Text Part Number: 78-5044-12

Release Notes for the Cisco 4000 Series for Cisco IOS Release 11.3

August 2, 1999

These release notes for the Cisco 4000 series support Cisco IOS Release 11.3, up to and including Release 11.3(11). These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, changes to the microcode or modem code and related document.

For a list of software caveats that apply to Release 11.3(11), see the "Caveats" section on page 18. The caveats are updated for every maintenance release.

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

Contents

These release notes describe the following topics:

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

Introduction

The Cisco 4000 series routers offer Flash memory EPROM technology as a standard feature. Flash memory EPROMs enable you to distribute new software releases from a central location. After the software is distributed, the routers can reboot from programs stored in local Flash memory.

All models provide a configurable modular router platform by using network processor modules (NPMs)—individual removable cards used for external network connections. Because the router's modules support many variations of protocols, line speeds, and transmission media, the Cisco 4000 series can accommodate all types of network computing environments. As Cisco introduces new modules, the Cisco 4000 series can be upgraded to keep pace with technological advances.

System Requirements

Memory Requirements

Table 1 Memory Requirements for the Cisco 4000 Series

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs From
Cisco 4000				
IP	c4000-i-mz	4 MB Flash	16 MB DRAM	RAM
IP Plus	c4000-is-mz	4 MB Flash	16 MB DRAM	RAM
IP Plus 40	c4000-is40-mz	4 MB Flash	16 MB DRAM	RAM
IP Plus 56	c4000-is56-mz	4 MB Flash	16 MB DRAM	RAM
IP/IPX/AT/DEC	c4000-d-mz	4 MB Flash	16 MB DRAM	RAM
IP/IPX/AT/DEC Plus	c4000-ds-mz	4 MB Flash	16 MB DRAM	RAM
Enterprise Plus	c4000-js-mz	8 MB Flash	16 MB DRAM	RAM
Enterprise Plus 40	c4000-js40-mz	8 MB Flash	16 MB DRAM	RAM
Enterprise Plus 56	c4000-js56-mz	8 MB Flash	16 MB DRAM	RAM
Enterprise/APPN Plus	c4000-ajs-mz	8 MB Flash	32 MB DRAM	RAM
Enterprise/APPN Plus 40	c4000-ajs40-mz	8 MB Flash	32 MB DRAM	RAM
Enterprise/APPN Plus 56	c4000-ajs56-mz	8 MB Flash	32 MB DRAM	RAM
Cisco 4000-M				
IP	c4000-i-mz	4 MB Flash	8 MB DRAM	RAM
IP Plus	c4000-is-mz	4 MB Flash	8 MB DRAM	RAM
IP Plus 40	c4000-is40-mz	4 MB Flash	16 MB DRAM	RAM
IP Plus 56	c4000-is56-mz	4 MB Flash	16 MB DRAM	RAM

Table 1 Memory Requirements for the Cisco 4000 Series (continued)

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs From
IP/IPX/AT/DEC	c4000-d-mz	4 MB Flash	8 MB DRAM	RAM
IP/IPX/AT/DEC Plus	c4000-ds-mz	4 MB Flash	16 MB DRAM	RAM
Enterprise Plus	c4000-js-mz	8 MB Flash	16 MB DRAM	RAM
Enterprise Plus 40	c4000-js40-mz	8 MB Flash	16 MB DRAM	RAM
Enterprise Plus 56	c4000-js56-mz	8 MB Flash	16 MB DRAM	RAM
Enterprise/APPN Plus	c4000-ajs-mz	8 MB Flash	32 MB DRAM	RAM
Enterprise/APPN Plus 40	c4000-ajs40-mz	8 MB Flash	32 MB DRAM	RAM
Enterprise/APPN Plus 56	c4000-ajs56-mz	8 MB Flash	32 MB DRAM	RAM
Cisco 4500, Cisco 4500-M, Cisco 4700				
IP	c4500-i-mz	4 MB Flash	16[1] MB DRAM	RAM
IP Plus	c4500-is-mz	4 MB Flash	16[2] MB DRAM	RAM
IP Plus 40	c4500-is40-mz	4 MB Flash	32 MB DRAM	RAM
IP Plus 56	c4500-is56-mz	4 MB Flash	32 MB DRAM	RAM
IP/IPX/AT/DEC	c4500-d-mz	4 MB Flash	16 MB DRAM	RAM
IP/IPX/AT/DEC Plus	c4500-ds-mz	8 MB Flash	16 MB DRAM	RAM
Enterprise Plus	c4500-js-mz	8 MB Flash	32 MB DRAM	RAM
Enterprise Plus 40	c4500-js40-mz	8 MB Flash	32 MB DRAM	RAM
Enterprise Plus 56	c4500-js56-mz	8 MB Flash	32 MB DRAM	RAM
Enterprise/APPN Plus	c4500-ajs-mz	8 MB Flash	32 MB DRAM	RAM
Enterprise/APPN Plus 40	c4500-ajs40-mz	8 MB Flash	32 MB DRAM	RAM
Enterprise/APPN Plus 56	c4500-ajs56-mz	8 MB Flash	32 MB DRAM	RAM

1 The IP feature set for Cisco 4500, Cisco 4500-M, and Cisco 4700 platforms for Release 11.3(4) had a required DRAM memory of 32 MB DRAM.

2 The IP Plus feature set for Cisco 4500, Cisco 4500-M, and Cisco 4700 platforms for Release 11.3(4) had a required DRAM memory of 32 MB DRAM.

Hardware Supported

Cisco IOS Release 11.3 supports the Cisco 4000 series routers:

- Cisco 4000, Cisco 4000-M
- Cisco 4500, Cisco 4500-M
- Cisco 4700

Table 2 Interfaces for the Cisco 4000 Series

Interface, Network Module, or Data Rate	Platforms Supported
LAN Interfaces	
ATM Interface	All Cisco 4000 series platforms
Ethernet (10BaseT)	All Cisco 4000 series platforms

Table 2 Interfaces for the Cisco 4000 Series

Ethernet (AUI)	All Cisco 4000 series platforms
Dual Ethernet Full-Duplex	Cisco 4500, Cisco 4500-M, Cisco 4700
Fast Ethernet (100BaseFX)	All Cisco 4000 series platforms
Fast Ethernet (100BaseTX)	All Cisco 4000 series platforms
FDDI DAS	All Cisco 4000 series platforms
FDDI multimode (DAS/SAS)	All Cisco 4000 series platforms
FDDI SAS	All Cisco 4000 series platforms
FDDI single-mode	All Cisco 4000 series platforms
16-Mbps Token Ring	All Cisco 4000 series platforms
4-Mbps Token Ring	All Cisco 4000 series platforms
WAN Data Rates	
48/56/64 kbps	All Cisco 4000 series platforms
1.544/2.048 Mbps	All Cisco 4000 series platforms
WAN Interfaces and Network Modules	
56K/64K DSU/CSU	All Cisco 4000 series platforms
Channelized E1	All Cisco 4000 series platforms
Channelized T1	All Cisco 4000 series platforms
E1-G.703/G.704	All Cisco 4000 series platforms
EIA/TIA-232	All Cisco 4000 series platforms
EIA/TIA-449	All Cisco 4000 series platforms
EIA/TIA-613 (HSSI)	All Cisco 4000 series platforms
EIA-530	All Cisco 4000 series platforms
ISDN BRI	All Cisco 4000 series platforms
ISDN PRI	All Cisco 4000 series platforms
MultiChannel Interface (Channelized E1/T1)	All Cisco 4000 series platforms
Serial	All Cisco 4000 series platforms
V.35	All Cisco 4000 series platforms
X.21	All Cisco 4000 series platforms

Determining the Version of Your Cisco IOS Software Release

To determine the version of Cisco IOS software running on your Cisco 4000 series router, log in to the router and use the **show version** EXEC command:

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) 4000 Software (C4000-JS-MZ), Version 11.3(11), RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information on upgrading to a new software release, see *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 **Cisco IOS Software Release 11.3 Upgrade Paths (#703: 12/97)**

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 4000 Series

Feature Set	Feature Set Matrix Term	Software Image	Platforms Supported
IP Standard Feature Sets			
IP	Basic[1]	c4000-i-mz	Cisco 4000, Cisco 4000-M
		c4500-i-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
IP Plus	Plus[2]	c4000-is-mz	Cisco 4000, Cisco 4000-M
		c4500-is-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
IP Plus 40	Plus, Plus 40[3]	c4000-is40-mz	Cisco 4000, Cisco 4000-M
		c4500-is40-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
IP Plus IPSec 56	Plus, Plus IPSec 56[4]	c4000-is56i-mz	Cisco 4000, Cisco 4000-M
		c4500-is56i-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
Desktop IBM Standard Feature Sets			
Desktop IBM (IP/IPX/AppleTalk/DEC)	Basic	c4000-d-mz	Cisco 4000, Cisco 4000-M
		c4500-d-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
Desktop IBM Plus (IP/IPX/AppleTalk/DEC Plus)	Plus	c4000-ds-mz	Cisco 4000, Cisco 4000-M
		c4500-ds-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
Enterprise Standard Feature Sets			
Enterprise Plus	Plus	c4000-js-mz	Cisco 4000, Cisco 4000-M
		c4500-js-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
Enterprise Plus 40	Plus, Plus 40	c4000-js40-mz	Cisco 4000, Cisco 4000-M
		c4500-js40-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
Enterprise Plus 56	Plus, Plus 56	c4000-js56-mz	Cisco 4000, Cisco 4000-M
		c4500-js56-mz	Cisco 4500, Cisco 4500-M, Cisco 4700

Table 3 Feature Sets Supported by the Cisco 4000 Series (continued)

Feature Set	Feature Set Matrix Term	Software Image	Platforms Supported
Enterprise/APPN Standard Feature Set			
Enterprise/APPN Plus	Plus	c4000-ajs-mz	Cisco 4000, Cisco 4000-M
		c4500-ajs-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
Enterprise/APPN Plus 40	Plus, Plus 40	c4000-ajs40-mz	Cisco 4000, Cisco 4000-M
		c4500-ajs40-mz	Cisco 4500, Cisco 4500-M, Cisco 4700
Enterprise/APPN Plus 56	Plus, Plus 56	c4000-ajs56-mz	Cisco 4000, Cisco 4000-M
		c4500-ajs56-mz	Cisco 4500, Cisco 4500-M, Cisco 4700

1 This feature set matrix term is offered in the Basic feature set.
2 This feature set matrix term is offered in the Plus feature set.
3 This feature set matrix term is offered in the encryption feature sets which consist of 40-bit (Plus 40) data encryption feature sets.
4 This feature set matrix term is offered in the encryption feature sets which consist of 56-bit (Plus 56) data encryption feature sets.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit (3DES) 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 e-mail to export@cisco.com.

Table 4 and Table 5 list the features and feature sets supported in Cisco IOS Release 11.3(11) by the Cisco 4000/4000-M and Cisco 4500/4500-M/4700/4700-M routers, respectively. Both tables use 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.

Note These feature set tables contain only a selected list of features. The tables are not a cumulative or complete list of all the features in each image.

Table 4 Feature List by Feature Set for the Cisco 4000 and Cisco 4000-M Routers

	Feature Set								
Feature	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/AT / DEC Plus	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus 56
IBM Support									
APPN High-Performance Routing	No	No	No	No	No	No	No	No	No
APPN MIB Enhancements	No	No	No	No	No	No	No	No	No

Table 4 Feature List by Feature Set for the Cisco 4000 and Cisco 4000-M Routers (continued)

Feature	Feature Set								
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/AT / DEC Plus	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus 56
APPN over Ethernet LAN Emulation	No	No	No	No	No	No	No	No	No
APPN Scalability Enhancements	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
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	Yes	No	Yes	Yes	Yes	Yes
FRAS Enhancements: — FRAS Boundary Network Node Enhancement — FRAS Dial Backup over DLSw+ — FRAS DLCI Backup — FRAS Host — FRAS MIB — SRB over Frame Relay	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
SRB over FDDI	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
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	Yes	No	Yes	Yes	Yes	Yes
Internet									
DRP Server Agent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Routing									
Easy IP (Phase 1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 4000 and Cisco 4000-M Routers (continued)

Feature	Feature Set								
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/AT / DEC Plus	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus 56
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations	No	No	No	No	No	No	No	No	No
IP Enhanced IGRP Route Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Enhancements: — TCP Selective Acknowledgment — TCP Timestamp	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN Support									
AppleTalk Access List Enhancements	No	No	No	No	Yes	Yes	Yes	Yes	Yes
DECnet Accounting	No	No	No	No	Yes	Yes	Yes	Yes	Yes
IPX Named Access Lists	No	No	No	No	Yes	Yes	Yes	Yes	Yes
IPX SAP-after-RIP	No	No	No	No	Yes	Yes	Yes	Yes	Yes
NLSP Enhancements	No	No	No	No	No	No	Yes	Yes	Yes
NLSP Multicast Support	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Management									
Cisco Call History MIB Command-Line Interface	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
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
Virtual Profiles	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia									
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
Stub IP Multicast Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quality of Service									
RTP Header Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security									
Double Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encrypted Kerberized Telnet	No	No	No	No	No	No	No	No	Yes
HTTP Security	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	No	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 4000 and Cisco 4000-M Routers (continued)

Feature	Feature Set								
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/AT / DEC Plus	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus 56
Vendor-Proprietary RADIUS Attributes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching									
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs	No	No	No	No	No	No	No	No	No
CLNS and DECnet Fast Switching over PPP	No	No	No	No	No	No	Yes	Yes	Yes
DECnet/VINES/XNS over ISL: — Banyan VINES Routing over ISL Virtual LANs — DECnet Routing over ISL Virtual LANs — XNS Routing over ISL Virtual LANs	No	No	No	No	No	No	Yes	Yes	Yes
Fast-Switched Policy Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs	No	No	No	No	No	No	No	No	No
VIP Distributed Switching Support for IP Encapsulated in ISL	No	No	No	No	No	No	No	No	No
Terminal Services									
Virtual Templates for Protocol Translation	No	No	No	No	No	No	Yes	Yes	Yes
WAN Optimization									
ATM MIB Enhancements	No	No	No	No	No	No	No	No	No
PAD Enhancements	No	No	No	No	No	No	Yes	Yes	Yes
PAD Subaddressing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services									
Bandwidth Allocation Control Protocol	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	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Caller ID Callback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Forwarding—Fast Switching	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Leased-Line ISDN at 128 kbps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP over ATM	No	No	No	No	No	No	No	No	No
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

Table 4 Feature List by Feature Set for the Cisco 4000 and Cisco 4000-M Routers (continued)

Feature	Feature Set								
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/AT / DEC Plus	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus 56
X.25 on ISDN	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

Table 5 Feature List by Feature Set for the Cisco 4500, 4500-M, 4700, and 4700-M Routers

Feature	Feature Set											
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus 56	Enter-prise/ APPN Plus	Enter-prise/ APPN Plus 40	Enter-prise/ APPN Plus 56
IBM Support												
APPN High-Performance Routing	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
APPN MIB Enhancements	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
APPN over Ethernet LAN Emulation	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
APPN Scalability Enhancements	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
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	Yes	Yes
Cisco MultiPath Channel (CMPC)	No	No	No	No	No	No	No	No	No	No	No	No

Table 5 Feature List by Feature Set for the Cisco 4500, 4500-M, 4700, and 4700-M Routers (continued)

Feature	Feature Set											
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus 56	Enter-prise/ APPN Plus	Enter-prise/ APPN Plus 40	Enter-prise/ APPN Plus 56
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	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FRAS Enhancements: — FRAS Boundary Network Node Enhancement — FRAS Dial Backup over DLSw+ — FRAS DLCI Backup — FRAS Host — FRAS MIB — SRB over Frame Relay	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SRB over FDDI	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TN3270 LU Nailing	No	No	No	No	No	No	No	No	No	No	No	No
TN3270 Server Enhancements	No	No	No	No	No	No	No	No	No	No	No	No
Token Ring LANE	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunneling of Asynchronous Security Protocols	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 4500, 4500-M, 4700, and 4700-M Routers (continued)

Feature	Feature Set											
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise Plus	Enterprise Plus 40	Enterprise Plus 56	Enterprise/ APPN Plus	Enterprise/ APPN Plus 40	Enterprise/ APPN Plus 56
Internet												
DRP Server Agent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Routing												
Easy IP (Phase 1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Enhanced IGRP Route Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Enhancements: — TCP Selective Acknowledgment — TCP Timestamp	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN Support												
AppleTalk Access List Enhancements	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DECnet Accounting	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Named Access Lists	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX SAP-after-RIP	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NLSP Enhancements	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
NLSP Multicast Support	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management												
Cisco Call History MIB Command-Line Interface	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS Internationalization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB, Phase 1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv2C	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Profiles	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 4500, 4500-M, 4700, and 4700-M Routers (continued)

Feature	Feature Set											
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise Plus	Enterprise Plus 40	Enterprise Plus 56	Enterprise/ APPN Plus	Enterprise/ APPN Plus 40	Enterprise/ APPN Plus 56
Multimedia												
IP Multicast Load Splitting across Equal-Cost Paths	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast over ATM Point-to-Multipoint Virtual Circuits	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast over Token Ring LANs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stub IP Multicast Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quality of Service												
RTP Header Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security												
Double Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encrypted Kerberized Telnet	No	No	No	No	No	No	No	No	Yes	No	No	Yes
HTTP Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Per-User Configuration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reflexive Access Lists	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Intercept	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Vendor-Proprietary RADIUS Attributes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching												
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CLNS and DECnet Fast Switching over PPP	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
DECnet/VINES/XNS over ISL: — Banyan VINES Routing over ISL Virtual LANs — DECnet Routing over ISL Virtual LANs — XNS Routing over ISL Virtual LANs	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 4500, 4500-M, 4700, and 4700-M Routers (continued)

Feature	Feature Set											
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enterprise Plus	Enterprise Plus 40	Enterprise Plus 56	Enterprise/ APPN Plus	Enterprise/ APPN Plus 40	Enterprise/ APPN Plus 56
Fast-Switched Policy Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VIP Distributed Switching Support for IP Encapsulated in ISL	No	No	No	No	No	No	No	No	No	No	No	No
Terminal Services												
Virtual Templates for Protocol Translation	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
WAN Optimization												
ATM MIB Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PAD Enhancements	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
PAD Subaddressing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services												
Bandwidth Allocation Control Protocol	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced Local Management Interface (ELMI)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay MIB Extensions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Router ForeSight	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Advice of Charge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Caller ID Callback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Forwarding—Fast Switching	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Leased-Line ISDN at 128 kbps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP over ATM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Telnet Extensions for Dialout	No	No	No	No	No	No	No	No	No	No	No	No

Table 5 Feature List by Feature Set for the Cisco 4500, 4500-M, 4700, and 4700-M Routers (continued)

Feature	Feature Set											
	IP	IP Plus	IP Plus 40	IP Plus 56	IP/ IPX/ AT/ DEC	IP/ IPX/ AT/ DEC Plus	Enter-prise Plus	Enter-prise Plus 40	Enter-prise Plus 56	Enter-prise/ APPN Plus	Enter-prise/ APPN Plus 40	Enter-prise/ APPN Plus 56
X.25 Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 on ISDN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Switching between PVCs and SVCs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.28 Emulation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

New and Changed Information

Cisco IOS Release 11.3(1) and all later releases support features in the following categories:

- IBM Support
- Internet
- LAN Support
- Management
- Multimedia
- Quality of Service
- Security
- Switching
- Terminal Services
- WAN Optimization
- WAN Services

For more information about new features, see the “Related Documentation” section on page 33.

Important Notes

The following sections contain important notes about Cisco IOS Release 11.3 and can apply to the Cisco 4000 series.

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 following maintenance releases scheduled on the EOE date are 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, see *End of Sales and End of Engineering for Cisco IOS Software Releases* product bulletin on CCO.

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

Service & Support: Product Bulletins: Software

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

Booting Cisco 4000 Series Routers

You must use the Cisco IOS Release 9.14 rxboot image for Cisco 4000 series routers because the Release 11.0 rxboot image is too large to fit in the ROMs. (Note that rxboot image size is not a problem for Cisco 4500 series routers.) However, because the Release 9.14 rxboot image does not recognize new network processor modules, such as the Multiport Basic Rate Interface (MBRI), its use causes two problems:

- You cannot boot from a network server over BRI lines. Instead, you can only boot from a network server over other media or use the **copy tftp flash** command to copy images over BRI or other media to Flash memory. If you use the **copy tftp flash** command over a BRI interface, you must be running the full system image.
- If you use the rxboot image on a Cisco 4000 series router that is already configured, the following error messages are displayed, with one pair of messages for each BRI interface configured:

```
Bad interface specification
No interface specified – IP address
Bad interface specification
No interface specified – IP address
```

Enabling IPX Routing

The Token Ring interface is reset whenever IPX routing is enabled on that interface.

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 (AARP) table in any AppleTalk node that is performing MAC-address gleaning.

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 Cisco Connection Online (CCO) or on the Documentation CD-ROM.

New TACACS+ Attribute-Value 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 {

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 4700 series routers, and Cisco 7000 and 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 prior to Version 2.5.
- The LS2020 cannot be used 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.
- HSRP is supported.
- LANE does not support CLNS or LANE over PVCs.
- AppleTalk Phase 1 cannot be routed to AppleTalk Phase 2 via LANE.

Using Source-Route Transparent Bridging and Source-Route Bridging on Cisco 2500 and Cisco 4000 Series Routers

Certain products containing the Texas Instruments TMS380C26 Token Ring controller do not support source-route transparent bridging (SRT). SRT is the concurrent operation of Source Router Bridging (SRB) and transparent bridging on the same interface. The affected products, shipped between March 30, 1994 and January 16, 1995, are the Cisco 4000 NP-1R, Cisco 4000 NP-2R, Cisco 2502, Cisco 2504, Cisco 2510, Cisco 2512, Cisco 2513, and Cisco 2515.

Units shipped before March 30, 1994 or after January 16, 1995, are not affected. They use the Texas Instruments TMS380C16 Token Ring controller, which supports SRT.

SRT support is necessary in two situations:

- Token Ring networks are configured to SRB protocols such as SNA and NetBIOS, and they transparently bridge other protocols, such as IPX.
- SNA or NetBIOS uses SRB, and Windows NT is configured to use NetBIOS over IP. Certain other configuration alternatives do not require SRT. (Contact the Technical Assistance Center for more information.)

Beginning with Cisco IOS Release 10.3(1), SRB in the following Cisco IOS feature sets is no longer supported:

- IP, IP/IPX
- Desktop

To use SRB, you need one of the following feature sets:

- IP/IBM base
- IP/IPX/IBM base
- IP/IPX/IBM/APPN
- Desktop/IBM base
- Enterprise
- Enterprise/APPN

In most non-IBM Token Ring environments, the multiring feature in IP, IP/IPX, and Desktop eliminates the need for IP/IBM base, IP/IPX/IBM base, IP/IPX/IBM/APPN, Desktop/IBM base, Enterprise, or Enterprise/APPN.

Caveats

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

This section only contains open and resolved caveats for the current Cisco IOS maintenance release.

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

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.

Caveats for Release 11.3(1) through 11.3(11).

This section describes possibly unexpected behavior by Release 11.3(11). Unless otherwise noted, these caveats apply to all 11.3 releases up to and including 11.3(11).

Access Server

- CSCdk02299

  Cable length options are missing for T1 lines on Cisco AS5200 access servers. The options exist for Cisco AS5300 access servers in Cisco IOS Releases 11.2 and 11.3.

  Cisco should remove conditional compile and provide similar functionality.

Basic System Services

- CSCdj14601

  When hardware compression is enabled, packets are normally fast switched. If the user turns fast switching off and then back on, fast switching remains disabled.

  Workaround is to reconfigure compression by using the **no compress** and then the **compress stac** commands.

- CSCdk18966

  When configured for SDLC, serial ports on a Cisco MC3810 may report input abort errors when the clock rate is greater than 38,400 bps. These errors do not affect performance; they are not typically input aborts. This problem does not result in retransmitted frames, and there is no performance impact.

- CSCdk75925

  All router interfaces are reset with their states changing from up to down and then back to up again. The cause for the restart is:

  ```
  System restarted by error - an arithmetic exception, PC 0x6016B6E0
  ```

- CSCdm11401

  When doing FRF.9 compression with the CSA, it may be impossible to compress packets with certain repetitive patterns. The CSA can decompress these same packets.

- CSCdm14585

  A router running Cisco IOS Release 11.3(8) may experience a software forced crash caused by memory corruption.

- CSCdm70109

  After a succesful completion of the SNMP poll to the CISCO-MEMORY-POOL-MIB on a Cisco AS5800 access server, the poll may fail for several minutes before it becomes available again.

IBM Connectivity

- CSCdm08494

  A Cisco 3600 series router running Cisco IOS Release 11.3 T may restart with either the following bus error or a software forced crash when running BSTUN. There is no workaround.

  ```
  System restarted by error - a Software forced crash, PC 0x601C4398
  System image file is "flash:c3640-is-mz.113-4", booted via flash
  ```

- CSCdm37638

  Some Cisco 4500 and 4700 series routers with a 2-Port Token Ring Network Processor Module (NP-2R) hang once a week displaying a "%SYS-2-INPUTQ: INPUTQ set, but no IDB" message. All revision levels of the motherboard are affected.

- CSCdm55118

  An APPN Network Node (NN) router has consumed 40 MB for the APPN process.

- CSCdm58166

  A BSTUN router running Cisco IOS Release 11.3(10) hangs and crashes. No workaround is available.

- CSCdm59018

  When configuring for FRAS BAN with DDR backup, the backup is only driven if the primary interface goes to the down/down state. If the DLCI is lost, the interface goes to the up/down state and the backup is not driven.

- CSCdm59024

  This problem concerns a Cisco 4700 series router defined as APPN NN with an APPN link across Frame Relay RFC 1490 to an IBM NN950 configured as a NN. Occasionally, when the DLCI fails, the APPN link does not restart, even though the router is configured to retry infinitely.

- CSCdm64065

  No SNA traffic passes between a server and a Cisco Network Node router because the Network Node was using DLSw flow control to disallow the sending of further SNA traffic by the server.

Interfaces and Bridging

- CSCdk93782

  A Cisco 7500 series router running Cisco IOS Release 11.3(7) does not crash, but the Fast Ethernet interface goes down with the following message.

```
%SYS-2-QCOUNT: Bad dequeue 611E3EBC count -1 -Process= "<interrupt
level>", ipl= 6
6d18h: %ALIGN-3-SPURIOUS:
Spurious memory access made at 0x601A35D8 reading 0x1C 6d18h
Interface FastEthernet12/1, changed state to down
Line protocol on Interface FastEthernet12/0,changed state to up
```

  The only way to bring the router up is to reload it.

  Possible workaround: Disable weighted fair-queue.

- CSCdm42807

  A Cisco router running BSC/BSTUN on a PowerQUICC serial interface at half-duplex causes bad queue error messages.

  Workarounds:

  — Configure the interface for full-duplex operation by using the **full-duplex** command.

  — If half-duplex operation is required, disable the RTS timer for the interface by using the **half-duplex timer rts-timeout 0** command.

- CSCdm61507

  When a router is configured for FRF.9 compression, input packets are counted twice: once in compressed format and again in uncompressed format.

  For every received packet the “input pkts” and the “in bytes” fields (in output from the **show frame pvc** command) are invalid.

  Workaround: Disable FRF.9 compression by using the **no frame-relay ip** *ip-address* command.

IP Routing Protocols

- CSCdj45202

  The new **ip spd mode aggressive** configuration command is available. When configured, all IP packets that fail sanity check (such as “bad checksum not version 4” and “bad TTL”) are dropped aggressively to guard against bad IP packets spoofing. The **show ip spd** command displays whether aggressive mode is enabled or not. SPD random drop in RSP is supported.

  When enabled, Selective Packet Discard (SPD) now works as follows:

  — When the **ip spd mode aggressive** command is issued, IP packets that fail sanity checks are classified as aggressive droppable packets.

- When the IP input queue reaches the SPD min-threshold (specified by the **ip spd queue min-threshold** *min* command), all aggressive droppable packets are dropped immediately while normal IP packets (not high-priority SPD packets) are dropped with increasing probability as the length of the IP input queue grows.
- When the IP input queue reaches the SPD max-threshold (specified by the **ip spd queue max-threshold** *max* command), all normal IP packets are dropped at 100 percent.
- The default SPD min-threshold is 10, and the default max-threshold is 75.

To avoid an input interface that takes too many router resources, new packets (SPD or non-SPD) received from that interface are dropped when the interface has more than the input hold queue limit of input packets in the router.

- CSCdm16194

  EIGRP does not trigger the selection of a new route when one of the less favorable or equal paths is removed from the routing table. The route disappears but no new route is selected from the topology table.

- CSCdm44976

  IP access lists always permit IP fragments.

  There is no workaround for this problem.

- CSCdm51483

  Using the **show ip igmp group** command may cause a bus error reload if an IGMP entry is deleted during the execution of the **show ip igmp group** command.

  There is no workaround.

Miscellaneous

- CSCdj08265

  A BRI leased line interface on a Cisco 3600 series router that has been configured for XNS may not transfer data.

  Workaround: Clear the interface or reload the router following the configuration change.

- CSCdj68910

  When you have two simultaneous accesses to NVRAM (for example, one access from the console and another access from a Telnet session), one session might attempt to issue the **show configuration** command and might pause at the More prompt while the other session issues the **write memory** command. This problem is unlikely during normal router usage. There is no workaround.

- CSCdk12891

  While waiting for a crypto key exchange session with a Telnet session into the router, the user cannot abort the crypto key exchange session.

Workaround: Enter the **show tcp bri** and **clear tcp tcb** commands in the following manner:

```
router(config)#crypto key-ex passive
Enter escape character to abort if connection does not complete.
Wait for connection  from peer[confirm]
Waiting ....

telnet> quit
Connection closed.
janedoe@janedoe-ultra:/users/janedoe> telnet router
Trying 171.21.114.109...
Connected to router.cisco.com.
Escape character is '^]'.

User Access Verification
Password:
router>enable
Password:

router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#crypto key-ex passive
TCP bind failed: Address already in use

router(config)#exit
router#show tcp bri
TCB Local Address Foreign Address (state)
60C3DF74 router.cisco.com.23 janedoe-ultra.ci.42272 ESTAB
60A23A24 router.cisco.com.23 janedoe-ultra.ci.42271 CLOSEWAIT
router#clear tcp tcb
60A23A24
[confirm]
[OK]
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#crypto key-ex passive
Enter escape character to abort if connection does not complete.
Wait for connection from peer[confirm]n
router(config)#
```

- CSCdk55110

  When tunneling IPX over an IP tunnel and using an extended inbound access list for IP on the tunnel interface, the IPX traffic is blocked by the access list.

  Workaround is to add the **permit gre** command to the extended access list.

- CSCdk56600

  The Ascend-Idle-Limit attribute is defined as a value in seconds. However, when it is applied to a client using PPP interactive mode, the attribute is interpreted as a value in minutes.

  This attribute works properly in PPP dedicated mode.

- CSCdk57206

  When printing is performed over asynchronous lines by using software flow control, large numbers of overruns occur.

- CSCdk61320

  When you perform an encrypted Kerberized Telnet to a Cisco 7500 series router, the initial setup works properly, but nonsense output results when the decryption of packets from the router occurs on the client side. There is no workaround.

- CSCdk62335

  Cisco encryption crashes the router when it is used over an ISDN backup line.

- CSCdk70846

  Using the **clear vpdn tunnel** command for a tunnel using L2F protocol sends individual close packets for all L2F sessions (Mids), rather than a single close packet for the tunnel itself. This results in congestion on the WAN interfaces on the requesting peer. Simultaneously, the receiving peer is not able to keep up with the flood of multiple L2F close packets—resulting in dropped packets, interface throttle, and the remaining Mids taking a long time to idle out and eventually close.

- CSCdk72937

  A Cisco 2600 series router with an E1 balanced network module may inadvertently reload. There is no workaround.

- CSCdk73369

  Under heavy uses of L2F VPDN configurations on Cisco access servers, some virtual-access interfaces do not have a corresponding MID (L2F session) entry.

  Turning on the **debug vpdn l2x-error** command shows messages similar to the these:

  ```
  *Dec 9 20:37:59.421: Vi291 L2X: Discarding packet because of no mid/session *Dec 9
  20:37:59.421: Vi419 L2X: Discarding packet because of no mid/session *Dec 9
  20:37:59.421: Vi169 L2X: Discarding packet because of no mid/session *Dec 9
  20:37:59.421: Vi36 L2X: Discarding packet because of no mid/session
  ```

  Other problems also may cause these messages.

- CSCdk88739

  When a hub-and-spoke frame relay configuration is run and the hub router is set as a multipoint interface, DHCP requests fail.

  Workaround: Configure both the hub and the spoke to use point-to-point subinterfaces.

- CSCdm05125

  A Cisco 3640 router with BRI interfaces locks up every two weeks. Approximately six hours prior to lockup, ISDN dial-in users notice a significant slowdown in transfer rates. When the router locks up, it continuously displays the message below.

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=0, count=0 -Traceback= 601AA500
  600B55C8 600B9F64
  ```

  At this point, the router does not respond to console or Telnet input. Even though the indicator LEDs show steady traffic, the router also does not route any packets. The router must be reloaded to recover.

  There is no workaround.

- CSCdm37466

  Spurious accesses and router hangs can occur when using fair queuing.

- CSCdm59007

  SNA packets are dropped and not forwarded over a 64 KB leased line with HDLC encapsulation. There is no workaround.

- CSCdm59013

  A Cisco 3640 router is unable to use E&M ports and displays the following message "error C542-1 to big rxx port 1/1/1 pkt (size 41318) to big."

- CSCdm66536

  A Bus error occurs during the scheduler process.

Protocol Translation

- CSCdm69108

  TCP to X.25 PVC translation does not work.

Wide-Area Networking

- CSCdi70242

  Two Cisco 4500 series routers connected using back-to-back E1 controllers are running PPP. When an FAS alarm is generated, PPP reliable does not reconnect. When an AIS alarm is generated, PPP reliable reconnects.

  This problem only affects the PPP reliable protocol. No other protocols, such as HDLC, are affected.

- CSCdi81986

  No packets can be forwarded over synchronous DDR lines with X.25/X.25-IETF encapsulation. There is no workaround.

- CSCdj39383

  A router with over 180 DLCIs cannot boot properly because of excessive console log messages related to the startup of Frame Relay PVCs.

- CSCdj51284

  Some protocol translation configurations produce "%ALIGN-3-SPURIOUS: ..." messages, usually when a PPP over LAT session is terminated ungracefully.

- CSCdk09757

  The input queue of an ATM interface on a Cisco 7200 series router slowly fills with Novell packets. These packets are visible in the output of the **show buffer old packet** command. It can take days for the input queue to completely fill up and prevent input of any packets on that interface.

  Workaround: Monitor the router and reload it before the input queue gets wedged (as indicated by 76/75 in the output of the **show interface** command). Increasing the size of the input queue can delay the wedge.

- CSCdk24781

  When using X.25 encapsulation, the serial interface input queue shows a negative value.

- CSCdk53602

  When an X.25 host sends a "set parameters" packet assembler/disassembler (PAD) message followed by several octets for X.3 parameters (1 through 18) to a Cisco router acting as a PAD, the parameter setting "6=1" is improperly rejected by the router.

Parameter 6 is control of PAD service signals. Value 1 is PAD service signals are transmitted in the standard format.

Workaround: Locally preset parameter 6 to value 1 before making the call to the X.25 host. Then the Cisco router acting as a PAD will accept the X.3 parameters coming from the X.25 host.

- CSCdk66742

  A Cisco 2500 series router's async line may hang when a PAD call is not cleared correctly. Clearing the line does not solve the problem. This has been observed in Cisco IOS Release 11.3(6). Restarting the router is the only workaround.

- CSCdk72835

  A Cisco 3600 series router with a WIC-1T serial interface experiences instability when Adtran TSU 100 or TSU 600 devices are attached. Customers have seen slowness and retransmissions of packets or flapping of the leased line.

- CSCdm10918

  When configuring PPP multilink on a router running Cisco IOS Release 11.3(7)T, the different B channels on an E1 hang. When running Release 11.3(8)T, the problem seems to be limited to one B channel. When PPP multilink is not used, the problem does not appear.

- CSCdm21174

  A Cisco 7200 series router crashed due to memory corruption caused by large numbers of protocol translations.

- CSCdm28510

  Adding the **dialer isdn short-hold** command to the map-class dialer to optimize ISDN costs based on AOC-D messages breaks the dialer idle-timeout. This means that:

  1) The idle timer resets to 4294966 seconds when expiring and does not disconnect the ISDN call.
  2) The short-hold timer gets incremented on receipt of an AOC-D message and never disconnects an ISDN call either.

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

- CSCdm37706

  On a BRI that is used for backup of a serial interface, when standby time arrives, a disconnect on q931 is never sent. The ISDN switch needs to declare that remote TE is out of order.

- CSCdm46165

  A router intermittently displays the "%TCP-2-INVALIDTCPENCAPS" message.

- CSCdm47600

  Although BRI is used as a backup and the dialer interface is in stanby, the router will make an ISDN call.

  This call should never occur because the leased lines are up and no backup is needed.

  Both rotary groups and dialer profiles result in the same problem.

- CSCdm49685

  After reloading a router, the ATM interfaces assumes the default UNI value (3.0) instead of the actual configuration.

  Workaround: Reset the interface by using the **shutdown** and **no shutdown** commands.

- CSCdm58042

  When doing TCP to X.25 translation, the router does not negotiate X.3 parameters with the PAD, and the whole session drops after a couple of seconds.

- CSCdm69357

  ATCP (appletalk) negotiation over asynchronous PPP fails. There is no workaround. Cisco IOS Releases 11.2(19)P and 11.1(24) exibit the same problem.

Caveats for Release 11.3(1) through 11.3(10).

This section describes possibly unexpected behavior by Release 11.3(10). Unless otherwise noted, these caveats apply to all 11.3 releases up to and including 11.3(10). For additional caveats applicable to Release 11.3(10), 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(11).

Basic System Services

- 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 here 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.

  The **show user** command has been modified, so that the user field is filled up by the host name.

  The **no-enable** and **high-security** keywords have been added to the **sna host** and **dspu host** commands. These keywords must be configured with focalpoint and are defined as follows:

  no-enable: Does not allow enable commands from the host.

  high-security: Allows the following commands in user EXEC mode. (Privileged EXEC mode is not affected by this option.)

  Note All these commands have to be entered in full or they will not be allowed.

  For example, **sh ver** is not allowed as an abbreviation for the **show version** command.

  — **enable**

  — **quit**

  — **exit**

  — **show ?**

- CSCdm02753

  A Cisco 7200 series router with an encryption card (ESA) reloads periodically. No workaround is available.

- CSCdm26534

  On a Cisco 7200 series routers running Cisco IOS Release 11.3(7)T, the EnvMonTemperature trap value sent for the temperature sensor at chassis outlet 3 is incorrect.

- CSCdm45535

  A Cisco 7500 series router can erroneously detect output stuck conditions, which causes interfaces to reset or perform cBus restarts and all IPs on the router to reset.

DECnet

- CSCdk23805

  When DECnet accounting is implemented, the router may crash, depending on the number of connections.

- CSCdm28939

  During configuration of DEC net on a router, it is possible to specify an address translation gateway (ATG) network number in the range 0 to 3. If the *atg-network-number* argument is specified incorrectly while configuring an interface, the router will reload.

  Workaround: Ensure that the *atg-network-number* argument 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

  A router crashes when using the **username** command under the following conditions:

  If you enter a long username, type a shortened form of the **password** keyword, and press the Tab key to complete the **password** keyword, the router crashes.

IBM Connectivity

- CSCdm30793

  A Cisco 7206 router running Cisco IOS Release 11.3(9)T configured for DLSw priority peers may crash with a bus error. There is no workaround.

- 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:
32730770000000000F7C1000000008000010B5100050000000000007000E11F4C4C5C2E5D4E4F0F04BD5D5C
3C9D7F0F110380037110C0804F1F2F0F0F0F00908F0F0F0F0F0F0F01406C3C9E2C3D640C1D7D7D540D5D561
```

```
C4D3E4D90F0FC3C9E2C3D640C1D7D7D540D5D52207000000083E0001
%APPN-3-logcsCS_XXXXIP11_LOGMSG_05: CS - Associated inbound XID data in alert (length
>= 29):
%APPN-3-Error:
326705D56F010000B008100000000000000010B410005B8000000000700103700231l0C0804F0F3F0F0F0F00
F06D4E240E2D5C140E2C5D9E5C5D90908F0F0F0F0F0F0F0131103100010F0F0F0F0F0F0F0F0F0F0F00E
0FF4C4C5C2E5D4E4F0F04BC3E3F5F6C6
```

Workaround: Disable console logging.

- CSCdm49573

  The router crashes with a bus error when executing the **show dlsw circuit** command, and there is a circuit with a local RIF of 18 bytes.

  This is a regression introduced by CSCdk83294.

- CSCdm50361

  DLSw Lite (LLC2 encapsulation) peers leak CLS connect request buffers.

  Workaround: Use a different peer type. This will free an outstanding connect request if additional requests are received while the first is still pending.

- CSCdm51010

  An APPN router may run out of memory because of 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” message from the DLUS.

- CSCdm59430

  In a rare situation, a Cisco router may crash in the TCPD routines or managed timer. There is no workaround.

Interfaces and Bridging

- CSCdk10376

  When router traffic and memory usage is heavy, a router may crash in frf9_preComp().

  Workaround: Disable compression, use a different type of compression, or tune the memory tuning.

- CSCdm16052

  In Cisco IOS Releases 11.3(8.5) to 11.3(10.4), and 11.3(8.5)T through 11.3(10.4)T, all RSM and RSP platforms that use a VIP2/PA-4R IBM2692 adapter will potentially ignore non-RIF Token Ring packets because the VIP Token Ring driver incorrectly classifies these packets as runts and drops them.

  This is a regression introduced by CSCdk64195.

- CSCdm41644

  An overwrite issue in the BSS area with FDDI modules equipped can cause a router to crash.

IP Routing Protocols

- CSCdm20483

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

- CSCdm28898

  ARP to a Cisco 2500 series router running Cisco IOS Release 11.2(17) or 12.0(3.7) fails on the serial interface when bridging is enabled, and the router is reloaded. This problem was seen on the following topology:

  ----Ethernet----Cisco 2500 series router---serial interface---Cisco 2500 series router---Ethernet---

  The workaround is to remove and reenter the IP address on the serial interface.

- CSCdm44957

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

- CSCdm45873

  If you are redistributing OSPF routes into any other routing protocol, the redistributed routes do not include NSSA external routes. There is no workaround.

- CSCdm53317

  DNS replies passing from inside to outside by way of 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 may stop receiving packets on interfaces. This happens when CLNS packets with an N-selector of 0x20 (the DECnet NSP protocol selecter) are received by the router and the **decnet conversion** command 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 workaround is to reload the router.

Miscellaneous

- CSCdk45491

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

  Workaround: Manually set the speed to 100 by using the following new **speed** command. By default, the command is configured as **speed auto**.

  [**no**] **speed** {**10** | **100** | **auto**}

- CSCdm04861

  A race condition can occur between the processes that tried to get connection status and dropped packet information from the VIP.

  Workaround: Put in a semaphore to prevent multiple processes from accessing the globals used at the same time.

- CSCdm22032

  Configuring PPP encapsulation on an interface and then making that interface a member of a bridge group causes tracebacks and “fair-queue not initialized properly” messages.

Workaround: Remove bridging from the interface, or turn off fair queueing.

```
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
```

- CSCdm33707

  After a router is reloaded, ESA can not re-establish active crypto connections.

  Workaround: Remove the crypto map, reload the router again, and then re-apply the crypto map.

- CSCdm36128

  A Cisco 3600 series router with a 4T card configured for DTR goes down because the DTR downtime is too short.

- CSCdm44057

  A Cisco 7500 series router running virtual profiles continually resets the ciscoBus (cBus).

  The first message is "%RSP-3-RESTART: interface Serial4/0:1, output stuck." shortly before the cBus resets. To see more detailed information, enter the **debug cbus** command.

  This BUS resetting also causes all attached controllers to loose connectivity. Then, the only way to access the device is through the console port.

- CSCdm54169

  On a router running Cisco IOS Release 11.3(9.2), you cannot change the MTU size of a tunnel interface. CSCdk15279 permitted this ability to exceed the MTU size of the physical interface, which is 24.

  Workarounds:

  — Use Cisco IOS Release between 11.3(5.1)T and 11.3(9.3) or 12.0(0.16) and 12.0(4.2) (after CSCdk15279 but before CSCdm06422).

  — Configure the **ip mtu** command on the tunnel interface before configuring the **tunnel destination** command. If the **tunnel destination** command is already configured, then unconfigure it, configure the **ip mtu** command, wait five seconds, and then reconfigure the **tunnel destination** command.

  Once this workaround is issued, there should be no problems in the event of a router reboot because 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 routers may time out prematurely. Also, some connection setup attempts may not set up properly.

Novell IPX, XNS, and Apollo Domain

- CSCdk04507

  Routers running IPX and EIGRP on Cisco IOS Release 11.2 or greater can experience crashes when there is a high frequency of interface up/down transitions, especially with dial-up interfaces.

  Workaround: Disable IPX EIGRP.

VINES

- CSCdk80167

  Cisco 2500 series and Cisco 4000 series routers (68000-based routers) might reload a few minutes after VINES Sequenced Routing Update Protocol (SRTP) is configured.

  Workaround: Do not use VINES SRTP. If it is enabled, disable it by issuing the **no vines srtp-enabled** command.

Wide-Area Networking

- CSCdk37517

  DDR with the **dialer dtr** command 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 using the **show dialer** command to ensure that the dialer state is idle, and enter using the **show interface serial** *interface* command to check the state of DTR.

  This problem does not occur in Cisco IOS Release 11.1.

- CSCdm01618

  When a router is functioning as an X.28 PAD, it should send an 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.

- CSCdm12648

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

- CSCdm19188

  ISDN looses packets and headers when:

  1) Switch type is PRI_4ESS or PRI_5ESS.
  2) A connect request is sent by the router.
  3) The switch does not respond to a connect within T313.

  This causes the connect to be retransmitted, and that packet and header memory to not be released.

- CSCdm22162

  STAC compression LZS DCP becomes stuck in an R-Req loop.

  This problem is seen with Cisco IOS Release 11.1 or 11.2 hardware compression/RSP on one end and Cisco IOS Release 11.3 or 12.0 software compression on the other.

  Workaround: If you are using a Cisco 7500 series router, disable compression. If you are using a non-RSP router, you could also use software compression (instead of hardware compression) on both sides.

There still may be some problems with 11.1/11.2 hardware compression or RSP interfacing to 11.3/12.0 hardware compression or RSP (see CSCdm31447).

- 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. This problem is most likely to occur when the call cannot be forwarded immediately (for example, when using X.25-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

  A customer is deterministically getting a crash (segV) when dialer rotor best is configured and the **deb dialer** command is used once to traffic trigger a call.

- CSCdm37153

  A Cisco 5200 series router's PRI never sends a UAF response to a telco's switch.

- CSCdm37653

  Reliable PPP can cause an intermittent crash when used with WFQ.

  Workaround: Disable reliable PPP or WFQ.

- CSCdm48047

  A Cisco 4000 series router running Cisco IOS Release 11.3(9)WA4(11.1) crashes when configuring LECS, LES/BUS, and LEC. There is no workaround.

- CSCdm57650

  In a Multi-chassis MLP stack group, when two stack group members cross project MLP link interfaces, one of the stack group members may crash. There is no workaround.

Related Documentation

The following sections describe the documentation available for the Cisco 4000 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents.

Use these release notes with these documents:

- Release-Specific Documents, page 33
- Platform-Specific Documents, page 34
- Cisco IOS Software Documentation, page 34

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*

  On CCO:

  Service & Support: Documentation Home Page: 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

  As a supplement to the caveats listed in the "Caveats" section on page 18 in these release notes, see the "Important Notes and Caveats for Release 11.3" section in the *Cross-Platform Release Notes for Cisco IOS Release 11.3*, which contains caveats applicable to all platforms for all maintenance releases of Release 11.3.

  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: Cross-Platform Release Notes for Cisco IOS Release 11.3: Important Notes and Caveats for Release 11.3

  On the Documentation CD-ROM:

  Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Cross-Platform Release Notes for Cisco IOS Release 11.3: Important Notes and Caveats for Release 11.3

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 4000 series routers. These documents are also available online on CCO and on the Documentation CD-ROM.

- *Cisco 4000 Hardware Installation and Maintenance*
- *Cisco 4000 Series Installation Guide*
- Cisco 4000 Series Configuration Notes
- *Cisco 4000 Series Regulatory Compliance and Safety Information*
- *Redundant Power Systems*
- *Network Processor Two-Port Ethernet Full-Duplex (NP-2E-FDX)*
- *FDDI Frames-Per-Token Limit for the Cisco 4000 Series*
- Platform-specific release notes

On CCO:

Service & Support: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers: Cisco 4000 Series Routers

On the Documentation CD-ROM:

Access Servers and Access Routers: Modular Access Routers: Cisco 4000 Series Routers

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 documents, 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 & Support: Documentation Home Page: 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 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 & Support: Documentation Home Page: 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 6 Cisco IOS Software Release 11.3 Documentation Set

Books	Chapter Topics
• Configuration Fundamentals Configuration Guide • Configuration Fundamentals Command Reference	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management Interface Configuration System Management
• Network Protocols Configuration Guide, Part 1 • Network Protocols Command Reference, Part 1	IP Addressing IP Services IP Routing Protocols
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	Wide-Area Networking Overview ATM Frame Relay SMDS X.25 and LAPB
• *Security Configuration Guide* • *Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering Network Data Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options

Table 6 Cisco IOS Software Release 11.3 Documentation Set (continued)

Books	Chapter Topics
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	Business Applications and Scenarios Dial-In Port Setup Dial-In Terminal Services and Remote Note Configuration Dial Authentication Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Dial-Related Addressing Services (NAT/Easy IP) Cost-Control Solutions Network Traffic over ISDN Channels X.25 over ISDN Virtual Private Dialup Networks
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Paths for IP Networks NetFlow Switching Virtual LAN (VLAN) Routing LAN Emulation
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	Transparent Bridging Source-Route Bridging Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point Support SNA Frame Relay Access Support APPN NCIA Client/Server Topologies IBM Channel Attach
• *Configuration Guide Master Index* • *Command Reference Master Index*	

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" in *Cisco Information Packet* shipped with your product.

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

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

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

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

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: Technical Tips.**

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Lists tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.
- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Lists other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can reach CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which 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 33.