type (**isdn switch-type vn3**) supports French vn2 switches.
- Removes the ISDN basic-nwnet3 switch type (**isdn switch-type basic-nwnet3**) used in Norway. The basic-net3 switch type (**isdn switch-type basic-net3**) supports Norway NET3 switches.
- Removes the ISDN basic-nznet3 switch type (**isdn switch-type basic-nznet3**) used by New Zealand NET3 switches. The ISDN basic-net3 switch type (**isdn switch-type basic-net3**) supports New Zealand NET3 switches.

- Adds the ability to configure outgoing PRI B channel selection for the T1 controller in ascending order (channel 1 to channel 23) or descending order (channel 23 to channel 1). Previously, the router selected a B channel for outgoing calls from the highest free channel in descending order. The E1 controller channel selection for ascending order is channel 1 to 31, and 31 to 1 for descending order.

---

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

---

### X.25 over ISDN D-Channel

Basic Rate Interface (BRI) is an Integrated Systems Digital Network (ISDN) interface, and it consists of two B channels (B1 and B2) and one D channel. The B channels are used to transfer data, voice, and video. The D channel controls the B channels.

ISDN uses the D channel to carry signal information. ISDN can also use the D channel in a BRI to carry X.25 packets. The D channel has a capacity of 16 kbps, and the X.25 over D channel can use up to 9.6 kbps.

You can set the parameters of the X.25-over-D-channel interface without disrupting the original ISDN interface configuration. In a normal ISDN BRI interface, the D and B channels are bundled together and represented as a single interface. The original BRI interface continues to represent the D, B1, and B2 channels.

Because some end-user equipment uses static terminal endpoint identifiers (TEIs) to access this feature, static TEIs are supported. The dialer recognizes the X.25-over-D-channel calls and initiates them on a new interface.

X.25 traffic over the D channel can be used as a primary interface where low-volume, sporadic interactive traffic is the normal mode of operation. Supported traffic includes IPX, AppleTalk, transparent bridging, XNS, DECnet, and IP.

## New Hardware Feature in Release 11.3(2)T

The following new hardware feature is supported by the Cisco 3600 series in Cisco IOS Release 11.3(2)T and later releases.

### Digital Modem Network Module for the Cisco 3640

The Digital Modem Network Module for the Cisco 3640 is a high-density digital network module containing 6, 12, 18, 24, or 30 V.34+ (28.8 kbps) digital (MICA) modems. These modems provide a direct digital connection to an Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) channel. This digital modem network module allows you to support a mix of both digital (ISDN) and POTS analog modem calls over a single digital network interface.

Depending on the modem license you purchase with your Cisco 3640, the modems on the Digital Modem Network Module are either manageable or not manageable by Cisco IOS software commands. Manageable modems support the one out-of-band feature, which is used for gathering modem performance statistics and transmitting attention (AT) commands. If the license you purchase includes this modem management capability, you can use the modem management commands to gather call statistics and upgrade modem firmware for large modem pools.

## New Software Features in Release 11.3(2)T

The following new software features are supported by the Cisco 3600 series in Cisco IOS Release 11.3(2)T and later releases.

### Dialer Watch

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

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

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

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

- 1 Whenever a watched route is deleted, Dialer Watch checks to see if there is at least one valid route for any of the watched IP addresses defined.
- 2 If there is no valid route, the primary line is considered down and unusable.
- 3 If there is a valid route for at least one of the defined watched IP addresses, and if the route is pointing to an interface other than the backup interface configured for Dialer Watch, the primary link is considered up.
- 4 In the event that the primary link goes down, Dialer Watch is immediately notified by the routing protocol and the secondary link is brought up.
- 5 When the secondary link is up, at the expiration of each idle timeout, the primary link is rechecked.
- 6 If the primary link remains down, the idle timer is indefinitely reset.
- 7 If the primary link is up, the secondary backup link is disconnected. Additionally, a disable timer can be set to create a delay for the secondary link to disconnect, after the primary link is reestablished.

### MS Callback

The MS Callback feature provides client-server callback services for Microsoft Windows 95 and Microsoft Windows NT clients. MS Callback supports the Microsoft Callback Control Protocol (MSCB). MSCB is Microsoft's proprietary protocol that is used by Windows 95 and Windows NT clients. MS Callback supports negotiated PPP Link Control Protocol (LCP) extensions initiated and agreed upon by the Microsoft client. MS Callback is added to existing PPP Callback functionality. Therefore, if you configure your Cisco access server to perform PPP Callback using Cisco IOS Release 11.3(2)T or later, MS Callback is automatically available.

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

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

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

## PIM Version 2

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

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

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

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

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

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

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

### DRP Server Agent Enhancements

DRP Server Agent Enhancements—The DRP Server Agent is a Director Response Protocol (DRP) server application based on UDP for use only with Distributed Director. The DRP Server Agent will provide the following additional functionality:

- Enable the Distributed Director to use Border Gateway Protocol Multi-Exit Discriminators in traffic redirection decisions.
- Enable the DRP Server to measure client-to-server link latency (round-trip time) for use in traffic redirection decisions.

## Important Notes

### Image Deferral, Cisco IOS Release 11.3(8)T

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

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

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

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

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

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

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

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

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

On CCO, click on this path:

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

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

## Release 11.3(3a) Fixes Caveats CSCdk01707 and CSCdk08772

The Cisco 7500 RSP2 and RSP4 products in Cisco IOS Releases 11.3(1) through 11.3(3) were deferred due to a severe defect. It was determined that this caveat was significant enough to merit a software rebuild. The rebuild includes the caveat fix and is renumbered to 11.3(3a).

The defect is caveat CSCdk01707 and is described as follows:

- When the system gets an Error interrupt, a 4-byte IOS data area is accidentally overwritten. Because of this, the system may reload with a “Bus Error Exception” message. The error interrupt may be caused by events like an HSA Slave state transition on HSA systems, fatal system errors (like a parity error), or non-fatal errors (like a QAERROR with Null/reuse link error).

**Software Releases affected:** This caveat affects all systems configured with dual RSPs (HSA feature). All “v” images for the following Cisco IOS Releases have been deferred: 11.1(18.1)CA through 11.1(18.2)CA, 11.1(16.3)CC through 11.1(17.4)CC, 11.1(17)CT, 11.2(12.3)P through 11.2(13.4)P, 11.3(1) through 11.3(3), and 11.3(1)T through 11.3(3)T.

**Solution:** To eliminate the problems mentioned, we strongly recommend that you download and install one of the following Cisco IOS software release updates: 11.1(18)CA, 11.1(18)CC, 11.1(18)CT, 11.2(14)P, 11.3(3a) and 11.3(3a)T.

[CSCdk01707]

CSCdk08772 is a duplicate of CSCdk01707 and is described as follows:

- Dual RSPs in a High System Availability (HSA) configuration in a Cisco 7500 router will crash and reload in cycles during bootup when using the RSP-DSV Desktop/Plus/VIP image for versions later than 11.2(12a)P. [CSCdk08772]

CSCdk01707 was caused by CSCdj36366, which is described as follows:

- On RSP-based platforms, the message which reports a write bus error may report an incorrect value for the address of the bad access. [CSCdj36366]

Release 11.3(3a) and all subsequent releases of Cisco IOS Release 11.3 software include the fix for this caveat.

## Encryption Images

Encryption images are available in this Cisco IOS Release 11.3(4)T and later 11.3 T releases. See Table 1, “Memory Requirements for the Cisco 3600 Series”.

## New TACACS+ Attribute-Value (AV) Pair

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

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

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

### Bridge Multicast-Source Command

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

### 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* (78-4746-01). For complete documentation of all source-route bridging commands refer to the *Bridging and IBM Networking Command Reference* (78-4743-01). You may also obtain the most current documentation on the Documentation CD-ROM or Cisco Connection Online (CCO).

## Caveats

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

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

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

---

**Note** If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support: Online Technical Support: Software Bug Toolkit** or at <http://www.cisco.com/support/bugtools>.

---

## Related Documentation

The following sections describe the documentation available for the Cisco 3600 series. 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 only available online.

Use these release notes with these documents:

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

## Release-Specific Documents

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

- *Cross-Platform Release Notes for Cisco IOS Release 11.3*

On CCO:

**Service and Support: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3**

On the Documentation CD-ROM:

**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 on CCO:

**Service & Support: Technical Documents**

- Caveats document

On CCO:

**Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T**

On the Documentation CD-ROM:

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

---

**Note** If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support: Online Technical Support: Software Bug Toolkit** or at <http://www.cisco.com/support/bugtools>.

---

## Platform-Specific Documents

The documents listed below are available for the Cisco 3600 series routers. These documents are also available online at Cisco Connection Online (CCO) and on the Documentation CD-ROM.

- *Cisco 3600 Series Hardware Installation Guide*
- *Cisco 3620 Router Installation and Configuration Guide*
- *Cisco 3640 Router Installation and Configuration Guide*
- *Network Module Hardware Installation Guide*
- *Update to Network Module Hardware and Software Guides*
- *WAN Interface Cards Hardware Installation Guide*
- *Update to WAN Interface Cards Hardware Installation Guide*
- Cisco 3600 Series Configuration Notes
- Redundant Power Systems
- *Regulatory Compliance and Safety Info for the Cisco 3600 Series*
- Digital Modem Portware

- MICA portware release notes and AT command set
- Analog Modem Firmware
- Analog modem firmware release notes and AT command set
- *Cisco Modular Access Router Cable Specifications*
- Platform-specific release notes

On CCO:

**Service and Support: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers: Cisco 3600 Series Routers**

On the Documentation CD-ROM:

**Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 3600 Series Routers**

## Feature Modules

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

On CCO:

**Service and Support: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3T New Features**

On the Documentation CD-ROM:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3T New Features**

## Cisco IOS Software Documentation

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting document which are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

### Documentation Modules and Indexes

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, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Each configuration guide can be used with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master hot-linked indexes provide indexing information for the Cisco IOS software documentation set.

On CCO:

**Service and Support: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index**

On the Documentation CD-ROM:

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

To reach documentation related to an index entry, click on the page number following the entry.

## Release 11.3 Documentation Set

Table 5 details the contents of the Cisco IOS Release 11.3 software documentation set. The document set 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.

---

On CCO:

**Service and Support: Cisco IOS Software Configuration: Cisco IOS Release 11.3**

On the Documentation CD-ROM:

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

**Table 5 Cisco IOS Software Release 11.3 Documentation Set**

<b>Books</b>	<b>Chapter Topics</b>
<ul style="list-style-type: none"> <li>• Configuration Fundamentals Configuration Guide</li> <li>• Configuration Fundamentals Command Reference</li> </ul>	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management Interface Configuration System Management
<ul style="list-style-type: none"> <li>• Network Protocols Configuration Guide, Part 1</li> <li>• Network Protocols Command Reference, Part 1</li> </ul>	IP Addressing IP Services IP Routing Protocols
<ul style="list-style-type: none"> <li>• Network Protocols Configuration Guide, Part 2</li> <li>• Network Protocols Command Reference, Part 2</li> </ul>	AppleTalk Novell IPX
<ul style="list-style-type: none"> <li>• Network Protocols Configuration Guide, Part 3</li> <li>• Network Protocols Command Reference, Part 3</li> </ul>	Apollo Domain Banyan VINES DECnet ISO CLNS XNS

**Table 5 Cisco IOS Software Release 11.3 Documentation Set (continued)**

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• Wide-Area Networking Configuration Guide</li> <li>• Wide-Area Networking Command Reference</li> </ul>	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> <li>• Security Configuration Guide</li> <li>• Security Command Reference</li> </ul>	AAA Security Services Security Server Protocols Traffic Filtering Network Data Encryption Other Security Feature
<ul style="list-style-type: none"> <li>• Dial Solutions Configuration Guide</li> <li>• Dial Solutions Command Reference</li> </ul>	Business Applications and Scenarios Dial-In Terminal Service and Remote Node Configuration Dial Authentication Dial-on-Demand Routing Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Other Network Traffic on ISDN Channels Dial-Related Addressing Services
<ul style="list-style-type: none"> <li>• Cisco IOS Switching Services Configuration Guide</li> <li>• Cisco IOS Switching Services Command Reference</li> </ul>	Switching Paths NetFlow Switching Overview of Routing between Virtual LANs Routing between VLANs with ISL Encapsulation Routing between VLANs with IEEE 802.10 Encapsulation LAN Emulation (LANE) Overview LAN Emulation
<ul style="list-style-type: none"> <li>• Bridging and IBM Networking Configuration Guide</li> <li>• Bridging and IBM Networking Command Reference</li> </ul>	Bridging and IBM Networking Overview Bridging IBM Networking
<ul style="list-style-type: none"> <li>• Cisco IOS Software Command Summary</li> <li>• Dial Solutions Quick Configuration Guide</li> <li>• System Error Messages</li> <li>• Debug Command Reference</li> </ul>	

---

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

---

## Service and Support

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

---

**Note** If you purchased your product from a reseller, you can reach 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 the Cisco 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](http://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 the Cisco 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 ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it may 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 reach 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, select **Documentation**, and click **Enter the feedback form**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used with the documents listed in the "Related Documentation" section on page 24.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, *The Cell*, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9907R)

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

