



Text Part Number: 78-2886-22 Rev. B0

Release Notes for Cisco IOS Release 11.1

March 19, 2001

These release notes describe the features and caveats for Cisco IOS Release 11.1 up to and including Release 11.1(24a). They include all routing and access server features.

Introduction

These release notes discuss the following topics:

- Documentation, page 3
- Platform Support, page 5
- Cisco IOS Packaging, page 9
- Memory Requirements, page 32
- New Features in Release 11.1(6) and Later 11.1 Releases, page 36
- New Features in Release 11.1(5), page 36
- New Features in Release 11.1(4), page 39
- New Features in Release 11.1(3), page 40
- New Features in Release 11.1(2), page 42
- New Features in Release 11.1(1), page 43
- Important Notes, page 57
- Caveats for Release 11.1(1) through 11.1(24a), page 63
- Caveats for Release 11.1(1) through 11.1(24), page 64
- Caveats for Release 11.1(1) through 11.1(23), page 67
- Caveats for Release 11.1(1) through 11.1(22), page 68
- Caveats for Release 11.1(1) through 11.1(21), page 69

Corporate Headquarters

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

Copyright © 1996–2001
Cisco Systems, Inc.
All rights reserved.

- Caveats for Release 11.1(1) through 11.1(20), page 70
- Caveats for Release 11.1(1) through 11.1(19), page 72
- Caveats for Release 11.1(1) through 11.1(18), page 75
- Caveats for Release 11.1(1) through 11.1(17), page 79
- Caveats for Release 11.1(1) through 11.1(16), page 82
- Caveats for Release 11.1(1) through 11.1(15), page 86
- Caveats for Release 11.1(1) through 11.1(14), page 90
- Caveats for Release 11.1(1) through 11.1(13), page 95
- Caveats for Release 11.1(1) through 11.1(12), page 102
- Caveats for Release 11.1(1) through 11.1(11), page 106
- Caveats for Release 11.1(1) through 11.1(10), page 110
- Caveats for Release 11.1(1) through 11.1(9), page 116
- Caveats for Release 11.1(1) through 11.1(8), page 121
- Caveats for Release 11.1(1) through 11.1(7), page 124
- Caveats for Release 11.1(1) through 11.1(6), page 129
- Caveats for Release 11.1(1) through 11.1(5), page 133
- Caveats for Release 11.1(1) through 11.1(4), page 141
- Caveats for Release 11.1(1) through 11.1(3), page 146
- Caveats for Release 11.1(1) through 11.1(2), page 152
- Caveats for Release 11.1(1), page 156
- Microcode Software, page 163
- Microcode Revision History (for Cisco 7000 Series Platforms), page 164
- Route Switch Processor (RSP) Microcode Revision History, page 173
- Cisco Connection Online, page 182
- Documentation CD-ROM, page 183
- Open Source License Acknowledgements, page 183

Documentation

Cisco IOS Release 11.1 access server and router software functionality and configuration information is documented in a six-module documentation set. (Previous to Release 11.1, access server software and router software were documented separately.) Each module consists of a configuration guide and a command reference. There are also five supporting documents.

The six documentation modules and supporting documents cover these topics:

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> 	Access Server and Router Product Overview User Interface Loading System Images and Configuration Files Setup Command Interfaces System Management
<ul style="list-style-type: none"> • <i>Access Services Configuration Guide</i> • <i>Access Services Command Reference</i> 	Terminal Lines and Modem Support AppleTalk Remote Access SLIP and PPP XRemote LAT Telnet TN3270 Protocol Translation
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	ATM Dial-on-Demand Routing (DDR) Frame Relay ISDN LANE SMDS X.25
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	AppleTalk IP IP Routing Novell IPX
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> 	Transparent Bridging
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Command Reference</i> 	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
	IBM Channel Attach
<ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> 	(Supporting Documents)
<ul style="list-style-type: none"> • <i>Cisco Management Information Base (MIB) User Quick Reference</i> 	
<ul style="list-style-type: none"> • <i>System Error Messages</i> 	
<ul style="list-style-type: none"> • <i>Debug Command Reference</i> 	
<ul style="list-style-type: none"> • <i>Cisco Access Connection Guide</i> 	

These documents are available both as printed manuals and as electronic documents. The most up-to-date Cisco IOS documentation can be found on the latest Documentation CD-ROM and on the Web. The electronic documents contain updates and modifications made after the paper documents were printed.

You can access the electronic documents either on the Cisco Documentation CD-ROM or at Cisco Connection Online (CCO) on the World Wide Web.

On the CD-ROM, go to the Cisco IOS Software Configuration database, select Cisco IOS Release 11.1, and follow the link to the Cisco IOS Configuration Guides and Command References.

CCO is on the World Wide Web at <http://www.cisco.com>, <http://www-europe.cisco.com>, or <http://www-china.cisco.com>. From CCO, go to the Technical Documentation page to find the Cisco IOS Software Configuration database. Then, select Cisco IOS Release 11.1, and follow the link to the Cisco IOS Configuration Guides and Command References.

Additional information about CCO and the Documentation CD-ROM is in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of these release notes.

Platform Support

You can run all Cisco IOS 11.1 releases on these Cisco hardware platforms, except as noted:

- Cisco 7500 series
- Cisco 7200 series (you cannot run Cisco IOS Releases 11.1(1) through 11.1(4) on this platform)
- Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI)
- Cisco 4000 series (includes the Cisco 4000, 4000-M, 4500, 4500-M, 4700, and 4700-M; Cisco 4700-M is supported by Cisco IOS Release 11.1(2) and later releases)
- Cisco 3000 series (except the Cisco 3202)
- Cisco 2500 series
- Cisco 1003 and Cisco 1004 ISDN routers
- Cisco 1005 router
- Cisco 1000 LAN Extender (you cannot run Cisco IOS Release 11.1(1) on this platform)
- AccessPro PC
- Cisco AS5100
- Cisco AS5200 (you cannot run Cisco IOS Releases 11.1(1) through 11.1(4) on this platform)

For each of the supported platforms, Release 11.1 enables your Cisco device to use certain LAN and WAN interfaces and data rates.

For a list of interfaces supported by Release 11.1 for each platform, see Table 1, Table 2, Table 3, and Table 4 (following).

- Table 1 summarizes the LAN interfaces supported on the Cisco 7500, 7200, 7000, 4000, 3000, and 2500 series platforms.
- Table 2 summarizes the LAN interfaces supported on Cisco 1003, 1004, and 1005 routers, the Cisco 1000 LAN Extender, the AccessPro PC card, and the Cisco AS5100 and 5200 platforms.
- Table 3 summarizes the WAN data rates and interfaces supported on Cisco 7500, 7200, 7000, 4000, 3000, and 2500 series platforms.
- Table 4 summarizes the WAN data rates and interfaces supported on Cisco 1003, 1004, and 1005 routers, the Cisco 1000 LAN Extender, the AccessPro PC card, and the Cisco AS5100 and 5200 platforms.

For each platform, you can use any of the interfaces or data rates labeled “Yes” in the table. Release 11.1 does not support interfaces or data rates that are labeled “No.”

Table 1 LAN Interfaces Supported by Router Platforms, Part 1

Interface	Cisco 7500 Series	Cisco 7200 Series	Cisco 7000 Series	Cisco 4000 Series	Cisco 3000 Series ¹	Cisco 2500 Series
Ethernet (AUI)	Yes	Yes	Yes	Yes	Yes	Yes
Ethernet (10BaseT)	Yes	Yes	Yes	Yes	No	Yes ²
Ethernet (10BaseFL)	Yes	Yes	Yes ³	No	No	No
Fast Ethernet (100BaseTX)	Yes	Yes	Yes ³	Yes ⁴	No	No
Fast Ethernet (100BaseFX)	Yes	Yes	Yes	Yes ⁴	No	No
4-Mbps Token Ring	Yes	Yes	Yes	Yes	Yes	Yes
16-Mbps Token Ring	Yes	Yes	Yes	Yes	Yes	Yes
FDDI DAS	Yes	Yes	Yes	Yes	No	No
FDDI SAS	Yes	No	Yes	Yes	No	No
FDDI multimode	Yes	Yes	Yes	Yes (DAS/SAS)	No	No
FDDI single-mode	Yes	Yes	Yes	Yes	No	No
ATM Interface	Yes	No	Yes	Yes	No	No
Channel Interface	Yes	No	Yes	No	No	No
Second-generation Channel Interface ⁵	Yes	No	Yes	No	No	No
Parallel Channel Adapter (Bus and Tag)	Yes	No	Yes	No	No	No
ESCON Channel Adapter (ECA)	Yes	No	Yes	No	No	No
Versatile Interface	Yes	No	Yes	No	No	No
Second-generation Versatile Interface ²	Yes	No	Yes	No	No	No
MultiChannel Interface (Channelized E1/T1)	Yes	No	Yes	Yes	No	No
Packet-Over-SONET OC-3 Interface ²	Yes	No	Yes	Yes	No	No
Synchronous Serial	Yes	Yes	Yes	Yes	Yes	Yes

1 Except the Cisco 3202.

2 Cisco 2505, Cisco 2507, Cisco 2516, Cisco 2518, and Cisco 2520–Cisco 2525 only.

3 May require the 7000 series Route Switch Processor (RSP7000).

4 Only the Cisco 4500, 4500-M, 4700, and 4700-M routers support Fast Ethernet.

5 In the Cisco 7000 series routers (Cisco 7000 and Cisco 7010), these interfaces require either a Route Processor (RP) and Switch Processor (SP) (or Silicon Switch Processor [SSP]) combination, or a combination of the 7000 series Route Switch Processor (RSP7000) and the 7000 series chassis interface (RSP7000CI).

Table 2 LAN Interfaces Supported by Router Platforms, Part 2

Interface	Cisco 1003/ 1004	Cisco 1005	Cisco 1000 LAN Extender	AccessPro PC Card	Cisco AS5100	Cisco AS5200
Ethernet (AUI)	No	No	Yes	No	Yes	Yes
Ethernet (10BaseT)	Yes	Yes	Yes	Yes	No	No
Ethernet (10BaseFL)	No	No	No	No	No	No
Fast Ethernet (100BaseTX)	No	No	No	No	No	No
Fast Ethernet (100BaseFX)	No	No	No	No	No	No
4-Mbps Token Ring	No	No	No	Yes	No	No
16-Mbps Token Ring	No	No	No	Yes	No	No
FDDI DAS	No	No	No	No	No	No
FDDI SAS	No	No	No	No	No	No
FDDI multimode	No	No	No	No	No	No
FDDI single-mode	No	No	No	No	No	No
ATM Interface	No	No	No	No	No	No
Channel Interface	No	No	No	No	No	No
Second-generation Channel Interface	No	No	No	No	No	No
Parallel Channel Adapter (Bus and Tag)	No	No	No	No	No	No
ESCON Channel Adapter (ECA)	No	No	No	No	No	No
Versatile Interface	No	No	No	No	No	No
Second-generation Versatile Interface	No	No	No	No	No	No
MultiChannel Interface (Channelized E1/T1)	No	No	No	No	No	Yes
Packet-Over-SONET OC-3 Interface	No	No	No	No	No	No
Synchronous Serial	No	No	No	No	Yes	Yes

Table 3 WAN Data Rates and Interfaces Supported by Router Platforms, Part 1

	Cisco 7500 Series	Cisco 7200 Series	Cisco 7000 Series	Cisco 4000 Series	Cisco 3000 Series ¹	Cisco 2500 Series
Data Rate						
48/56/64 kbps	Yes	Yes	Yes	Yes	Yes	Yes
1.544/2.048 Mbps	Yes	Yes	Yes	Yes	Yes	Yes
34/45/52 Mbps	Yes	Yes	Yes	No	No	No
Interface						
EIA/TIA-232	Yes	Yes	Yes	Yes	Yes	Yes
X.21	Yes	Yes	Yes	Yes	Yes	Yes
V.35	Yes	Yes	Yes	Yes	Yes	Yes
EIA/TIA-449	Yes	Yes	Yes	Yes	Yes	Yes
EIA-530	Yes	Yes	Yes	Yes	Yes	Yes
EIA/TIA-613 (HSSI)	Yes	No	Yes	No	No	No
ISDN BRI	No	No	No	Yes	Yes	Yes
ISDN PRI	Yes	No	Yes	Yes	No	No
E1-G.703/G.704	Yes	No	Yes	Yes	No	No

¹ Except the Cisco 3202

Table 4 WAN Data Rates and Interfaces Supported by Router Platforms, Part 2

	Cisco 1003/1004	Cisco 1005	Cisco 1000 LAN Extender	AccessPro PC Card	Cisco AS5100	Cisco AS5200
Data Rate						
48/56/64 kbps	Yes	Yes	Yes	Yes	Yes	Yes
1.544/2.048 Mbps	No	Yes	Yes	Yes	Yes	Yes
34/45/52 Mbps	No	No	No	No	No	No
Interface						
EIA/TIA-232	No	Yes	No	Yes	Yes	Yes
X.21	No	Yes	Yes	Yes	Yes	Yes
V.35	No	Yes	Yes	Yes	Yes	Yes
EIA/TIA-449	No	Yes	No	Yes	Yes	Yes
EIA-530	No	Yes	No	Yes	Yes	Yes
EIA/TIA-613 (HSSI)	No	No	No	No	No	No
ISDN BRI	Yes	Yes	No	Yes	No	No
ISDN PRI	No	No	No	No	No	Yes
E1-G.703/G.704	No	No	No	No	No	Yes

Cisco IOS Packaging

The Cisco IOS software is packaged into “feature sets” (also called “software images”). There are many different feature sets available, and each feature set contains a specific subset of Cisco IOS features. Not all feature sets are available with all platforms. Also, some feature sets support different features when run on different platforms.

To learn what features are available with each feature set, see tables Table 5 through Table 14 (following). These tables summarize what features you can use when running a specific feature set on a specific platform. A “Yes” in the table indicates that the feature is available in the feature set.

- Table 5 summarizes the feature sets and optional licenses for the Cisco 7500 series platforms.
- Table 6 summarizes the feature sets for the Cisco 7200 series platforms.
- Table 7 summarizes the feature sets and optional licenses for the Cisco 7000 series platforms.
- Table 8 and Table 9 summarize the feature sets for the Cisco 2500 series and AS5100 platforms. (There are too many feature sets to fit in one table, so the information is split into two tables.)
- Table 10 summarizes the feature sets for the Cisco AS5200 platform.
- Table 11 summarizes the features sets for the supported Cisco 4000 series platforms, which includes the Cisco 4000, Cisco 4000-M, Cisco 4500, Cisco 4500-M, and Cisco 4700 routers.
- Table 12 summarizes the feature sets for the Cisco 3000 series.
- Table 13 summarizes the feature sets for the Cisco 1003 and Cisco 1004 ISDN routers.
- Table 14 summarizes the feature sets for the Cisco 1005 router.

You can use these tables to determine if you can configure and use a specific feature with your platform and Release 11.1 feature set.

Note For some platforms, you can purchase a “feature pack,” which contains a group of one or more feature sets on a CD-ROM. For more information about feature packs, refer to the release notes for Cisco IOS Release 11.1 feature packs, or refer to the Feature Pack Information web page on CCO or the Documentation CD-ROM in the Cisco IOS Release 11.1 documentation area.

Table 5 Cisco 7500 Series Software Feature Sets

Feature	Feature Set											
	IP	IP/IPX/ IBM	IP/IPX/ IBM/ APPN	Desktop/ IBM	Enter- prise	Enter- prise/ APPN	IP/VIP	IP/IPX/ IBM/ VIP	IP/IPX/ IBM/ APPN/ VIP	Desktop/ IBM/VIP	Enter- prise/ VIP	Enter- prise/ APPN/ VIP
SNMP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RMON (events and alarms)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Asynchronous support (SLIP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SMDS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Cisco 7500 Series Software Feature Sets (continued)

Feature	Feature Set											
	IP	IP/IPX/ IBM	IP/IPX/ IBM/ APPN	Desktop/ IBM	Enter- prise	Enter- prise/ APPN	IP/VIP	IP/IPX/ IBM/ VIP	IP/IPX/ IBM/ APPN/ VIP	Desktop/ IBM/VIP	Enter- prise/ VIP	Enter- prise/ APPN/ VIP
X.25	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HDLC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIPv2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NHRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ES-IS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IS-IS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transparent bridging	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Translational bridging	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN extension host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
NLSP	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
IPXWAN 2.0	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
AppleTalk Versions 1 and 2	—	—	—	Yes	Yes	Yes	—	—	—	Yes	Yes	Yes
AURP	—	—	—	Yes	Yes	Yes	—	—	—	Yes	Yes	Yes
DECnet IV	—	—	—	Yes	Yes	Yes	—	—	—	Yes	Yes	Yes
DECnet V	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes

Table 5 Cisco 7500 Series Software Feature Sets (continued)

Feature	Feature Set											
	IP	IP/IPX/ IBM	IP/IPX/ IBM/ APPN	Desktop/ IBM	Enter- prise	Enter- prise/ APPN	IP/VIP	IP/IPX/ IBM/ VIP	IP/IPX/ IBM/ APPN/ VIP	Desktop/ IBM/VIP	Enter- prise/ VIP	Enter- prise/ APPN/ VIP
Apollo Domain	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
Banyan VINES	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
ISO CLNS	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
XNS	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
Lock-and-Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MD5 routing authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Kerberized login	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
TACACS+	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
RADIUS	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
V.120	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
SRB	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
RSRB	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
APPN	—	—	Yes	—	—	Yes	—	—	—	—	—	Yes
FRAS BAN	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
DLSw (RFC 1795)	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
DLSw+	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
SDLC	—	Yes	Yes	Yes	Yes	Yes	—	—	Yes	—	Yes	Yes
SDLLC	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
SRT bridging	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
STUN	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
TG/COS	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
QLLC	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
DSPU	—	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
NetView Native Service Point	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
Protocol translation	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
Telnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PAD	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
AutoInstall	—	—	Yes	Yes	Yes	Yes	—	—	Yes	Yes	Yes	Yes
Router monitoring	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes

Table 5 Cisco 7500 Series Software Feature Sets (continued)

Feature	Feature Set											
	IP	IP/IPX/ IBM	IP/IPX/ IBM/ APPN	Desktop/ IBM	Enter- prise	Enter- prise/ APPN	IP/VIP	IP/IPX/ IBM/ VIP	IP/IPX/ IBM/ APPN/ VIP	Desktop/ IBM/VIP	Enter- prise/ VIP	Enter- prise/ APPN/ VIP
High System Availability (HSA)	—	—	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes
DHCP	—	—	—	—	Yes	Yes	—	—	—	—	Yes	Yes
NetBEUI over PPP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 6 Cisco 7200 Series Software Feature Sets

Feature	Feature Set			
	Network Layer 3 Switching	Desktop/IBM	Enterprise	Enterprise/APPN
SNMP	Yes	Yes	Yes	Yes
RMON (events and alarms)	Yes	Yes	Yes	Yes
Asynchronous support (SLIP)	Yes	Yes	Yes	Yes
Frame Relay	—	Yes	Yes	Yes
SMDS	Yes	Yes	Yes	Yes
X.25	Yes	Yes	Yes	Yes
ISDN	—	Yes	Yes	Yes
PPP	—	Yes	Yes	Yes
HDLC	—	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes
RIPv2	Yes	Yes	Yes	Yes
IGRP	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes
OSPF	Yes	Yes	Yes	Yes
BGP	Yes	Yes	Yes	Yes
EGP	Yes	Yes	Yes	Yes
PIM	Yes	Yes	Yes	Yes
NHRP	Yes	Yes	Yes	Yes
Policy-based routing	Yes	Yes	Yes	Yes
ES-IS	—	—	Yes	Yes
IS-IS	—	—	Yes	Yes
DDR	—	Yes	Yes	Yes

Table 6 Cisco 7200 Series Software Feature Sets (continued)

Feature	Feature Set			
	Network Layer 3 Switching	Desktop/IBM	Enterprise	Enterprise/APPN
Snapshot routing	—	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes
Transparent bridging	Yes	Yes	Yes	Yes
Translational bridging	Yes	Yes	Yes	Yes
Concurrent routing and bridging	Yes	Yes	Yes	Yes
Multiring	Yes	Yes	Yes	Yes
LAN extension host	Yes	Yes	Yes	Yes
ISL	Yes	—	—	—
GRE	—	Yes	Yes	Yes
IPX	Yes	Yes	Yes	Yes
NLSP	Yes	Yes	Yes	Yes
IPX RIP	Yes	Yes	Yes	Yes
RTMP	Yes	Yes	Yes	Yes
IPXWAN 2.0	—	Yes	Yes	Yes
AppleTalk Versions 1 and 2	—	Yes	Yes	Yes
AURP	Yes	Yes	Yes	Yes
SMRP	Yes	Yes	Yes	Yes
S RTP	—	—	Yes	Yes
DECnet IV	—	Yes	Yes	Yes
DECnet V	—	—	Yes	Yes
OSI	—	—	Yes	Yes
Apollo Domain	—	—	Yes	Yes
Banyan VINES	—	—	Yes	Yes
ISO CLNS	—	—	Yes	Yes
XNS	—	—	Yes	Yes
Lock-and-Key	Yes	Yes	Yes	Yes
MD5 routing authentication	Yes	Yes	Yes	Yes
Kerberized login	—	—	Yes	Yes
TACACS+	Yes	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes
V.120	—	—	Yes	Yes
SRB ¹	—	Yes	Yes	Yes
RSRB	—	Yes	Yes	Yes
APPN	—	—	—	Yes

Table 6 Cisco 7200 Series Software Feature Sets (continued)

Feature	Feature Set			
	Network Layer 3 Switching	Desktop/IBM	Enterprise	Enterprise/APPN
FRAS BAN	—	Yes	Yes	Yes
DLSw (RFC 1795)	—	Yes	Yes	Yes
DLSw+ ²	—	Yes	Yes	Yes
SDLC	—	Yes	Yes	Yes
SDLLC	—	Yes	Yes	Yes
SRT bridging	—	Yes	Yes	Yes
STUN	—	Yes	Yes	Yes
TG/COS	—	—	Yes	Yes
QLLC	—	Yes	Yes	Yes
DSPU	—	—	Yes	Yes
NetView Native Service Point	—	Yes	Yes	Yes
Protocol translation	—	—	Yes	Yes
Telnet	Yes	Yes	Yes	Yes
Modem auto-configuring	Yes	Yes	Yes	Yes
PAD	—	—	Yes	Yes
AutoInstall	Yes	Yes	Yes	Yes
Router monitoring	—	—	Yes	Yes
DHCP	—	—	Yes	Yes
NetBEUI over PPP	—	—	Yes	Yes

1 SRB over FDDI is not supported in this release.

2 DLSw+ over TCP/IP is supported.

Table 7 Cisco 7000 Series Software Feature Sets

Feature	Feature Set												
	IP	IP/IPX/ IBM	IP/IPX/ IBM/ APPN	Desk- top/ IBM	Enter- prise	Source- Route Switch	Enter- prise/ APPN	IP/ VIP	IP/ IPX/ IBM/ VIP	IP/IPX/ IBM/ APPN/ VIP	Desk- top/ IBM/ VIP	Enter- prise/ VIP	Enter- prise/ APPN/ VIP
SNMP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RMON (events and alarms)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Asynchronous support (SLIP)	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SMDS	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HDLC	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes	Yes	Yes (host only)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIPv2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IGRP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BGP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EGP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NHRP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ES-IS	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IS-IS	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Snapshot routing	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transparent bridging	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Translational bridging	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multitring	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN extension host	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes

Table 7 Cisco 7000 Series Software Feature Sets (continued)

Feature	Feature Set												
	IP	IP/IPX/ IBM	IP/IPX/ IBM/ APPN	Desk- top/ IBM	Enter- prise	Source- Route Switch	Enter- prise/ APPN	IP/ VIP	IP/ IPX/ IBM/ VIP	IP/IPX/ IBM/ APPN/ VIP	Desk- top/ IBM/ VIP	Enter- prise/ VIP	Enter- prise/ APPN/ VIP
NLSP	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes
IPXWAN 2.0	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes
AppleTalk Versions 1 and 2	—	—	—	Yes	Yes	—	Yes	—	—	—	Yes	Yes	Yes
AURP	—	—	—	Yes	Yes	—	Yes	—	—	—	Yes	Yes	Yes
DECnet IV	—	—	—	Yes	Yes	—	Yes	—	—	—	Yes	Yes	Yes
DECnet V	—	—	—	—	Yes	—	Yes	—	—	—	—	Yes	Yes
Apollo Domain	—	—	—	—	Yes	—	Yes	—	—	—	—	Yes	Yes
Banyan VINES	—	—	—	—	Yes	—	Yes	—	—	—	—	Yes	Yes
ISO CLNS	—	—	—	—	Yes	—	Yes	—	—	—	—	Yes	Yes
XNS	—	—	—	—	Yes	—	Yes	—	—	—	—	Yes	Yes
Lock-and- Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—	—	Yes	Yes	Yes
MD5 routing authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Kerberized login	—	—	—	—	Yes	Yes	Yes	—	—	—	—	Yes	Yes
TACACS+	—	—	—	—	Yes	Yes	Yes	—	—	—	—	Yes	Yes
RADIUS	—	—	—	—	Yes	Yes	Yes	—	—	—	—	Yes	Yes
V.120	—	—	—	—	Yes	Yes	Yes	—	—	—	—	Yes	Yes
SRB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RSRB	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
APPN	—	—	Yes	—	—	—	Yes	—	—	—	—	—	Yes
FRAS BAN	—	—	—	—	Yes	—	Yes	—	—	—	—	Yes	Yes
DLSw (RFC 1795)	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes
DLSw+	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes
SDLC	—	Yes	Yes	Yes	Yes	—	Yes	—	—	Yes	—	Yes	Yes
SDLLC	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes
SRT bridging	—	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
STUN	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes
TG/COS	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes
QLLC	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes
DSPU	—	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes	Yes	Yes	Yes

Table 7 Cisco 7000 Series Software Feature Sets (continued)

Feature	Feature Set												
	IP	IP/IPX/ IBM	IP/IPX/ IBM/ APPN	Desk- top/ IBM	Enter- prise	Source- Route Switch	Enter- prise/ APPN	IP/ VIP	IP/ IPX/ IBM/ VIP	IP/IPX/ IBM/ APPN/ VIP	Desk- top/ IBM/ VIP	Enter- prise/ VIP	Enter- prise/ APPN/ VIP
NetView Native Service Point	—	—	—	—	Yes	Yes	Yes	—	—	—	—	Yes	Yes
Protocol translation	—	—	—	—	Yes	Yes	Yes	—	—	—	—	Yes	Yes
Telnet	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PAD	—	—	—	—	Yes	—	Yes	—	—	—	—	Yes	Yes
AutoInstall	—	—	Yes	Yes	Yes	—	Yes	—	—	Yes	Yes	Yes	Yes
Router monitoring	—	—	—	—	Yes	Yes	Yes	—	—	—	—	Yes	Yes
DHCP	—	—	—	—	Yes	—	Yes	—	—	—	—	Yes	Yes
NetBEUI over PPP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 8 Cisco 2500 Series and AS5100 Software Feature Sets, Part 1

Feature	Feature Set									
	IP	IP/RMON	IP/IBM Base	IP/IBM/ RMON	IP/IPX	IP/IPX/ RMON	IP/IPX/ IBM Base	IP/IPX/IBM/ RMON	IP/IPX/IBM/ APPN	
SNMP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
RMON ¹	—	Yes	—	Yes	—	Yes	—	Yes	—	
Asynchronous support (SLIP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
CSLIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
ARAP	—	—	—	—	—	—	—	—	—	
Frame Relay	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
SMDS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
X.25	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
ISDN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
PPP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
CPPP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
HDLC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
RIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
RIPv2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

Table 8 Cisco 2500 Series and AS5100 Software Feature Sets, Part 1 (continued)

Feature	Feature Set								
	IP	IP/RMON	IP/IBM Base	IP/IBM/RMON	IP/IPX	IP/IPX/RMON	IP/IPX/IBM Base	IP/IPX/IBM/RMON	IP/IPX/IBM/APPN
OSPF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NHRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ES-IS	—	—	—	—	—	—	—	—	—
IS-IS	—	—	—	—	—	—	—	—	—
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bridging (transparent and translational)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN extension host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX	—	—	—	—	Yes	Yes	Yes	Yes	Yes
NLSP	—	—	—	—	Yes	Yes	Yes	Yes	Yes
IPXWAN 2.0	—	—	—	—	Yes	Yes	Yes	Yes	Yes
RTMP	—	—	—	—	—	—	—	—	—
SMRP	—	—	—	—	—	—	—	—	—
SRTP	—	—	—	—	—	—	—	—	—
AppleTalk Versions 1 and 2	—	—	—	—	—	—	—	—	—
AURP	—	—	—	—	—	—	—	—	—
DECnet IV	—	—	—	—	—	—	—	—	—
DECnet V	—	—	—	—	—	—	—	—	—
Apollo Domain	—	—	—	—	—	—	—	—	—
Banyan VINES	—	—	—	—	—	—	—	—	—
ISO CLNS	—	—	—	—	—	—	—	—	—
XNS	—	—	—	—	—	—	—	—	—
Lock-and-Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MD5 routing authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Kerberized login	—	—	—	—	—	—	—	—	—
V.120	—	—	—	—	—	—	—	—	—
SRB	—	—	Yes	Yes	—	—	Yes	Yes	Yes
RSRB	—	—	Yes	Yes	—	—	Yes	Yes	Yes
APPN	—	—	—	—	—	—	—	—	Yes

Table 8 Cisco 2500 Series and AS5100 Software Feature Sets, Part 1 (continued)

Feature	Feature Set								
	IP	IP/RMON	IP/IBM Base	IP/IBM/RMON	IP/IPX	IP/IPX/RMON	IP/IPX/IBM Base	IP/IPX/IBM/RMON	IP/IPX/IBM/APPN
FRAS BAN	—	—	Yes	Yes	—	—	Yes	Yes	Yes
DLSw (RFC 1795)	—	—	Yes	Yes	—	—	Yes	Yes	Yes
DLSw+	—	—	Yes	Yes	—	—	Yes	Yes	Yes
SDLC	—	—	Yes	Yes	—	—	Yes	Yes	Yes
SDLLC	—	—	Yes	Yes	—	—	Yes	Yes	Yes
STUN	—	—	Yes	Yes	—	—	Yes	Yes	Yes
TG/COS	—	—	—	—	—	—	—	—	—
QLLC	—	—	Yes	Yes	—	—	Yes	Yes	Yes
Bisync	—	—	Yes	Yes	—	—	Yes	Yes	Yes
DSPU	—	—	—	—	—	—	—	—	—
NetView Native Service Point	—	—	Yes	Yes	—	—	—	Yes	Yes
Protocol translation	—	—	—	—	—	—	—	—	—
TN3270	—	—	—	—	—	—	—	—	—
LAT	—	—	—	—	—	—	—	—	—
SRT Bridging	—	—	Yes	Yes	—	—	Yes	Yes	Yes
XRemote	—	—	—	—	—	—	—	—	—
Telnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PAD	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AutoInstall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Modem auto-configuring	—	—	—	—	—	—	—	—	—
Router monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NASI	—	—	—	—	—	—	—	—	—
NetBEUI over PPP	—	—	—	—	—	—	—	—	—

1 All feature sets include RMON alarm and events groups. Full, nine-group RMON support is included in the feature sets indicated.

Table 9 Cisco 2500 Series and AS5100 Software Feature Sets, Part 2

Feature	Feature Set									
	Desktop	Desktop/ IBM Base	Enterprise	Enterprise/ RMON	Enterprise/ APPN	CFRAD	Remote Access Server	ISDN	LAN FRAD	OSPF LAN FRAD ¹
SNMP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RMON ²	—	—	—	Yes	—	—	—	—	—	—
Asynchronous support (SLIP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CSLIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARAP	Yes	Yes	Yes	Yes	Yes	—	Yes	—	—	—
Frame Relay	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes
SMDS	Yes	Yes	Yes	Yes	Yes	—	—	—	—	—
X.25	Yes	Yes	Yes	Yes	Yes	—	Yes	—	—	—
ISDN	Yes	Yes	Yes	Yes	Yes	—	—	Yes	—	—
PPP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CHPPP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HDLC	Yes	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes
IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIPv2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ³
OSPF	Yes	Yes	Yes	Yes	Yes	—	—	Yes	—	Yes
BGP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	—	—
EGP	Yes	Yes	Yes	Yes	Yes	—	—	Yes	—	—
PIM	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	—	—
NHRP	Yes	Yes	Yes	Yes	Yes	—	—	Yes	—	—
ES-IS	—	—	Yes	Yes	Yes	—	—	—	—	—
IS-IS	—	—	Yes	Yes	Yes	—	—	—	—	—
Snapshot routing	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	—	—
NTP	Yes	Yes	Yes	Yes	Yes	—	Yes	—	—	—
Bridging (transparent and translational)	Yes	Yes	Yes	Yes	Yes	—	—	Yes	Yes	Yes
Multiring	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes
LAN extension host	Yes	Yes	Yes	Yes	Yes	—	—	—	—	—
IPX	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes
NLSP	Yes	Yes	Yes	Yes	Yes	—	—	—	—	—
IPXWAN 2.0	Yes	Yes	Yes	Yes	Yes	—	Yes	—	Yes	Yes

Table 9 Cisco 2500 Series and AS5100 Software Feature Sets, Part 2 (continued)

Feature	Feature Set									
	Desktop	Desktop/ IBM Base	Enterprise	Enterprise/ RMON	Enterprise/ APPN	CFRAD	Remote Access Server	ISDN	LAN FRAD	OSPF LAN FRAD ¹
RTMP	Yes	Yes	Yes	Yes	Yes	—	Yes	—	—	—
SMRP	Yes	Yes	Yes	Yes	Yes	—	Yes	—	—	—
S RTP	—	—	Yes	Yes	Yes	—	Yes	—	—	—
AppleTalk Versions 1 and 2	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	—	—
AURP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	—	—
DECnet IV	Yes	Yes	Yes	Yes	Yes	—	—	—	—	—
DECnet V	—	—	Yes	Yes	Yes	—	—	—	—	—
Apollo Domain	—	—	Yes	Yes	Yes	—	—	—	—	—
Banyan VINES	—	—	Yes	Yes	Yes	—	—	—	—	—
ISO CLNS	—	—	Yes	Yes	Yes	—	—	—	—	—
XNS	—	—	Yes	Yes	Yes	—	—	—	—	—
Lock-and-Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MD5 routing authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		
Kerberized login	—	—	Yes	Yes	Yes	—	—	—		
V.120	—	—	Yes	Yes	Yes	—	—	—	—	—
SRB	—	Yes	Yes	Yes	Yes	—	—	—	Yes	Yes
RSRB	—	Yes	Yes	Yes	Yes	Yes	—	—	Yes	Yes
APPN	—	—	—	—	Yes	—	—	—	—	—
FRAS BAN	—	Yes	Yes	Yes	Yes	Yes	—	—		
DLSw (RFC 1795)	—	Yes	Yes	Yes	Yes	Yes	—	—	Yes	Yes
DLSw+	—	Yes	Yes	Yes	Yes	—	—	—	—	—
SDLC	—	Yes	Yes	Yes	Yes	Yes	—	—	Yes	Yes
SDLLC	—	Yes	Yes	Yes	Yes	Yes	—	—	Yes	Yes
STUN	—	Yes	Yes	Yes	Yes	Yes	—	—	Yes	Yes
TG/COS	—	—	Yes	Yes	Yes	—	—	—	—	—
QLLC	—	Yes	Yes	Yes	Yes	—	—	—	—	—
Bisync	—	Yes	Yes	Yes	Yes	Yes	—	—	Yes	Yes
DSPU	—	—	Yes	Yes	Yes	—	—	—	—	—
NetView Native Service Point	—	Yes	Yes	Yes	Yes	Yes	—	—		
Protocol translation	—	—	Yes	Yes	Yes	—	Yes	—	—	—
TN3270	—	—	Yes	Yes	Yes	—	Yes	—	—	—
LAT	—	—	Yes	Yes	Yes	—	Yes	—	—	—

Table 9 Cisco 2500 Series and AS5100 Software Feature Sets, Part 2 (continued)

Feature	Feature Set									
	Desktop	Desktop/ IBM Base	Enterprise	Enterprise/ RMON	Enterprise/ APPN	CFRAD	Remote Access Server	ISDN	LAN FRAD	OSPF LAN FRAD ¹
SRT Bridging	—	Yes	Yes	Yes	Yes	—	—	—	—	—
XRemote	—	—	Yes	Yes	Yes	—	Yes	—	—	—
Telnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PAD	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	—	—
AutoInstall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes
Modem auto configuration	—	—	Yes	Yes	Yes	—	Yes	—	—	—
Router monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	—	—
NASI	—	—	—	—	—	—	Yes	—	—	—
NetBEUI over PPP	—	—	Yes	Yes	Yes	—	Yes	—	—	—

1 The OSPF LANFRAD feature set is available in Release 11.1(9) and later.

2 All feature sets except CFRAD include RMON alarm and events groups. Full, nine-group RMON support is included in the feature sets indicated.

3 Enhanced IGRP is only available in Release 11.1(9). It is not supported in any subsequent releases of the Release 11.1 OSPF LANFRAD feature set.

Table 10 Cisco AS5200 Software Feature Sets

Feature	Feature Set		
	IP/Managed Modems	Desktop/ Managed Modems	Enterprise/RMON/ Managed Modems
SNMP	Yes	Yes	Yes
RMON ¹	—	—	Yes
Asynchronous support (SLIP)	Yes	Yes	Yes
CSLIP	Yes	Yes	Yes
ARA Protocol	—	Yes	Yes
Frame Relay	Yes	Yes	Yes
SMDS	Yes	Yes	Yes
X.25	Yes	Yes	Yes
ISDN	Yes	Yes	Yes
PPP	Yes	Yes	Yes
CPPP	Yes	Yes	Yes
HDLC	Yes	Yes	Yes
IP	Yes	Yes	Yes
RIP	Yes	Yes	Yes
RIPv2	Yes	Yes	Yes

Table 10 Cisco AS5200 Software Feature Sets (continued)

Feature	Feature Set		
	IP/Managed Modems	Desktop/Managed Modems	Enterprise/RMON/Managed Modems
IGRP	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes
OSPF	Yes	Yes	Yes
BGP	Yes	Yes	Yes
EGP	Yes	Yes	Yes
PIM	Yes	Yes	Yes
NHRP	Yes	Yes	Yes
ES-IS	—	—	Yes
IS-IS	—	—	Yes
Snapshot routing	Yes	Yes	Yes
NTP	Yes	Yes	Yes
Bridging (transparent and translational)	Yes	Yes	Yes
Multiring	Yes	Yes	Yes
LAN extension host	Yes	Yes	Yes
IPX	—	Yes	Yes
NLSP	—	Yes	Yes
IPXWAN 2.0	—	Yes	Yes
RTMP	—	Yes	Yes
SMRP	—	Yes	Yes
SRTP	—	—	Yes
AppleTalk Versions 1 and 2	—	Yes	Yes
AURP	—	Yes	Yes
DECnet IV	—	Yes	Yes
DECnet V	—	—	Yes
Apollo Domain	—	—	Yes
Banyan VINES	—	—	Yes
ISO CLNS	—	—	Yes
XNS	—	—	Yes
Lock-and-Key	Yes	Yes	Yes
MD5 routing authentication	Yes	Yes	Yes
Kerberized login	—	—	Yes
V.120	—	—	Yes
SRB	—	—	Yes
RSRB	—	—	Yes
APPN	—	—	—

Table 10 Cisco AS5200 Software Feature Sets (continued)

Feature	Feature Set		
	IP/Managed Modems	Desktop/Managed Modems	Enterprise/RMON/Managed Modems
FRAS BAN	—	—	Yes
DLSw (RFC 1795)	—	—	Yes
DLSw+	—	—	Yes
SDLC	—	—	Yes
SDLLC	—	—	Yes
STUN	—	—	Yes
TG/COS	—	—	Yes
QLLC	—	—	Yes
Bisync	—	—	Yes
DSPU	—	—	Yes
NetView Native Service Point	—	—	Yes
Protocol translation	—	—	Yes
TN3270	—	—	Yes
LAT	—	—	Yes
SRT bridging	—	—	Yes
XRemote	—	—	Yes
Telnet	Yes	Yes	Yes
PAD	Yes	Yes	Yes
AutoInstall	Yes	Yes	Yes
Modem autoconfiguring	—	—	Yes
Router monitoring	Yes	Yes	Yes
DHCP	Yes	Yes	Yes
NASI	—	—	—
NetBEUI over PPP	—	—	Yes
RADIUS	Yes	Yes	Yes
Modem Management	Yes	Yes	Yes

1 All feature sets include RMON alarm and events groups. Full, nine-group RMON support is included in the feature sets indicated.

Table 11 Cisco 4000 Series Software Feature Sets

Feature	Feature Set								
	IP	IP/IBM Base	IP/IPX	IP/IPX/IBM Base	IP/IPX/IBM/APPN	Desktop	Desktop/IBM Base	Enterprise	Enterprise/APPN
SNMP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RMON (events and alarms)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Asynchronous support (SLIP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARAP	—	—	—	—	—	—	—	—	—
Frame Relay	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SMDS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HDLC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NHRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ES-IS	—	—	—	—	—	—	—	Yes	Yes
IS-IS	—	—	—	—	—	—	—	Yes	Yes
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bridging (transparent and translational)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN extension host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NLSP	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RTMP	—	—	—	—	—	Yes	Yes	Yes	Yes
SMRP	—	—	—	—	—	Yes	Yes	Yes	Yes
S RTP	—	—	—	—	—	—	—	Yes	Yes
IPXWAN 2.0	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AppleTalk Versions 1 and 2	—	—	—	—	—	Yes	Yes	Yes	Yes
AURP	—	—	—	—	—	Yes	Yes	Yes	Yes

Table 11 Cisco 4000 Series Software Feature Sets (continued)

Feature	Feature Set								
	IP	IP/IBM Base	IP/IPX	IP/IPX/IBM Base	IP/IPX/IBM/APPN	Desktop	Desktop/IBM Base	Enterprise	Enterprise/APPN
DECnet IV	—	—	—	—	—	Yes	Yes	Yes	Yes
DECnet V	—	—	—	—	—	—	—	Yes	Yes
Apollo Domain	—	—	—	—	—	—	—	Yes	Yes
Banyan VINES	—	—	—	—	—	—	—	Yes	Yes
ISO CLNS	—	—	—	—	—	—	—	Yes	Yes
XNS	—	—	—	—	—	—	—	Yes	Yes
V.120	—	—	—	—	—	—	—	Yes	Yes
SRB	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
RSRB	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
APPN	—	—	—	—	Yes	—	—	—	Yes
FRAS BAN	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
DLSw (RFC 1795)	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
DLSw+	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
SDLC	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
SDLLC	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
STUN	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
TG/COS	—	—	—	—	—	—	—	Yes	Yes
QLLC	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
Bisync	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
DSPU	—	—	—	—	—	—	—	Yes	Yes
NetView Native Service Point	—	Yes	—	—	Yes	—	—	Yes	Yes
Protocol translation	—	—	—	—	—	—	—	Yes	Yes
TN3270	—	—	—	—	—	—	—	Yes	Yes
LAT	—	—	—	—	—	—	—	Yes	Yes
XRemote	—	—	—	—	—	—	—	Yes	Yes
Telnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PAD	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AutoInstall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Modem auto configuration	—	—	—	—	—	—	—	Yes	Yes
Router monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SRT Bridging	—	Yes	—	Yes	Yes	—	Yes	Yes	Yes
NetBEUI over PPP	—	—	—	—	—	—	—	Yes	Yes

Table 12 Cisco 3000 Series Software Feature Sets

Feature	Feature Set
	Enterprise
SNMP	Yes
RMON (events and alarms)	Yes
Asynchronous support (SLIP)	Yes
ARAP	Yes
Frame Relay	Yes
SMDS	Yes
X.25	Yes
ISDN	Yes
PPP	Yes
HDLC	Yes
IP	Yes
RIP	Yes
IGRP	Yes
Enhanced IGRP	Yes
OSPF	Yes
BGP	Yes
EGP	Yes
PIM	Yes
NHRP	Yes
ES-IS	Yes
IS-IS	Yes
Snapshot routing	Yes
NTP	Yes
Transparent bridging	Yes
Translational bridging	Yes
Multiring	Yes
LAN extension host	Yes
IPX	Yes
NLSP	Yes
IPXWAN 2.0	Yes
AppleTalk Versions 1 and 2	Yes
AURP	Yes
DECnet	Yes
Apollo Domain	Yes
Banyan VINES	Yes
ISO CLNS	Yes
XNS	Yes

Table 12 Cisco 3000 Series Software Feature Sets (continued)

Feature	Feature Set
	Enterprise
V.120	Yes
SRB	Yes
RSRB	Yes
SRT Bridging	Yes
APPN	—
FRAS BAN	Yes
DLSw (RFC 1795)	Yes
DLSw+	Yes
SDLC	Yes
SDLLC	Yes
STUN	Yes
TG/COS	Yes
QLLC	Yes
Bisync	Yes
DSPU	Yes
AutoInstall	Yes
Telnet	Yes
Protocol translation	Yes
TN3270	Yes
LAT	Yes
XRemote	Yes
DHCP	Yes
Router monitoring	Yes
NetBEUI over PPP	Yes

Table 13 Cisco 1003 and Cisco 1004 ISDN Routers Software Feature Sets

Feature	Feature Set			
	IP	IP/AT	IP/IPX	IP/IPX/AT
SNMP	Yes	Yes	Yes	Yes
Asynchronous support (SLIP)	—	—	—	—
ARAP	—	—	—	—
Frame Relay	—	—	—	—
SMDS	—	—	—	—
X.25	—	—	—	—
ISDN	Yes	Yes	Yes	Yes

Table 13 Cisco 1003 and Cisco 1004 ISDN Routers Software Feature Sets (continued)

Feature	Feature Set			
	IP	IP/AT	IP/IPX	IP/IPX/AT
PPP	Yes	Yes	Yes	Yes
HDLC	Yes	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes
IGRP	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes
OSPF	—	—	—	—
BGP	—	—	—	—
EGP	—	—	—	—
PIM	—	—	—	—
NHRP	—	—	—	—
ES-IS	—	—	—	—
IS-IS	—	—	—	—
Snapshot routing	Yes	Yes	Yes	Yes
NTP	—	—	—	—
Bridging (transparent)	Yes	Yes	Yes	Yes
Multiring	—	—	—	—
LAN extension host	—	—	—	—
IPX	—	—	Yes	Yes
NLSP	—	—	—	—
IPXWAN 2.0	—	—	Yes	Yes
AppleTalk Versions 1 and 2	—	Yes	—	Yes
AURP	—	—	—	—
DECnet IV	—	—	—	—
DECnet V	—	—	—	—
Apollo Domain	—	—	—	—
Banyan VINES	—	—	—	—
ISO CLNS	—	—	—	—
XNS	—	—	—	—
V.120	—	—	—	—
SRB	—	—	—	—
RSRB	—	—	—	—
DLSw (RFC 1795)	—	—	—	—

Table 13 Cisco 1003 and Cisco 1004 ISDN Routers Software Feature Sets (continued)

Feature	Feature Set			
	IP	IP/AT	IP/IPX	IP/IPX/AT
DLSw+	—	—	—	—
SDLC	—	—	—	—
SDLLC	—	—	—	—
STUN	—	—	—	—
TG/COS	—	—	—	—
QLLC	—	—	—	—
DSPU	—	—	—	—
Protocol translation	—	—	—	—
TN3270	—	—	—	—
LAT	—	—	—	—
XRemote	—	—	—	—
Telnet	Yes	Yes	Yes	Yes
AutoInstall	—	—	—	—
ClickStart	Yes	Yes	Yes	Yes
Router monitoring	Yes	Yes	Yes	Yes
DHCP	—	—	—	—
Lock-and-Key	—	—	—	—

Table 14 Cisco 1005 Router Software Feature Sets

Feature	Feature Set									
	IP	IP/AT	IP/AT/ X25	IP/IPX	IP/IPX/ X25	IP/IPX/ AT	IP/IPX/ AT/X25	IP/OSPF/ PIM	IP/IPX/ Async	IP/ Async
SNMP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Asynchronous support (SLIP)	—	—	—	—	—	—	—	—	Yes	Yes
ARAP	—	—	—	—	—	—	—	—	—	—
Frame Relay	Yes	Yes	—	Yes	—	Yes	—	Yes	—	—
SMDS	Yes	Yes	—	Yes	—	Yes	—	Yes	—	—
X.25	Yes	—	Yes	—	Yes	—	Yes	Yes	—	—
ISDN	—	—	—	—	—	—	—	—	—	—
PPP	Yes	Yes	—	Yes	—	Yes	—	Yes	Yes	Yes
HDLC	Yes	Yes	—	Yes	—	Yes	—	Yes	—	—
IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIPv2	—	—	—	—	—	—	—	—	—	—
IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 14 Cisco 1005 Router Software Feature Sets (continued)

Feature	Feature Set									
	IP	IP/AT	IP/AT/ X25	IP/IPX	IP/IPX/ X25	IP/IPX/ AT	IP/IPX/ AT/X25	IP/OSPF/ PIM	IP/IPX/ Async	IP/ Async
OSPF	—	—	—	—	—	—	—	Yes	—	—
BGP	—	—	—	—	—	—	—	—	—	—
EGP	—	—	—	—	—	—	—	—	—	—
PIM	—	—	—	—	—	—	—	Yes	—	—
NHRP	—	—	—	—	—	—	—	—	—	—
ES-IS	—	—	—	—	—	—	—	—	—	—
IS-IS	—	—	—	—	—	—	—	—	—	—
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	—	—	—	—	—	—	—	—	—	—
Bridging (transparent)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—
Multiring	—	—	—	—	—	—	—	—	—	—
LAN extension host	—	—	—	—	—	—	—	—	—	—
IPX	—	Yes	—	Yes	Yes	Yes	Yes	—	Yes	—
NLSP	—	—	—	—	—	—	—	—	—	—
IPXWAN 2.0	—	Yes	—	Yes	Yes	Yes	Yes	—	Yes	—
AppleTalk Versions 1 and 2	—	Yes	Yes	—	—	Yes	Yes	—	—	—
AURP	—	—	—	—	—	—	—	—	—	—
DECnet IV	—	—	—	—	—	—	—	—	—	—
DECnet V	—	—	—	—	—	—	—	—	—	—
Apollo Domain	—	—	—	—	—	—	—	—	—	—
Banyan VINES	—	—	—	—	—	—	—	—	—	—
ISO CLNS	—	—	—	—	—	—	—	—	—	—
XNS	—	—	—	—	—	—	—	—	—	—
Source-route bridging/ remote source-route bridging	—	—	—	—	—	—	—	—	—	—
DLSw (RFC 1795)	—	—	—	—	—	—	—	—	—	—
DLSw+	—	—	—	—	—	—	—	—	—	—
SDLC	—	—	—	—	—	—	—	—	—	—
SDLLC	—	—	—	—	—	—	—	—	—	—
STUN	—	—	—	—	—	—	—	—	—	—
TG/COS	—	—	—	—	—	—	—	—	—	—
QLLC	—	—	—	—	—	—	—	—	—	—
DSPU	—	—	—	—	—	—	—	—	—	—
Protocol translation	—	—	—	—	—	—	—	—	—	—
TN3270	—	—	—	—	—	—	—	—	—	—
LAT	—	—	—	—	—	—	—	—	—	—

Memory Requirements

Table 14 Cisco 1005 Router Software Feature Sets (continued)

Feature	Feature Set									
	IP	IP/AT	IP/AT/ X25	IP/IPX	IP/IPX/ X25	IP/IPX/ AT	IP/IPX/ AT/X25	IP/OSPF/ PIM	IP/IPX/ Async	IP/ Async
XRemote	—	—	—	—	—	—	—	—	—	—
Telnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AutoInstall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—
ClickStart	Yes	Yes	—	Yes	—	Yes	—	Yes	Yes	Yes
Router monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP	—	—	—	—	—	—	—	—	—	—
Lock-and-Key	—	—	—	—	—	—	—	—	—	—

Memory Requirements

Beginning with Cisco IOS Release 10.3, some software image (feature set) sizes exceed 4 MB and, when compressed, exceed 2 MB. Also, some systems now require more than 1 MB of main system memory for data structure tables.

For Cisco routers to take advantage of the Release 11.1 features, you need to have the code or main system memory as listed in Table 15. If you do not, you must upgrade your memory. Some platforms have specific chip or architecture requirements that affect what can be upgraded and in what increments.

The memory requirements listed in Table 15 are *minimum* requirements. Your specific hardware configuration and the software features you chose to deploy could require you to have more memory.

Note For the Cisco 7000 and Cisco 7010 routers to recognize Flash memory cards, 11.0 boot ROMs (or later) are required.

Table 15 Release 11.1 Memory Requirements

Hardware Platform	Minimum Required Code Memory	Required Main Memory	Release 11.1 Runs from
Cisco 1003 and Cisco 1004 ISDN Routers¹			
IP Set	2/4/8 MB optional Flash	4 MB RAM	RAM
IP/AT Set	2/4/8 MB optional Flash	4 MB RAM	RAM
IP/IPX Set	2/4/8 MB optional Flash	4 MB RAM	RAM
IP/IPX/AT Set	2/4/8 MB optional Flash	8 MB RAM	RAM
Cisco 1005 Router¹			
IP Set	2/4/8 MB optional Flash	4 MB RAM	RAM
IP/AT Set	2/4/8 MB optional Flash	4 MB RAM	RAM
IP/AT/X25 Set	2/4/8 MB optional Flash	4 MB RAM	RAM
IP/IPX Set	2/4/8 MB optional Flash	4 MB RAM	RAM

Table 15 Release 11.1 Memory Requirements (continued)

Hardware Platform	Minimum Required Code Memory	Required Main Memory	Release 11.1 Runs from
IP/IPX/AT/X25 Set	2/4/8 MB optional Flash	8 MB RAM	RAM
IP/IPX/AT Set	2/4/8 MB optional Flash	8 MB RAM	RAM
IP/IPX/X25 Set	2/4/8 MB optional Flash	4 MB RAM	RAM
IP/IPX/Async Set	2/4/8 MB optional Flash	4 MB RAM	RAM
IP/Async Set	2/4/8 MB optional Flash	4 MB RAM	RAM
Cisco 2500 Series			
IP Set	4 MB Flash	2 MB RAM ²	Flash
IP/RMON Set	4 MB Flash	4 MB RAM	Flash
IP/IBM Set	8 MB Flash	4 MB RAM	Flash
IP/IBM/RMON Set	8 MB Flash	4 MB RAM	Flash
IP/IPX Set	8 MB Flash	4 MB RAM	Flash
IP/IPX/RMON Set	8 MB Flash	4 MB RAM	Flash
IP/IPX/IBM Set	8 MB Flash	4 MB RAM	Flash
IP/IPX/IBM/RMON Set	8 MB Flash	4 MB RAM	Flash
IP/IPX/IBM/APPN Set	8 MB Flash	8 MB RAM	Flash
Desktop Set	8 MB Flash	4 MB RAM	Flash
Desktop/IBM Set	8 MB Flash	4 MB RAM	Flash
Enterprise Set	8 MB Flash	16 MB RAM	Flash
Enterprise/RMON Set	8 MB Flash	6 MB RAM	Flash
Enterprise/APPN Set	16 MB Flash	8 MB RAM	Flash
Cisco Frame Relay Access Device (CFRAD) Set	4 MB Flash	2 MB RAM ²	Flash
Remote Access Server	4 MB Flash	4 MB RAM	Flash
ISDN Set	4 MB Flash	2 MB RAM	Flash
LAN FRAD Set	4 MB Flash	4 MB RAM	Flash
OSPF LANFRAD Set ³	4 MB Flash	4 MB RAM	Flash
Cisco AS5100⁴			
IP Set	4 MB Flash per card	6 MB RAM per card	Flash
IP/RMON Set	4 MB Flash	6 MB RAM	Flash
IP/IBM Base Set	8 MB Flash	6 MB RAM	Flash
IP/IBM/RMON Set	8 MB Flash	6 MB RAM	Flash
IP/IPX Set	8 MB Flash per card	6 MB RAM per card	Flash
IP/IPX/RMON Set	8 MB Flash	6 MB RAM	Flash
IP/IPX/IBM Base Set	8 MB Flash	6 MB RAM	Flash
IP/IPX/IBM/RMON Set	8 MB Flash	6 MB RAM	Flash
Desktop Set	8 MB Flash per card	6 MB RAM per card	Flash
Desktop/IBM Base Set	8 MB Flash	6 MB RAM	Flash

Table 15 Release 11.1 Memory Requirements (continued)

Hardware Platform	Minimum Required Code Memory	Required Main Memory		Release 11.1 Runs from
Enterprise Set	8 MB Flash per card	16 MB RAM per card		Flash
Enterprise/RMON Set	8 MB Flash	6 MB RAM		Flash
Remote Access Server	4 MB Flash per card	6 MB RAM per card		Flash
Cisco AS5200				
IP/Managed Modems Set	8 MB Flash	8 MB RAM		Flash
Desktop/Managed Modems Set	8 MB Flash	8 MB RAM		Flash
Enterprise/RMON/Managed Modems Set	8 MB Flash	8 MB RAM		Flash
Cisco 3101, Cisco 3102, Cisco 3103	8 MB Flash	4 MB RAM		Flash
	4 MB Flash	16 MB RAM		RAM
Cisco 3104, Cisco 3204	8 MB Flash	4 MB RAM		Flash
	4 MB Flash	8 MB RAM		RAM
Cisco 4000/4000-M		Cisco 4000	Cisco 4000-M	
IP Set	4 MB Flash	16 MB RAM	8 MB RAM	RAM
IP/IBM Set	4 MB Flash	16 MB RAM	8 MB RAM	RAM
IP/IPX Set	4 MB Flash	16 MB RAM	8 MB RAM	RAM
IP/IPX/IBM Set	4 MB Flash	16 MB RAM	8 MB RAM	RAM
IP/IPX/IBM/APPN Set	4 MB Flash	16 MB RAM	16 MB RAM	RAM
Desktop Set	4 MB Flash	16 MB RAM	8 MB RAM	RAM
Desktop/IBM Set	4 MB Flash	16 MB RAM	8 MB RAM	RAM
Enterprise Set	4 MB Flash	16 MB RAM	16 MB RAM	RAM
Enterprise/APPN Set	4 MB Flash	16 MB RAM	16 MB RAM	RAM
Cisco 4500/4500-M		Cisco 4500	Cisco 4500-M	
IP Set	4 MB Flash	8 MB RAM	8 MB RAM ⁵	RAM
IP/IBM Set	4 MB Flash	32 MB RAM	16 MB RAM	RAM
IP/IPX Set	4 MB Flash	8 MB RAM	8 MB RAM ⁵	RAM
IP/IPX/IBM Set	4 MB Flash	32 MB RAM	16 MB RAM	RAM
IP/IPX/IBM/APPN Set	4 MB Flash	32 MB RAM	16 MB RAM	RAM
Desktop Set	4 MB Flash	32 MB RAM	16 MB RAM	RAM
Desktop/IBM Set	4 MB Flash	32 MB RAM	16 MB RAM	RAM
Enterprise Set	4 MB Flash	32 MB RAM	16 MB RAM	RAM
Enterprise/APPN Set	8 MB Flash	32 MB RAM	16 MB RAM	RAM
Cisco 4700				
IP Set	4 MB Flash	16 MB RAM		RAM
IP/IBM Set	4 MB Flash	16 MB RAM		RAM
IP/IPX Set	4 MB Flash	16 MB RAM		RAM

Table 15 Release 11.1 Memory Requirements (continued)

Hardware Platform	Minimum Required Code Memory	Required Main Memory	Release 11.1 Runs from
IP/IPX/IBM Set	4 MB Flash	16 MB RAM	RAM
IP/IPX/IBM/APPN Set	4 MB Flash	16 MB RAM	RAM
Desktop Set	4 MB Flash	16 MB RAM	RAM
Desktop/IBM Set	4 MB Flash	16 MB RAM	RAM
Enterprise Set	4 MB Flash	16 MB RAM	RAM
Enterprise/APPN Set	8 MB Flash	16 MB RAM	RAM
Cisco 7000⁶, Cisco 7010			
IP Set	8 MB Flash	16 MB RAM	RAM
IP/IPX/IBM Set	8 MB Flash	16 MB RAM	RAM
IP/IPX/IBM/APPN Set	8 MB Flash	16 MB RAM	RAM
Desktop/IBM Set	8 MB Flash	16 MB RAM	RAM
Enterprise Set	8/16 MB Flash memory card	16 MB RAM	RAM
Enterprise/APPN Set	8 MB Flash	16 MB RAM	RAM
IP/VIP Set	8 MB Flash	16 MB RAM	RAM
IP/IPX/IBM/VIP Set	8 MB Flash	16 MB RAM	RAM
IP/IPX/IBM/APPN/VIP Set	8 MB Flash	16 MB RAM	RAM
Desktop/IBM/VIP Set	8 MB Flash	16 MB RAM	RAM
Enterprise/VIP Set	8/16 MB Flash memory card	16 MB RAM	RAM
Enterprise/APPN/VIP Set	8 MB Flash	16 MB RAM	RAM
Source-Route Switch	4 MB Flash	16 MB RAM	RAM
Cisco 7200			
Enterprise Set	8/16/20 MB Flash memory card	16 MB RAM	RAM
Enterprise/APPN Set	8/16/20 MB Flash memory card	24 MB RAM	RAM
Desktop/IBM Set	8/16/20 MB Flash memory card	16 MB RAM	RAM
Network Layer 3 Switching Set	8/16/20 MB Flash memory card	16 MB RAM	RAM
Cisco 7505, Cisco 7507, Cisco 7513, Cisco 7000 with RSP7000			
		Cisco 7513 only	All Others
IP Set	8 MB Flash	16 MB RAM	16 MB RAM RAM
IP/IPX/IBM Set	8 MB Flash	16 MB RAM	16 MB RAM RAM
IP/IPX/IBM/APPN Set	8 MB Flash	24 MB RAM	24 MB RAM RAM
Desktop/IBM Set	8 MB Flash	16 MB RAM	16 MB RAM RAM
Enterprise Set	8 MB Flash memory card	24 MB RAM	16 MB RAM RAM
Enterprise/APPN Set	8 MB Flash memory card	32 MB RAM	24 MB RAM RAM

Table 15 Release 11.1 Memory Requirements (continued)

Hardware Platform	Minimum Required Code Memory	Required Main Memory		Release 11.1 Runs from
IP/VIP Set	8 MB Flash	24 MB RAM ⁷	24 MB RAM ⁸	RAM
IP/IPX/IBM/VIP Set	8 MB Flash	24 MB RAM ⁷	24 MB RAM ⁸	RAM
IP/IPX/IBM/APPN/VIP Set	8 MB Flash	24 MB RAM ⁷	24 MB RAM ⁸	RAM
Desktop/IBM/VIP Set	8 MB Flash	24 MB RAM ⁷	24 MB RAM ⁸	RAM
Enterprise/VIP Set	8/16/20 MB Flash memory card	32 MB RAM ⁷	24 MB RAM ⁸	RAM
Enterprise/APPN/VIP Set	8/16/20 MB Flash memory card	32 MB RAM ⁷	32 MB RAM	RAM

- 1 If you need to upgrade the main memory for your Cisco 1003, Cisco 1004, or Cisco 1005 router, be sure to order the upgrade specific to your router.
- 2 For Cisco 2509 through Cisco 2512 access servers, and the Cisco 2522 and Cisco 2523 routers, 4 MB DRAM is the minimum recommended.
- 3 The OSPF LANFRAD feature set is available in Release 11.1(9) and later.
- 4 Memory requirements listed are per card. Each AS5100 supports up to three cards, so that the maximum memory needed for any AS5100 is three times the listed number.
- 5 The Cisco 4500 requires 16 MB DRAM when two NP-CT1 or two NP-CE1 Network Processor Modules are installed in the chassis.
- 6 Except the Cisco 7000 with RSP7000. For a Cisco 7000 with an RSP7000 card, refer to the memory requirements for Cisco 75xx platforms.
- 7 To use the HSA feature, 32 MB DRAM is the minimum recommended memory (per RSP).
- 8 To use the HSA feature, 24 MB DRAM is the minimum recommended memory (per RSP).

New Features in Release 11.1(6) and Later 11.1 Releases

There are no new software features or platform support added in Release 11.1(6) or in any later Cisco IOS 11.1 release. Release 11.1(5) was the last maintenance release to add new features or platform support.

New Features in Release 11.1(5)

This section describes the software enhancements that were added to Release 11.1(5).

Support for Second-Generation Channel Interface (CIP2)

The CIP2 is the follow-on product to the original CIP, and provides increases in performance, capacity, reliability, and serviceability.

The CIP2 includes the following improvements over the original CIP:

- A secondary processor cache (providing a 50 percent performance increase)
- Increased memory options (CIP2 memory configurations come in 32 MB, 64 MB, and 128 MB)
- An on-board boot Flash, which is software upgradable (allowing upgrades to the boot microcode without physical replacement of parts)

The CIP2 operates with the CxBus in the Cisco 7000 series routers with either of the following processor types:

- Router Processor (RP) and Switch Processor (SP) (or Silicon Switch Processor [SSP]) combination

- Cisco 7000 series Route Processor (RSP7000) and Cisco 7000 series chassis interface (RSP7000CI) combination

The CIP2 operates with the CyBus in the Cisco 7500 series routers, which use the Route Switch Processor (RSP).

CIP microcode is required if you will be using the CIP2. See the “Important Notes” section for more information about CIP microcode.

Support for Cisco 7200 Series Platforms

The Cisco 7200 series is a series of multiprotocol routers that delivers the high-performance, high port density, and availability features typically associated with high-end systems. The Cisco 7200 series supports Cisco’s Inter-Switch Link (ISL) Protocol for transporting virtual LANs (VLANs) across Fast Ethernet. VLANs enable the logical definition of bridge groups that can be overlaid on the physical network.

The Cisco 7206 router can be configured with up to 48 Ethernet ports, 24 Token Ring ports, 24 serial ports, 7 Fast Ethernet ports, and 6 FDDI ports.

Four feature sets are available in Cisco IOS Release 11.1(5) to support the Cisco 7200 series:

- Network Layer 3 Switching
- Desktop/IBM
- Enterprise
- Enterprise/APPN

Refer to Table 6 for a list of features included in each of these sets.

Support for the Cisco AS5200

The Cisco AS5200 Universal Access Server provides mixed asynchronous and ISDN line service to accommodate both mobile users and telecommuters with one server. This line of access servers contains channel service units (CSUs), channel banks, communication servers, switches, routers, and 48 modems in one standalone chassis that accommodates up to 48 users dialing-in simultaneously.

The following feature sets are available for the Cisco AS5200. Refer to Table 10 for a complete list of the features provided in these sets.

- IP/Managed Modems
- Desktop/Managed Modems
- Enterprise/RMON/Managed Modems

Cisco Web Browser Interface

A Web browser interface is available on any Cisco product running Cisco IOS Release 11.1(5) software, or later. This Web interface allows you to log in to a router or access server and process Cisco IOS software commands. It operates much like the command line interface (CLI) on a terminal. To process commands using the Web interface, click on the “Monitor the Router” link from the router’s home page. All Cisco products running Cisco IOS Release 11.0(10) or 11.1(5) software or later have a home page.

ClickStart Enhancements

ClickStart, which allows you to use a standard Web browser to configure and monitor a Cisco router, has been enhanced. You can now use it to configure a Cisco 1005 router that has one Ethernet and either one Frame Relay or one asynchronous serial interface. For additional information about ClickStart, see the “New Features in Release 11.1(2)” section.

DLSw+ Enhancements

In Release 11.1(5), DLSw+ can be used as a “virtual” data-link control for other SNA features in the Cisco IOS software, including:

- LAN Network Manager (LNM) over DLSw+

LNM over DLSw+ allows DLSw+ to be used in Token Ring networks that are managed by IBM’s LNM software. Using this feature, LNM can be used to manage Token Ring LANs, control access units, and Token Ring attached devices over a DLSw+ network. All management functions continue to operate as they would in a source-route bridged network or an RSRB network.

- Downstream physical unit (DSPU) over DLSw+

DSPU over DLSw+ allows Cisco’s DSPU feature to operate in conjunction with DLSw+ in the same router. DLSw+ can be used either upstream (toward the mainframe) or downstream (away from the mainframe) of DSPU. DSPU concentration consolidates the appearance of multiple physical units (PUs) into a single PU appearance to VTAM, minimizing memory and cycles in central site resources (VTAM, NCP, and routers) and speeding network startup.

- SNA service point support over DLSw+

SNA service point over DLSw+ allows Cisco’s SNA service point feature to be used in conjunction with DLSw+ in the same router. Using this feature, SNA service point can be configured in remote routers, and DLSw+ can provide the path for the remote service point PU to communicate with NetView. This allows full management visibility of resources from a NetView 390 console, while concurrently offering the value-added features of DLSw+ in an SNA network.

Support for Fast Ethernet—100E NIM for Cisco 4500 and Cisco 4700

Support for the Fast Ethernet network interface module (NIM) is added in Release 11.1(5). The Cisco 4500 series (Cisco 4500, Cisco 4500-M, Cisco 4700, and Cisco 4700-M) routers support a Fast Ethernet network interface module (NIM) with a PCI bus interface to its DEC21140 controller chip. The Fast Ethernet NIM for Cisco 4500 and Cisco 4700 provides a single full-duplex, 100-Mbps Ethernet interface.

MIP Flow Control

Custom queuing and priority queuing are now available for the MultiChannel Interface Processor (MIP) in RSP systems (Cisco 7500 series and Cisco 7000 series with RSP7000).

NetFlow Switching

NetFlow Switching brings the benefits of connection-oriented switching to network layer devices. With NetFlow Switching, routers become network switches able to combine quality-of-service and security capabilities with high performance. Coupled with the large bandwidth capacity of Cisco's 7500 series, NetFlow Switching allows customers to provide many of the capabilities associated with ATM on their existing routed infrastructure.

NetFlow Switching operates at the network and transport layers so it can incorporate user and application oriented information to make switching decisions such as allowing access and providing specific quality of service. NetFlow Switching achieves high performance by operating on connection-like flows between source/destination IP addresses. Cisco LAN Switches such as the Catalyst 5000, will be able to take advantage of NetFlow Switching with the incorporation of support for multilayer switching and Cisco IOS software.

Optimum Switching

Optimum Switching is quite similar to fast switching from a high level. The optimum switching cache is a separate cache using a more efficient data structure than the fast-switching cache to achieve better performance. In addition, the data caching at the processor is optimized to boost performance further. Optimum Switching requires the architecture of the Cisco 7500 series Route Switch Processor (RSP).

Support for the Packet OC-3 Interface

Support for the Packet OC-3 interface on the Packet over SONET Interface Processor (POSIP) is added in Release 11.1(5). The POSIP for Cisco 7500 series and Cisco RSP/7000 routers provides a single 155.520-Mbps, OC-3 physical layer interface for packet-based traffic. This OC-3 interface is fully compatible with SONET and Synchronous Digital Hierarchy (SDH) network facilities and is compliant with RFC 1619, "PPP over SONET/SDH," and RFC 1662, "PPP in HDLC-like Framing."

To support this interface, Packet over SONET Interface Processor microcode is also added to this release.

New Features in Release 11.1(4)

This section describes the software enhancements that were added to Release 11.1(4).

New Feature Sets for Cisco 1005

Cisco IOS Release 11.1(4) supports two new Cisco 1005 feature sets:

- IP/Async
- IP/IPX/Async

Refer to Table 14 for a list of features included in each of these sets.

High System Availability (HSA)

HSA is an advanced software feature of the Cisco 7500 series architecture. HSA increases the availability and uptime of the Cisco 7507 and Cisco 7513 routers. This increase is accomplished through a master/slave relationship between two RSPs. If the slave RSP detects an error condition, it automatically takes control and reboots the system without user intervention. This automatic action minimizes network interruption and increases system availability.

Note HSA requires a ROM Monitor upgrade. See the “Important Notes” section for more information.

HSA can be used in the following situations:

- *Hardware backup.* Protects against single processor failure.
- *Software error protection.* Protects against critical software errors by keeping different software images on each RSP.
- *Configuration switching.* Enables users to store different configurations in each RSP. If the new feature configuration on the master causes a system failure, the slave RSP takes over the routing function after a system reboot.

HSA is only supported in feature set images that include a “v” in the name, such as the RSP subset image `rsp-jv-mz.111-4`.

See the “Important Notes” section for more information.

New Features in Release 11.1(3)

This section describes the software enhancements that were added to Release 11.1(3).

Channel Service Unit/Data Service Unit (CSU/DSU) Management Information Base (MIB)

This Cisco-proprietary MIB for integrated CSU/DSU is available in Release 11.1(3) and later. This MIB is available for use with the Cisco 2524 and Cisco 2525 products, and is for T1 and switched 56-kbps interfaces. It enables network managers to retrieve line statistics and CSU/DSU configuration data.

Support for the Cisco 2524 and Cisco 2525 Platforms

The Cisco 2524 and Cisco 2525 routers eliminate the need for a separate terminal adapter on an ISDN line, or separate channel service unit/data service units (CSU/DSUs) on synchronous serial WAN interfaces.

These platforms support a removable BRI or BRI with integrated NT1 interface, a LAN interface (either Ethernet or Token Ring), and two WAN interface slots.

New commands have been added to the Cisco IOS software to support the Cisco 2524 and Cisco 2525.

The Cisco 2524 and Cisco 2525 support RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types*.

Cisco IOS Release 11.0(5) also supports the Cisco 2524 and Cisco 2525 routers.

Note The Cisco 2524 and Cisco 2525 require a minimum 11.0(5)-level boot ROM.

Support for the Cisco 2520, Cisco 2521, Cisco 2522, and Cisco 2523 Platforms

The Cisco 2520 through Cisco 2523 models merge router and communication server features to serve access and telecommuting requirements in a single platform. WAN aggregation, telecommuting, branch office, and IBM protocol applications are well-suited to these Cisco devices.

The interfaces available in each model are shown below.

Cisco 2520	1 Ethernet, 2 high-speed synchronous serial, 2 low-speed synchronous/asynchronous serial, 1 ISDN BRI
Cisco 2521	1 Token Ring, 2 high-speed synchronous serial, 2 low-speed synchronous/asynchronous serial, 1 ISDN BRI
Cisco 2522	1 Ethernet, 2 high-speed synchronous serial, 8 low-speed synchronous/asynchronous serial, 1 ISDN BRI
Cisco 2523	1 Token Ring, 2 high-speed synchronous serial, 8 low-speed synchronous/asynchronous serial, 1 ISDN BRI

The low-speed serial interfaces (maximum speed 115.2 kbps) are capable of supporting both synchronous and asynchronous protocols.

LAN Frame Relay Access Device (FRAD) Feature Set

The LAN FRAD feature set is supported on the Cisco 2501, Cisco 2502, Cisco 2520, Cisco 2521, Cisco 2522, and Cisco 2523 routers.

IP/Open Shortest Path First (OSPF)/Protocol Independent Multicast (PIM) Feature Set

This feature set for the Cisco 1005 router contains the functionality of the IP feature set, but includes support for OSPF and PIM.

New Features in Release 11.1(2)

This section describes the software enhancements that were added to Release 11.1(2).

New Configuration Tool—ClickStart

ClickStart allows you to use a standard Web browser, such as Netscape or Mosaic, to configure and monitor a Cisco router. You can use ClickStart to configure a Cisco 1003 or Cisco 1004 router that has one Ethernet and one ISDN Basic Rate Interface (BRI). You configure the router to dial your Internet service provider, and your Internet service provider supplies an ISDN connection to the Internet. You can also use ClickStart to monitor any Cisco router that is running Cisco IOS Release 11.1(2), Release 11.0(6), or later.

If you have a Cisco 1003 or Cisco 1004 router, you can automatically use ClickStart to monitor your router.

If you have any other Cisco router, you must enable ClickStart before you can use it to monitor your router. To do this, follow this procedure:

- Step 1** To enable ClickStart, use the **ip http server** global configuration command.
- Step 2** By default, ClickStart uses port 80 to communicate with the router. If you want to configure a different port, use the **ip http port number** global configuration command. The *number* argument is the number of the port you want to use for ClickStart.

Virtual LAN (VLAN) Routing

Release 11.1(2) supports IP and IPX routing and transparent 802.1d bridging between Inter-Switch Link (ISL)-encapsulated VLANs on Cisco 7000 and Cisco 7500 series routers with RSPs. This functionality is also supported on the Cisco 7000 with Route Processors (RPs) and Switch Processors (SPs) and/or Silicon Switch Processors (SSPs), with limited performance.

VLAN allows you to logically segment end-user ports into autonomous virtual workgroups. Logical segmentation provides benefits in address administration, security, and management of network broadcast activity across the enterprise. To communicate between VLANs, a routing function is required (or bridging, in the case of nonroutable protocol types). Cisco IOS software offers two alternatives for communication between VLANs: dedicated VLAN ports and VLAN subinterfaces.

- Dedicated VLAN ports allow you to assign a physical interface to each VLAN group. This is a cost-effective approach if you run high-bandwidth applications between VLANs.
- VLAN subinterfaces enable multiple VLANs to be configured on a single physical interface. A VLAN interface, referred to as a *trunk interface*, logically transports multiple VLANs across Fast Ethernet by encapsulating with Cisco Inter-Switch Link (ISL). Trunked VLAN subinterfaces

conserve router or switch physical ports and are a cost-effective solution for environments where the majority of traffic is within a VLAN.

Note that the only IPX encapsulation supported in ISL is 802.3.

Security access lists for controlling the type of access within or outside of a VLAN can be configured using subinterfaces within Cisco routers. This control provides an additional layer of security when VLANs are interconnected.

VLAN routing

- Enables communications between logically defined VLAN groups, while maintaining the integrity of VLAN firewalls (security, traffic isolation, and common logical addressing)
- Performs a central role in planning and configuring VLANs within a switched internetwork
- Conserves router and switch physical interfaces
- Provides VLAN communications within workgroups, across the campus, and across WANs
- Allows bridging mode (Layer 2) for end-station protocols that function only at Layer 2 (for example, NetBIOS and LAT)
- Enables security access lists for controlling the type of access within or outside of a VLAN
- Provides a wide range of VLAN configuration options with concurrent routing and VLAN forwarding where both Layer 2 and Layer 3 applications reside within the network

New Features in Release 11.1(1)

This section describes new features and enhancements available in the initial Cisco IOS Release 11.1 of the router products software.

Platform Support

This section describes new platforms and interfaces supported by the initial release of Cisco IOS Release 11.1.

Cisco 1005

The Cisco 1005 synchronous serial router connects small, remote Ethernet LANs to WANs over leased lines, Frame Relay, Switched Multimegabit Data Service (SMDS), Switched-56, and X.25. The Cisco 1005 is already supported on Releases 11.0(4), 10.3(6), and higher.

AAL3/4 E3/DS3 for Cisco 4500 and Cisco 4700 ATM NIM

Asynchronous Transfer Mode (ATM) is supported on the Cisco 4500 and Cisco 4700 routers, using the Cisco ATM Network Interface Module (NIM) cards. The ATM adaptation layer 3/4 (AAL3/4), and additional NIM variants for use with E3/DS3 services are supported in Release 11.1. (Support is also available in Cisco IOS Release 11.0(5).) ATM on the Cisco 4500 and Cisco 4700 routers is configured differently from that on the Cisco 7000 routers. Refer to the *Wide-Area Networking Configuration Guide* for configuration information.

Backbone Protocol Routing Features

This section describes the backbone protocol routing features that are new in the initial release of Cisco IOS Release 11.1.

TCP/IP Features

The following features have been added to the Cisco IOS TCP/IP software:

- Next Hop Resolution Protocol (NHRP) Enhancements for IPX—NHRP allows routers to dynamically discover data-link addresses for other routers on a WAN cloud, eliminating the need to configure network layer- and data link layer-addresses for all neighbors on a WAN cloud.

NHRP has been enhanced to support IPX in addition to the IP support introduced in Cisco IOS Release 10.3. With NHRP, you can dynamically resolve IPX addresses in large-scale WAN environments in addition to resolving IP addresses. NHRP will operate using ATM, SMDS, or GRE tunneling.

- Fast Install for Static Routes—Floating static routes are static routes that have a higher administrative distance than other dynamic or static routes, and are often used to back up a leased-line or Frame Relay service in conjunction with the Cisco IOS software dial-on-demand routing (DDR) functionality.

Fast Install ensures that the floating static route is installed as soon as either the routing protocol or interface reports a connectivity loss. This enables faster convergence when using dial-on-demand circuits to back up, for example, a leased-line or Frame Relay service.

- Fast-Switched Generic Route Encapsulation (GRE)—GRE provides the ability to handle multiple network protocols in the same tunnel. In addition, GRE includes optional sequencing and an optional security key. This feature enables fast switching for GRE tunnels. Previously, encapsulation and de-encapsulation were process switched. The increased performance of GRE tunnels aids Cisco 2500, Cisco 4000, and Cisco 7500 series users.
- Routing Information Protocol Version 2 (RIPv2)—While RIPv2 shares the same basic algorithms as RIPv1, it supports several new features:
 - Authentication: RIPv2 offers two modes of authentication, a plain-text password or MD5 authentication.

Note MD5 authentication in RIPv2 is not supported in Release 11.1(1) or Release 11.1(2).

- Subnet Masks: Subnet mask information makes RIP more useful in a variety of environments and allows the use of variable subnet masks on the network. Subnet masks are also necessary for implementation of “classless” addressing, such as classless interdomain routing (CIDR).
- Multicasting: RIPv2 packets can be multicast instead of being broadcast. Using an IP multicast address reduces the load on hosts that do not support routing protocols. It also allows RIPv2 routers to share information that RIPv1 routers cannot hear. This is useful since a RIPv1 router may misinterpret route information because it cannot apply the supplied subnet mask.
- External Route Tags: The route tag field may be used to propagate information acquired from an Exterior Gateway Protocol (EGP).

If you implement RIP you can now make more efficient use of allocated address space by implementing variable-length subnet masks (VLSM) within networks.

RIPv2 adds to the choices of classless routing protocols supported by Cisco IOS software. This is the primary mechanism to improve scaling of the Internet routing system as a whole.

Note Care must be taken when combining RIPv2 routers and RIPv1-compatible hosts. Because it cannot apply the supplied subnet mask, a RIPv1 host may misinterpret route information.

In some multi-homed environments, hosts listen to RIPv1 broadcasts to enable them to switch their traffic to a new router, should the main router or connection fail. Cisco recommends the choice of alternative technologies such as RFC 792 ICMP Router Discovery Protocol, or Hot Standby Router Protocol (HSRP) as alternatives for hosts.

Desktop Protocols

This section describes the desktop protocol features that are new in the initial release of Cisco IOS Release 11.1.

AppleTalk Features

The following features have been added to Cisco's AppleTalk software:

- Simple Multicast Routing Protocol (SMRP) Fast Switching—Fast switching of the AppleTalk multicast routing protocol, SMRP, is supported for Cisco 2500, Cisco 4000, Cisco 4500, Cisco 7000, and Cisco 7500 series routers.

SMRP optimizes Apple Computer's Quicktime Conferencing (QTC) traffic flow of audio, video, and shared data over AppleTalk-based routed networks. QTC is a powerful multimedia application that enables multiple end stations to participate in multipoint, collaborative, multimedia operations. SMRP is the networking complement of QTC. SMRP optimizes communication among QTC end systems with reduced CPU utilization by eliminating the duplicate transmission of identical packets to multiple receivers. SMRP streamlines network throughput by eliminating duplicate and unnecessary traffic propagation. It dynamically establishes unique shortest-path distribution trees to restrict traffic propagation to only those parts of the network that contain receiving end stations. SMRP provides just-in-time packet duplication upon encountering a branch in the distribution tree.

Cisco routers have been SMRP-enabled since Cisco IOS Release 11.0. New in this release is enhanced performance through fast switching on the Cisco 4000 and Cisco 7500 series routers.

ISO CLNS Features

- Target Identifier Address Resolution Protocol (TARP) Support—TARP is an address resolution protocol for mapping Synchronous Optical Network (SONET) identifiers to OSI NSAPs (much like a DNS, which will return an NSAP given a name string, or the reverse). Some applications that run on SONET devices identify these devices by a target identifier (TID). Cisco TARP-enabled routers cache TID-to-network address mapping. Because these applications usually run over OSI, the network addresses are OSI NSAPs.

The benefits for TARP include:

- Implementing the Bellcore TARP specification for Intermediate Systems.
- Networking support for applications (typically used by telephone companies) running on SONET devices.

- Mapping SONET identifiers (for example, TID) to OSI NSAPs (much like a DNS, which will return an NSAP given a name string, or the reverse).
- Propagating TARP PDUs not destined for the router.

Novell Features

The following features have been added to Cisco's Novell software:

- **Enhanced IGRP to NLSP Route Redistribution**—Enhanced IGRP to NLSP Route Redistribution is the method by which routing information is passed between Enhanced IGRP and NLSP routing domains in IPX networks. While route redistribution between Enhanced IGRP and IPX RIP is automatic by default (as is redistribution between NLSP and IPX RIP), this new Cisco IOS software feature adds comprehensive tools for enabling the direct flow of routing information between Enhanced IGRP and NLSP networks.

Enhanced IGRP to NLSP route redistribution provides unparalleled flexibility to users of large IPX networks. Previously, when IPX networks grew to the point where RIP and SAP were no longer able to adequately support them, users were forced to upgrade to either Enhanced IGRP or NLSP to gain the scalability benefits inherent to these protocols. Through the use of Enhanced IGRP to NLSP route redistribution, users may now select the routing protocol, or combination of routing protocols, that meets their needs. For example, an IPX network can now be built that uses a combination of RIP and NLSP on the NetWare servers and uses Enhanced IGRP as the single backbone protocol.

- **IPX Input Access Lists**—This is a security enhancement feature that provides the capability of applying access lists to incoming router interfaces and the added flexibility in building secure IPX networks. The IPX input access lists can be used to validate user information at the borders of networks and to build more sophisticated firewalls. By moving the filter process from an outgoing to an incoming interface, IPX Input Access Lists enhance security and reduce processor overhead by denying packets before they transit the router. They also provide the capability of filtering traffic at the originating end of GRE-tunneled networks.

Note IPX Input Access Lists can be fast switched, but they cannot be enabled on a cBus-based router configured for autonomous or SSE switching.

- **IPX Per-host Load Sharing**—This load-sharing process transmits successive packets (or a traffic stream) for a given end host over the same path when multiple equal-cost paths are present. Load sharing is achieved when traffic streams for different end hosts use different paths.

Other implementations of load sharing rely on a round-robin algorithm that transmits successive packets over alternate, equal-cost paths without regard to the end host. Round-robin load sharing increases the likelihood of packets being received out of order at the destination host.

Out-of-order packets must often be retransmitted in IPX environments, leading to much higher application delay and network congestion.

Because per-host load sharing sends all packets destined for an end host over the same media interface, the likelihood of packets being received out of order is greatly reduced and minimizes retransmissions and network overhead.

- **NetWare Link Services Protocol (NLSP) Route Aggregation**—NLSP is the link-state routing protocol for IPX networks. Cisco IOS software now includes additional functionality for NLSP that permits multiple NLSP areas to directly and succinctly share information without using IPX RIP between groups. NLSP route aggregation is designed to be compatible with the NetWare Link Services Protocol (NLSP) Specification, Revision 1.1, from Novell.

NLSP route aggregation provides several important benefits to users of large IPX networks:

- Ability to divide IPX networks into multiple NLSP areas.

It is recommended that large IPX networks (conservatively estimated as those containing over 400 network addresses according to Novell design guidelines) be split into smaller NLSP areas. Previously, NLSP was specified as a single-area routing protocol, meaning that individual NLSP areas had to use IPX RIP to communicate routing information. Cisco's new implementation of NLSP allows multiple instances of NLSP to run on the same router, and allows routing information to be redistributed between areas. This allows much larger NLSP networks to exist.

- Routing information is shared more efficiently in properly designed hierarchically addressed networks.

When possible, ranges of addresses within an area can be aggregated (or summarized) into a single route entry. Because the number of these entries in the routing databases is minimized and update traffic is reduced, aggregation results in a much more efficient routing process.

Note To derive the maximum benefit from NLSP route aggregation it is important that network addresses be assigned properly in IPX environments. Network addresses should be assigned in a structured, hierarchical manner. Additionally, since other IPX routing protocols cannot interpret summarized route entries, the use of NLSP route aggregation in a Cisco router that is also using IPX RIP or Enhanced IGRP must be carefully planned and implemented.

- Raw FDDI IPX Encapsulation—Support for an additional IPX encapsulation on FDDI media is added. Cisco now supports routing of FDDI_RAW along with two standard FDDI encapsulations: FDDI_SNAP and FDDI_802.2. FDDI_RAW encapsulation is most often encountered when bridges or switches connect Ethernet-based Novell networks using the 802.3_Ethernet encapsulation to FDDI-based networks. The FDDI_RAW encapsulation is not currently supported by Novell networking standards, but is becoming more common with the deployment of switched networks.

Without routing support for FDDI_RAW IPX encapsulation, packets of this format are recognized only by switches or bridges on the FDDI ring. Neither clients, servers, nor routers directly connected to the ring can recognize this type of packet. By implementing FDDI_RAW encapsulation, it is possible to recognize and route these packets, either to other LAN or WAN media, or back onto FDDI in one of the Novell-approved FDDI formats. Routing support for FDDI_RAW can eliminate the requirement of changing Ethernet encapsulation on servers and clients when deploying switched internetworks.

- IPX Header Compression—IPX header compression permits the compression of IPX packet headers over various WAN media. IPX header compression (CIPX) is described in RFC 1553, *Compressing IPX Headers Over WAN Media*. CIPX is based on Van Jacobson's TCP/IP header compression. CIPX will operate over PPP WAN links using either the IPXCP or IPXWAN communications protocols.

IPX header compression can reduce header information size from 30 bytes to as little as 1 byte. This can save bandwidth and reduce costs associated with IPX routing over WAN links. In addition, the use of CIPX is negotiated automatically on WAN links using the IPXWAN protocol, which reduces the complexity of implementing these circuits.

Wide-Area Networking Features

This section describes the wide-area networking features that are new in the initial release of Cisco IOS Release 11.1.

ISDN/DDR Enhancements

The following feature has been added to Cisco's ISDN and DDR software:

- **Asynchronous ISDN Access (V.120 Support)**—Asynchronous ISDN access allows an ISDN terminal adapter (TA) connected to the serial port of a personal computer to call an ISDN BRI or PRI hub router and be recognized as if it were connected to a Cisco access server.

SMDS

The following features have been added to Cisco's SMDS software:

- **Fast-Switched Transparent Bridging over SMDS**—Transparent bridging over SMDS can be fast switched using IEEE 802.6i encapsulation, allowing for better bridging performance and enhanced bridged media support.

Only IEEE 802.3, IEEE 802.5, and FDDI with or without frame check sequence (FCS) frames will be supported in the fast-switched and process-switched modes. Previously, only IEEE 802.3 frames were process-switched.

- **Fast-Switched IPX over SMDS**—Fast-switching of Novell IPX packets over SMDS provides better performance for IPX over SMDS. This feature is enabled by default. The existing **ipx route-cache** commands work for SMDS interfaces.

ATM Enhancements

The following features have been added to Cisco's Asynchronous Transfer Mode (ATM) software:

- **Classic IP over ATM Enhancements**—The Classic IP over ATM client software has been enhanced to support the configuration of multiple independent ATM ARP servers. When used with other clients that support similar functionality, this feature eliminates the single point of failure associated with having only one server.
- **Bridged Emulated LANs**—Bridging between emulated LANs is now supported.
- **LANE MIBs**—Three new Cisco MIBs are now available for LAN Emulation (LANE):
 - Cisco LANE Broadcast-and-Unknown Server MIB: Used to manage LANE broadcast-and-unknown servers.
 - Cisco LANE Configuration MIB: Used to manage LANE configuration servers in Cisco devices.
 - Cisco LANE Service MIB: Used to manage LANE service in Cisco devices.

Core Enhancements

The following features have been added to the Cisco 7000 series and Cisco 7500 series routers:

- **VIP-1FE, VIP-1FE/1FE, VIP-1FE/4E, VIP-4E/4T, and VIP-4R/4T Support**—The Versatile Interface Processor (VIP) is a new class of interface processor for the Cisco 7000 series and Cisco 7500 series routers. The VIP is a modular, RISC-based, intelligent interface processor that accepts up to two port adapters. Port adapters provide the media-specific interface, while the VIP motherboard provides support for high-performance switching and other value-added features.

The VIP-1FE is based on a single one-port Fast Ethernet port adapter. The VIP-1FE/1FE is based on two one-port Fast Ethernet port adapters. Both the VIP-1FE and VIP-1FE/1FE support IEEE 802.3u Fast Ethernet specifications for half- and full-duplex operation.

The VIP-1FE/4E is based on a one-port Fast Ethernet port adapter that supports distributed IP switching for the FEIP and a four-port (10BaseT) Ethernet port adapter. VIP distributed IP switching can switch to these output interfaces: VIP-FE/4E, VIP-FE, EIP, FIP, and FSIP, HIP, and MIP with HDLC encapsulations. (VIP distributed IP switching is not available in Release 11.1(1). It will be available in a future maintenance release of Cisco IOS Release 11.1.)

Each Fast Ethernet port has an RJ-45 connector (100BaseTX, two-pair category 5 UTP), and an MII connector that provides connectivity to 100BaseFX and 100BaseT4 through customer-provided external transceivers. The Fast Ethernet port adapters can be configured for Inter-Switch Link (ISL), which supports VLANs between Catalyst 5000 high-performance switches and IEEE 802.1000 TB-VLAN for transparently bridging VLANs. (ISL is not supported in Release 11.1(1), but will be supported in Release 11.1(2) for RSP and RSP7000 processors with the FEIP and VIP cards.)

Because of its modular design, the VIP can be configured to support mixed media. Because this version of the VIP supports both Ethernet and Fast Ethernet, customers can now realize much better slot utilization in either the Cisco 7000 series or the Cisco 7500 series.

For full-duplex operation, the VIP-1FE is recommended.

- **VIP Distributed IP Flow Switching**—VIP Distributed IP Switching enables the new VIP to make its own switching decisions. With this release, the VIP can be configured to support distributed IP switching. This feature is not available in Release 11.1(1). It will be available in a future maintenance release of Cisco IOS Release 11.1.

The primary goal of distributed IP switching is to provide scalable switching performance for the Cisco 7500 series of high-end multiprotocol routers. With the introduction of distributed IP switching, Cisco 7500 switching performance scales as more VIPs are introduced into the system. VIP distributed IP switching can switch to these output interfaces: VIP-FE/4E, VIP-FE, EIP, FIP, and FSIP, HIP, and MIP with HDLC encapsulations.

VIP Distributed Switching requires the architecture of the Cisco 7500 series Route Switch Processor (RSP). VIP distributed IP flow switching is not available for VIPs installed in Cisco 7000 series platforms.

- **High System Availability (HSA)**

HSA is an advanced software feature of the Cisco 7500 series architecture. HSA increases the availability and uptime of the Cisco 7507 and Cisco 7513 routers. This increase is accomplished through a master/slave relationship between two RSPs. If the slave RSP detects an error condition it automatically takes control and reboots the system without user intervention. This automatic action minimizes network interruption and increases system availability.

HSA can be used in the following situations:

- *Hardware backup.* Protects against single processor failure.
- *Software error protection.* Protects against critical software errors by keeping different software images on each RSP.
- *Configuration switching.* Enables users to store different configurations in each RSP. If the new feature configuration on the master causes a system failure, the slave RSP takes over the routing function after a system reboot.

This feature became available in Cisco IOS Release 11.1(4).

Note HSA requires a ROM Monitor upgrade. See the “Important Notes” section for more information.

- Standard Serial Interface Processor (SSIP) and Service Provider Multichannel Interface Processor (SMIP)—The SSIP is an 8-port serial card and supports the same physical interfaces and port speeds as the FSIP8.

The SMIP is a 2-port channelized interface processor that supports T1 and E1 interfaces and offers the same port configuration options as the MIP.

In conjunction with the Cisco 1000 series, the SSIP and SMIP provide the capability to cost-effectively network even the smallest branches. For Internet service providers, the SSIP, SMIP, and Cisco 1000 series significantly reduce the cost of adding customers, which allows Internet services to be profitably provided to a larger market.

The SSIP and SMIP do not currently support full Cisco IOS software functionality. Please refer to Product Bulletin 397, which details the Cisco IOS software functionality supported by the SSIP and SMIP.

Although these features are included in Cisco IOS Software Release 11.1, the SSIP and SMIP are already supported in Release 10.3(6), Release 11.0(4), and later.

- Source-Route Bridging (SRB) over FDDI on Cisco 7500 series routers—Supports SRB from Token Ring to Token Ring over FDDI on the Cisco 7500 series. Previously, the only way to transport SNA and NetBIOS over FDDI was with remote source-route bridging (RSRB), which is process switched. With SRB over FDDI, traffic is autonomously switched, greatly improving performance for SRB traffic that uses FDDI as a backbone and eliminating the need for RSRB peer definitions.

Note Cisco routers do not support SRB over FDDI when the router is an end station on an FDDI LAN.

- Flash Management Information Base (MIB) on Cisco 7500 series routers—The Cisco 7500 series supports the new Cisco Flash MIB. This feature enables various SNMP operations on system Flash devices that normally require manual console access to the router.

The Flash MIB enables a user to use network management stations and CiscoWorks to manage and upgrade router software. With MIB support, this feature is now SNMP-manageable.

- Cisco RSP7000—The RSP7000 provides an upgrade in the Cisco 7000 series routers to an integrated Route/Switch Processor (RSP), which was previously only available with Cisco 7500 series routers. RSP combines the switched routing and high-speed switching functions of the separate Route Processor (RP) and Switch Processor (SP), obsoleting the need for two separate processor units.

RSP7000 functionality is similar to a Cisco 7505 with RSP1, except that CyBus is not supported. CIP, FEIP, and VIP (CyBus interface processors) operate in CxBus mode.

Access and Communication Servers

- Media Access Control (MAC) Security for Hublets (Cisco 2505, Cisco 2507, and Cisco 2516)—MAC security for Hublets goes down a layer in the OSI model to provide security detection and protection at the MAC layer. Each repeater port on the hub can be assigned an

acceptable source MAC address. The hublet detects if the source address is different from the legal source address. If there is a violation, the port will be shut down (partitioned) for 1 minute. This capability currently exists.

In Cisco IOS Release 11.1, the network manager can have a trap message sent when the source MAC address violation occurs. The SNMP trap message may be sent once, or at a decaying rate. The decaying rate option provides the first SNMP trap message immediately, the second trap at 2 minutes, the third trap at 4 minutes. This continues until 32 minutes have passed. The decaying trap messages can be terminated by the NMS by using the MIB variable *TrapAcked*.

Additional MIB variables are provided in the agent to allow the NMS to query the violation. MAC security MIB variables provide information such as last illegal source address, timestamp of the first violation, timestamp of the last violation, and number of violation frames.

Because SNMP uses UDP, a single trap notification might get lost. It is possible to configure the router to send multiple traps at a decaying rate. This ensures that the trap message will be received by the NMS.

- LANE on the Cisco 4500—The LANE feature emulates an Ethernet segment over ATM that allows higher-layer protocols and their applications to operate without modification. LANE features service components—LANE configuration server (LECS), LANE server (LES) and broadcast and unknown server (BUS)—as well as a client component called the LANE client (LEC). LANE includes a connectionless broadcast that can support important protocol mechanisms such as ARP. This service is not available in other ATM networks. In LANE, LE_ARP requests resolve MAC addresses to ATM addresses. LECS, LES, BUS, and LEC are supported on the router ATM interfaces.

LANE is also the underlying technology that supports virtual LANs (VLANs) over ATM networks. By providing the needed Layer 3 routing connection between Layer 2 VLANs, a Cisco 4500 or Cisco 4700 router with an NP-1A ATM network processor module and LANE technology provides standards-based routing between VLANs over ATM.

LANE requires Interim Local Management Interface (ILMI) and point-to-multipoint signaling capabilities on the switches on which it operates (VP tunneling is acceptable where signaling is not offered, such as a ATM WAN). The LANE services on the router ATM interfaces interoperate with Cisco LECs, including Cisco's ATM NICs and the Catalyst 5000. Cisco is pursuing interoperability with other third-party ATM LECs.

IBM Functionality Features

This section describes the IBM network software features and support that are new in the initial release of Cisco IOS Release 11.1.

New Features

The following new IBM software features are available:

- Downstream Physical Unit (DSPU) Network Management Events—DSPU has been enhanced to support six new network management events. These events are mapped to SNMP traps and SNA messages and are used to notify network management when:
 - Upstream PU changes state
 - Downstream PU changes state
 - Upstream LU changes state
 - Downstream LU changes state

- DSPU is unable to activate a downstream PU
- DSPU is unable to activate a downstream LU

This feature simplifies network management by providing additional visibility of SNA network resources and by sending notifications about problems with PU and LU connectivity. When a downstream PU changes state, a DSPU is unable to activate a downstream PU, or a DSPU is unable to activate a downstream LU, it is mapped to an SNA message sent to a host operator, which generally appears in a NetView or NetMaster log. To minimize unnecessary noise across the network and in SNMP and NetView or NetMaster logs, there are four configurable notification levels (off, low, medium, and high).

- Advanced Peer-to-Peer Networking (APPN) Enhancements—APPN enhancements include data link layer enhancements and enhanced logging and debugging functions.

Data link layer enhancements include:

- APPN over Asynchronous Transport Mode (ATM) using RFC 1483.
- APPN over the Point-to-Point Protocol (PPP) using RFC 1661.
APPN over PPP also allows APPN to be transported over an Integrated Switched Digital Network (ISDN).
- APPN over Switched Multimegabit Digital Services (SMDS) using a Cisco-proprietary encapsulation.

Enhanced logging and debugging functions enable debug output that is more meaningful and useful, including better documentation of the error and debug output, more user control of the type and amount of debug output generated, and more descriptive information in the messages.

Because there is no standard way for transporting APPN over SMDS, a Cisco-proprietary method is used.

Note In some cases, APPN over SMDS may not interoperate with other vendors' SMDS implementations, because a proprietary method is being implemented.

- Frame Relay Access Server (FRAS) Boundary Access Node (BAN) Support—BAN provides a way of connecting remote SNA offices over Frame Relay directly into a front-end processor. Unlike the FRAS boundary network node (BNN) feature supported in Cisco IOS Release 10.3, BAN includes the MAC address in every frame, eliminating the need to do SAP multiplexing if there are multiple SNA physical units (PUs) sharing a single PVC. BAN uses the RFC 1490 bridged-frame format.

BAN simplifies configuration in an environment where multiple remote SNA devices need to share a single PVC, and where there are no central site routers for SNA. It offers load balancing and provides the flexibility to build a redundant path to the Network Control Programs (NCPs).

Note BAN only applies to SNA devices on Ethernet or Token Ring. It does not apply to SDLC-attached devices. BAN requires NCP 7.3 at the central site. BNN and BAN can share the same DLCI to the NCP.

Data Link Switching+ (DLSw+) Features and Enhancements

The following features have been added to Cisco's DLSw+ software:

- **DLSw+ LNM Support**—DLSw+ has been enhanced to support IBM's LAN Network Manager (LNM), enabling LNM to communicate to a remote DLSw+ router, and manage or monitor any Token Ring connected to a Cisco router.

LNM support includes configuration report services, ring error monitor, and the ring parameter server. In addition, the DLSw+ router notifies LNM of certain events that might occur on a Token Ring, such as notification of a new station joining the Token Ring, or that the ring has entered failure mode known as beaconing.

This feature will be available in a future Cisco IOS 11.1 software maintenance release.

- **DLSw+ Support on Cisco 7500**—Support for DLSw+ Fast-Sequenced Transport (FST) and Direct on the Cisco 7500 series routers is added, increasing network design flexibility of Cisco 7500 series routers.
- **DLSw+ Management Information Base (MIB)**—DLSw+ now offers a MIB for faster problem determination. In addition, the DLSw+ MIB is the basis for DLSw+ Logical Maps.
- **DLSw+ Multidrop PU 2.0/2.1 Support**—Multidrop PU 2.0 and PU 2.1 support enables multiple PU 2.1 devices to share the same SDLC line. In addition, PU 2.0 and PU 2.1 devices can also now share the same SDLC line.
- **80D5 (Ethernet version 2) Support**—80D5 (Ethernet version 2) is now supported by DLSw+. This support extends DLSw+ to environments that have not converted to IEEE 802.3.
- **Local DLC Conversion over DLSw+**—DLSw+ now supports local conversion between SDLC or QLLC and LLC2. With local conversion, only one DLSw+ router is required for conversion of a link-level protocol. Previously, a remote peer was required to perform this conversion.
- **DLSw+ Backup Peer Enhancements**—DLSw+ allows you to specify a backup peer to use in the event that a primary peer fails. Previously, when the primary peer recovered, the backup peer connection terminated along with any sessions using that peer. The backup peer feature has been enhanced to allow the backup peer to remain active after the primary recovers, to prevent disrupting SNA and NetBIOS sessions a second time. Once the primary peer is active, all new sessions are established using the primary peer. The backup peer connection remains active until there are no active LLC2 connections on it or after a user-configurable idle time.
- **DLSw+ Enhancements for ISDN/Switched Environments**—DLSw+ has been enhanced to allow more effective use of ISDN/switched lines:
 - ISDN links are allowed to terminate during idle periods, but still maintain SNA sessions.
 - The router can be configured to activate a peer dynamically under certain conditions (for example, when there is an SNA test frame or a NetBIOS Name Query for a preconfigured device). When there is no traffic on that peer, the peer connection is disabled.

These enhancements minimize WAN costs in switched environments. In addition, peer connections are only established when needed, maximizing scalability and minimizing cost.

Access and Communication Server Features

This section describes the access and communication server features that are new in the initial release of Cisco IOS Release 11.1.

- NetBEUI over Point-to-Point Protocol (PPP)—Microsoft has published a draft RFC that defines a protocol for passing NetBEUI over PPP. Application of this RFC allows remote PCs with remote access client software to dial into network access servers connecting into NetBEUI networks. The protocol used in these connections is a PPP Network Control Protocol (NCP) called NetBIOS Frames Control Protocol (NBFCP).

NBFCP:

- Supports both asynchronous and ISDN interfaces.
- Is compatible with Microsoft's remote access client with NBFCP.
- Supports NetBIOS name caching.
- Supports NetBIOS name filtering.

With NBFCP:

- PCs with NetBIOS applications and NBFCP-capable remote access clients can dial into Cisco access servers for access into NetBEUI networks.
- Microsoft's remote access clients with NBFCP can dial into Cisco access servers for access into NetBEUI networks.
- Modem Auto-Configuring—Modem auto-configuring allows Cisco access servers to discover and identify an attached modem and configure it with the appropriate modem command strings. Identification and configuration are performed for each line reset. Modem strings are kept in an internal database that administrators can add to.

With modem auto-configuring, no direct configuration of modems is required. All modems with a modem database entry are automatically recognized, and modems not found in the modem database can be defined clearly and quickly as the access server prompts for specific modem command strings.

- Novell Asynchronous Services Interface (NASI) Support—Novell Connection Services (NCS) server uses NASI to provide outgoing serial line access for PCs with NASI client drivers. This function is generally used to provide dial-out modem services to PCs on SPX/IPX networks. Cisco access servers can now function as NCS servers providing dialout over IPX for PCs. This allows Cisco access servers to:
 - Advertise their Novell Connection Services via SAPs.
 - Support NASI out-of-band, encrypted username and password authentication.
 - Support Cisco SAP filters and management controls.

Using the NCS server network, network managers can offer IPX dial-in and dial-out services on the same Cisco access server.

Note Because of Novell split-horizon rules it is necessary to disable all other NCS servers on the same network where the Cisco access server is deployed for NASI outbound connections.

- Identification Protocol Support—Identification Protocol (also called "ident" or "the Ident Protocol"), specified in RFC 1413, is a protocol for reporting the identity of a TCP connection initiator to the connection-receiving host.

This feature allows the identification of a username associated with a TCP connection.

The Identification Protocol support is not useful for securing access servers. It is a protocol for identifying the other end of a TCP connection. It does not authenticate or authorize the connection.

- **Kerberos Authentication**—Kerberos is an authentication protocol developed by the Massachusetts Institute of Technology (MIT). Its primary use is to authenticate users and the network services they use. This is accomplished by the issuance of “tickets” to both services and users by a “trusted” Kerberos server. These tickets have a limited life span and can be used in place of the standard user/password authentication mechanism if a service trusts the Kerberos server from which the ticket was issued. Cisco’s implementation of Kerberos is based on code developed by CyberSafe, which was derived from the MIT code.

Cisco is implementing a two-phased approach to the implementation of Kerberos. Phase 1, delivered in Cisco IOS Release 11.1, permits authentication on the router using Kerberos. (Phase 2, which will be available in another major Cisco IOS software release, will allow a user to carry credentials to other services, such as Telnet, without having to reauthenticate.)

A Cisco white paper explaining Kerberos in more detail can be found on the World Wide Web (you need to be a registered CCO user) at:

<http://www.cisco.com/warp/public/789/1.html>

- **Remote Authentication Dial-In User Service (RADIUS)**—RADIUS is an access server authentication, authorization, and accounting protocol developed by Livingston, Inc. It is a distributed security system that protects remote access to networks and network services against unauthorized access. RADIUS has three components: a protocol with a frame format that utilizes UDP/IP, a server, and a client.

The server resides on a central computer typically at the user’s site. The clients reside in the dial-up access servers and can be distributed throughout the network. The RADIUS client is available in Cisco IOS Release 11.1.

Cisco’s implementation of RADIUS is currently defined in draft documents at <ftp.livingston.com:pub/radius/draft-ietf-radius-radius-02.txt>. Cisco’s implementation is based on this version of the draft. Cisco will attempt to keep current with any newer drafts issued. A sample RADIUS server can be obtained from Livingston’s FTP site.

RADIUS is configured on the network access server much like TACACS+.

Network Management Features

This section describes the network management feature that is new in the initial release of Cisco IOS Release 11.1.

- **Remote Monitoring (RMON) Support**—The RMON MIB (RFC 1757) is added as an option to several Cisco IOS software feature sets for use on Cisco 2500 series routers. Full, 9-group Ethernet support is available and includes:
 - **statistics:** Tracks segment usage, errors, and frame-size distribution information.
 - **history:** Logs historical snapshots of RMON statistics at user-defined time intervals.
 - **alarms:** Detects changes in network behavior based on increasing and decreasing thresholds of performance and error statistics.
 - **hosts:** Provides basic traffic statistics, such as packets and octets in and out, broadcast, and total error counts for each network node or device based on MAC addresses.

- **hostTopN**: Keeps a sorted list of top “talkers” by node-level statistics.
- **matrix**: Tracks basic traffic information between physical source and destination pairs.
- **filter**: Allows focused analysis by selectively reducing the number of packets to be captured remotely based on address, protocol, and user-defined data patterns.
- **capture**: Acquires and buffers complete or partial packets for protocol decoding and detailed analysis with a console application.
- **event**: Logs alarms and generates SNMP traps as a result of thresholds being crossed or capture buffers being filled.

Note As a security precaution, the packet capture group captures only useful packet header information; data payloads are not captured.

All Cisco IOS software images that do not explicitly include full RMON support include RMON alarm and events groups. These groups can be coupled with existing Cisco MIB variables and allow customers to set thresholds and alarms on any MIB variables supported by Cisco.

RMON not only provides visibility of individual nodal activity, it allows the monitoring of all nodes and their interaction on a LAN segment. RMON used specifically as an agent in the router allows network managers to view either only traffic that flows through the router or all Ethernet segment traffic not necessarily destined for the router.

An RMON console application such as Cisco Traffic Director or NETscout Manager™ by Frontier Software Development, Inc., is required to take full advantage of the embedded RMON’s network management capabilities.

Security Features

This section describes the security feature that is new in the initial release of Cisco IOS Release 11.1.

- **Lock-and-Key Access**—Lock-and-Key access allows you to set up dynamic IP access lists that grant access per user to a specific source or destination host through a user authentication process.

Before Lock-and-Key access, IP access lists were created and maintained by manually defining lists on a router and distributing them to all other routers in the network. In networks with many hosts, this task could consume time and resources. Access lists do not provide any challenge mechanism beyond a static network address, making it possible for an unauthorized user to access network resources through any authorized network address. The Lock-and-Key access feature is an ideal solution for the proliferation of remote networks. Lock-and-Key access supports various WAN technologies such as ISDN, Frame Relay, X.25, dial-on-demand routing (DDR), and Point-to-Point Protocol (PPP).

When a user Telnets to a router configured with Lock-and-Key access, the software challenges the user to respond to a login and password prompt before placing a temporary entry in the dynamic access list. The network administrator can dictate an idle time-out or an absolute period for authorization and reauthorization.

Lock-and-Key access provides the following benefits:

- Allows per-user authorization and authentication in a shared-media environment.
- Authenticates a user beyond an IP network address.

- Maintains authentication information at a central network access server such as TACACS, XTACACS, TACACS+, and RADIUS.
- Provides application independence—Lock-and-Key access does not require modification to user applications.
- Supports one-time password token cards.
- Provides a flexible policy mechanism to require remote reauthorization during periods of inactivity.
- Understands the concept of organizational templates, which allow the network administrator to create an access list for a group of users with similar access requirements, but provides unique authentication challenges to each user.



Caution Lock-and-Key access allows an external event to place an opening in the firewall. Once this opening is placed, the router is susceptible to source-address spoofing. To prevent this, you need to provide encryption support using IP authentication or encryption.

Lock-and-Key access requires Telnet. Standard Telnet is the required application on the host platform that activates a Lock-and-Key session.

Further information on Lock-and-Key access can be found on the World Wide Web in the *Cisco IOS Lock and Key* white paper (Product Bulletin 308) at <http://www.cisco.com/warp/customer/417/66.html>. (You need to be a registered CCO user.)

Important Notes

This section describes warnings and cautions about using the Cisco IOS Release 11.1 software. This section discusses these topics:

- BSC and SDLC Commands in Release 11.1(2)
- Upgrading to a New Software Release
- Channel Interface Processor (CIP) Microcode
- Cisco 7500 Series High System Availability (HSA)
- VLAN Routing
- Netbooting from VIP
- Source-Route Bridging (SRB) over FDDI
- Enabling IPX Routing
- Using AIP Cards
- Booting Cisco 4000 Routers
- Using LAN Emulation (LANE)
- Forwarding of Locally Sourced AppleTalk Packets
- Using Source-Route Transparent Bridging (SRT) and Source-Route Bridging (SRB) on Cisco 2500 and Cisco 4000 Routers
- Release 11.1(5a)
- Release 11.1(11a)

- ATM Multipoint Signaling
- Release 11.1(13a)

BSC and SDLC Commands in Release 11.1(2)

In Release 11.1(2), the **bsc fdx** and **sdlc hdx** commands were deprecated and replaced by the **full-duplex** and **half-duplex** commands, respectively. The deprecated commands continue to be supported in Release 11.1(2) and later, but might not be supported in the next major release of Cisco IOS software.

Upgrading to a New Software Release

If you are upgrading to Cisco IOS Release 11.1 from an earlier Cisco IOS software release, you should save your current configuration file before installing Release 11.1 software on your router.

Channel Interface Processor (CIP) Microcode

Starting with Cisco IOS Release 11.1, CIP microcode is available as a separate image, unbundled from the Cisco IOS image. CIP microcode (for the CIP or second-generation (CIP2)) resides only in router Flash memory as multiple files. The router loads a “kernel” to the CIP (based on hardware revision), and the CIP selectively loads and relocates the software it requires from the router’s Flash memory. The CIP image is available on pre-loaded Flash memory cards, on floppy diskette, or via FTP from Cisco. Every version of Cisco IOS Release 11.1 has a corresponding version of CIP microcode. Refer to the *Channel Interface Processor (CIP) Microcode Release Note and Microcode Upgrade Requirements* publication (Document Number 78-4715-xx) for information about the recommended pairs of Cisco IOS Release 11.1 and CIP microcode.

The CIP loader has the following effect on the router’s system memory requirements:

- DRAM utilization decreases by 0.5 MB to 1 MB
- Bundled image sizes decrease by 0.5 MB to 1 MB
- Flash memory utilization increases by 1 MB to 1.5 MB

Consider the following before you use the CIP loader:

- If you have a router with Release 11.1 and a Release 11.1 CIP image on a Flash memory card, no action is required. The CIP microcode will load automatically upon booting the router.
- If you have an existing router with Release 11.1 in Flash memory or ROM and a pre-11.1 Flash memory card, either:
 - Replace the Flash memory card with a Release 11.1 pre-loaded Flash memory card, or
 - Boot the router with Release 11.1 software (CIP load will fail), then copy the Release 11.1 CIP image to the Flash memory card, and reboot the router.

When the CIP image is copied to an existing Flash memory card, the existing **flash copy** commands are used, just as before. If a CIP image other than the default for the release is being used, then the **microcode cip flash** configuration command must be issued.

The **show microcode** command has been expanded to display the default CIP image name for the Cisco IOS release.

Note The router must already be running Cisco IOS Release 11.1 before performing a copy of the CIP image to Flash memory, because the CIP image must be “exploded” from the single image file on the TFTP server to multiple files in Flash memory. This capability is added in Release 11.1.

There are a number of ways to determine what is loaded on each CIP:

- The CIP MIB has been enhanced to show the segments loaded on each CIP and their version and compilation information.
- The **show controller cbus** command has been expanded to include segments loaded and their version and compilation information.

Multiple CIP cards of different hardware revisions can run in the same router.

Cisco 7500 Series High System Availability (HSA)

To successfully use the HSA feature, you should take note of the following:

- The HSA feature available on the Cisco 7500 series routers requires a ROM monitor upgrade to ROM monitor version 11.1(2), or later.
- For spare RSP2 cards to function with HSA, they must also be upgraded. Spare Flash cards require Release 11.1(4) or higher boot or system images.
- HSA installation requires the both RSP2s have the same amount of DRAM (24 MB minimum each RSP2).
- To use the HSA feature, you must use a Cisco IOS feature set image that contains a “v,” such as the RSP subset image `rsp-jv-mz.111-4`.
- You should also note the following HSA-related caveats:
 - The BOOTDLR variable of the slave RSP is incorrectly set to NVRAM by default. This could cause a netbooting of the slave to fail if the master RSP were to crash. [CSCdi48170]
 - On-line insertion and removal (OIR) of an HSA slave RSP (removing an HSA slave RSP with the router online) causes the router to reload. [CSCdi57076]
 - The HSA feature does not work if a Versatile Interface Processor (VIP) or second-generation VIP (VIP2) is installed in the router. If you install a VIP or VIP2 in an HSA-configured system, or if you install a second RSP2 into a system containing a VIP or VIP2, the system will crash with the following error message:

```
%RSP-3-INVRSP_IPC: Slave RSP slot x not supported with VIP slot y, crashing router
```

```
[CSCdi60891]
```

VLAN Routing

Support for VLAN routing is not available in Release 11.1(1). Support for this feature is available in Release 11.1(2). VLAN routing allows Inter-Switch Link (ISL)-encapsulated IP, IPX, and transparently bridged traffic to be routed or bridged to any other VLAN or native interface.

Netbooting from VIP

To netboot from Ethernet or Fast Ethernet ports on a VIP card the system must contain version 11.1 boot ROMs. If the system contains version 11.0 boot ROMs, you can work around this requirement by using the **boot bootldr** *device: filename* global configuration command to load a bootstrap image from Flash memory.

Source-Route Bridging (SRB) over FDDI

This feature supports forwarding of source-route bridged traffic between Token Ring and FDDI interfaces on the Cisco 7000, Cisco 7010, and Cisco 7500 series routers. Previously, the only way to transport SNA and NetBIOS over FDDI was with remote source-route bridging (RSRB), which is either fast switched (direct or Fast-Sequence Transport (FST) encapsulation) or process-switched (TCP encapsulation). With SRB over FDDI, traffic can be autonomously switched, greatly improving performance for SRB traffic that uses FDDI as a backbone. This feature eliminates the need for RSRB peer definitions to connect Token Ring networks over the FDDI backbone.

Note SRB over FDDI does not support RSRB traffic forwarded to RSRB peers. Routers that have connections to local Token Ring networks as well as RSRB connections to remote networks cannot use this feature. The work around is to move the RSRB connections to routers that are not connected to the FDDI backbone.

Enabling IPX Routing

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

Using AIP Cards

Cisco 7000 series ATM Interface Processor (AIP) cards that support E3, DS3, or Transport Asynchronous Transmitter/Receiver Interface (TAXI) connections and that were shipped after February 22, 1995, require Cisco IOS Release 10.0(9), 10.2(5), 10.3(1), or later.

Booting Cisco 4000 Routers

You must use the Release 9.14 rxboot image for Cisco 4000 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 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 boot either 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 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
```

Using LAN Emulation (LANE)

Note the following information regarding the LAN Emulation (LANE) feature:

- LANE is available for use with Cisco 4500, 4700, 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, and AppleTalk is supported.
- LANE does not support
 - DECnet, CLNS, VINES, and XNS
 - LANE over PVCs
 - HSRP
- AppleTalk Phase 1 cannot be routed to AppleTalk Phase 2 via LANE.

Forwarding of Locally Sourced AppleTalk Packets

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

Using Source-Route Transparent Bridging (SRT) and Source-Route Bridging (SRB) on Cisco 2500 and Cisco 4000 Routers

Certain products containing the Texas Instruments TMS380C26 Token Ring controller do not support SRT. SRT is the concurrent operation of 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. In one, Token Ring networks are configured to SRB protocols such as SNA and NetBIOS, and they transparently bridge other protocols, such as IPX. In the other situation, 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).

As of Release 10.3(1), SRB in the following Cisco IOS features sets is no longer supported: IP, IP/IPX, and 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, or 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.

Release 11.1(5a)

After the release of Cisco IOS Release 11.1(5), a caveat was discovered within the Cisco IOS rsp-images. It was determined that this caveat was significant enough to merit a rebuild of the rsp-images. The rebuild includes the caveat fix and is renumbered to 11.1(5a).

This defect is bug CSCdi66673 and is described as follows:

When Ethernet runt packets are received by Cisco 7500 series router processors (RSP1, RSP2, or RSP7000), a Reserved Exception crash or a QAERROR error will occur. When either of these problems happens, a switching complex restart is forced. The Reserved Exception crash has the following output:

```
Queued messages:
Aug 14 10:44:16: %RSP-3-ERROR: memd write exception, addr 08000000
Aug 14 10:44:16: %RSP-3-ERROR:   RSP alignment error on write to QA, addr 080000
00
*** System received a reserved exception ***
signal= 0x9, code= 0x0, context= 0x60c72fd0
PC = 0x60107514, Cause = 0x2020, Status Reg = 0x34008702
DCL Masked Interrupt Register = 0x000000ff
DCL Interrupt Value Register = 0x00000000
MEMD Int 6 Status Register = 0x00000000
```

The QAERROR error has the following output:

```
Jun 17 10:50:23.329: %RSP-2-QAERROR: reused or zero link error, write at addr 03
08 (QA)
log 260308C0, data A816FFFF 00000000
```

Release 11.1(5a) and all subsequent releases of Cisco IOS software, including Release 11.1(6), include the fix for this caveat.

Release 11.1(11a)

After the release of Cisco IOS Release 11.1(11), caveats were discovered within the Cisco IOS rsp-images. It was determined that these caveats were significant enough to merit a rebuild of the rsp-images. The rebuild includes the caveat fixes and is renumbered to 11.1(11a).

The defects are bugs CSCdi67315, CSCdj08722 and CSCdj09576 and are described as follows:

- Under high traffic conditions excessive packet drops may be noticed. [CSCdi67315]
- A problem may occur when the VIP2 FIFO buffers overflow, resulting in a silent failure of data written to SRAM. This may cause a number of protocol-related failures including TCP checksum errors and other packet data errors. This problem is not limited to any particular network configuration, traffic load or other specific circumstances. [CSCdj08722]
- A problem may occur when the FDDI port adapter experiences a receive ring overrun under heavy traffic load with packet sizes larger than 512 bytes. This may cause a number of protocol-related failures including TCP checksum errors and other packet data errors. [CSCdj09576]

Release 11.1(11a) and all subsequent releases of Cisco IOS software, including Release 11.1(12), include the fix for these caveats.

ATM Multipoint Signaling

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

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

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

Users will have to enable the **atm multipoint-signaling** command on all subinterfaces that require it. Previously, they only needed to enable it on the main interface.

Release 11.1(13a)

After the release of Cisco IOS Release 11.1(13), caveats were discovered within the Cisco IOS software. It was determined that these caveats were significant enough to merit a software rebuild. The rebuild includes the caveat fixes and is renumbered to 11.1(13a).

The defect is bug CSCdi73194. Related bugs are CSCdj25806, CSCdj25905, CSCdj26494, CSCdj26898, CSCdj28362, CSCdj30980, and CSCdj32710. CSCdi73194 is described as follows:

- High utilization on the router can sometimes be caused by the IP Background process. This can be noticed by issuing the **show processes cpu** command. The router usually reaches about 80 to 85 percent utilization but does not crash.

Release 11.1(13a) and all subsequent releases of Cisco IOS software, including Release 11.1(14), include the fix for these caveats.

Caveats for Release 11.1(1) through 11.1(24a)

Cisco IOS Release 11.1(24a) is a rebuild release for Cisco IOS Release 11.1(1). The caveats in this section are resolved in Cisco IOS Release 11.1(24a) but may be open in previous Cisco IOS releases.

- Cisco IOS software releases based on versions 11.x and 12.0 contain a defect that allows a limited number of SNMP objects to be viewed and modified without authorization using a undocumented ILMI community string. Some of the modifiable objects are confined to the MIB-II system group, such as “sysContact”, “sysLocation”, and “sysName”, that do not affect the device's normal operation but that may cause confusion if modified unexpectedly. The remaining objects are contained in the LAN-EMULATION-CLIENT and PNNI MIBs, and modification of those objects may affect ATM configuration. An affected device might be vulnerable to a denial-of-service attack if it is not protected against unauthorized use of the ILMI community string.

The vulnerability is only present in certain combinations of IOS releases on Cisco routers and switches. ILMI is a necessary component for ATM, and the vulnerability is present in every IOS release that contains the supporting software for ATM and ILMI without regard to the actual presence of an ATM interface or the physical ability of the device to support an ATM connection.

To remove this vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is documented in DDTS record CSCdp11863.

In lieu of a software upgrade, a workaround can be applied to certain IOS releases by disabling the ILMI community or “*ilmi” view and applying an access list to prevent unauthorized access to SNMP. Any affected system, regardless of software release, may be protected by filtering SNMP traffic at a network perimeter or on individual devices.

This notice will be posted at
<http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shtml>. [CSCdp11863]

- Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at
<http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml>. [CSCds04747]

Caveats for Release 11.1(1) through 11.1(24)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(24). These caveats also apply to Releases 11.1(1) through 11.1(23) (unless otherwise noted).

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

Basic System Services

- On a Cisco 7000 series router, if you replace one interface processor (for example, a TRIP or an FSIP) with a different type of interface processor online, the **show ip interface brief** and **show interface** commands display information for both the old and new controllers. Rarely, this also results in the continual reinitialization of the newly inserted controller.

The only known workaround is to unconfigure the old interface processor before replacing it with the new one. Sometimes, it might even be necessary to issue a **write erase** command, reboot the router, and then redefine the existing interfaces to completely remove all configuration traces of the old interface processor. Once the information that is displayed by the **show** commands is self-consistent, the newly inserted interface processor behaves normally. [CSCdi49800]

- If you see the message “%RSP-3-RESTART: interface Serial x/y, output stuck” on an RSP-based platform, you might have problems with the output interfaces. This problem can occur when bursty traffic is optimum-switched to an output interface on which either the **fair queue** or **transmit-buffers backing-store** command is enabled. A possible workaround is to disable optimum switching. [CSCdi56782]

- When a Cisco 7206 router reboots, the **show version** command output indicates a restart by power on. Output from the **show stack** command indicates spurious interrupts. [CSCdj30733]
- If you try to customize the username prompt by issuing the command **aaa authentication username-prompt ""** to make it either null or blank (" " or " "), the command is accepted, but the command does not work and does not appear in the display of the **show running-config** command. [CSCdk22051]
- A memory leak may occur if **view block** is used as part of an **snmp-server** command. [CSCdk40202]
- Route/switch processor (RSP) resets are occurring and disrupting the network. [CSCdk73457]

DECnet

- A VIP may report SRAM parity errors when accessing locations beyond the allowed 2 MB MEMD range. [CSCdk62414]

EXEC and Configuration Parser

- The router may restart with the following error:

System was restarted by bus error at PC 0x3122B6A, address 0xD0D0D3D

Stack trace may look similar to this:

```
Enter hex value: 0x312227A
0x312227A: _connect_new_session(0x30391f0+0xe9008)+0x82
Enter hex value: 0x31223EA
0x31223EA: _connect_command(0x30391f0+0xe90be)+0x13c
Enter hex value: 0x314C6D8
0x314C6D8: _parse_cmd(0x30391f0+0x113044)+0x4a4
Enter hex value: 0x3164850
0x3164850: _exec(0x30391f0+0x12b1e4)+0x47c
Enter hex value: 0x3144D38
0x3144D38: _process_hari_kari(0x30391f0+0x10bb48)+0x0
```

[CSCdj92253]

Interfaces and Bridging

- Token Ring interfaces are put into the reset state after the interface reports ring beaconing, and the interface is not brought back into the ring. This problem occurs because when the interface changes state, it causes IGRP (or other routing protocol) to recompute the route and cause other problems. Error messages on the console indicate that the Token Ring interface is in the reset state. To bring the interface back online, the user should issue the **clear interface** or **no shut** command. [CSCdi48080]
- The FDDI port adapter now has a software address filter at VIP level to filter out unwanted multicast packets. This helps performance and also prevents unnecessary entries in the netflow tables. [CSCdj43445]
- A Cisco 4000 series router with traffic incoming on its FDDI interface may incorrectly count the CEF or fast-switched packets as being process switched. This may cause the input queue to artificially seem backed up. Packets directed to the router (or destined to be process switched) may be incorrectly dropped as a result of these bogus counters. The workaround is to disable CEF/fast switching on the output interface. [CSCdk32659]

- A Cisco 7200 series router with PA-2CE1/PRI-75 port adapters with two E1s configured may display the errors “%MPA68360-1-STARTFAIL:” and “%MPA68360-1-STOPFAIL:”. The controllers fail; the only way to bring the controllers up is to reload the router. Issuing the **show controller** command displays a large number of path code violations, slipped seconds, and framing losses. A workaround is to place a single E1 on each port adapter. [CSCdk44225]

IP Routing Protocols

- The Enhanced IGRP bandwidth parameters are not functioning correctly, and these false metrics are forcing remote sites to select one path rather than load balancing over two paths. [CSCdj70556]
- AS-path access lists have a line length limitation which is exceeded when you use automatic generation. The usual workaround of splitting the access list across lines will not work because you are using automatic generation. [CSCdk01910]

ISO CLNS

- Fast-switching of CLNS traffic with non-zero N-Selector does not work on platforms not using the old MCI controller [CSCdk36270]

Miscellaneous

- When running Cisco 2523 and 2524 serial ports in asynchronous mode, modem control is only supported when using DTE style 5-in-1 cables (in order to connect to DCE devices). The DCE 5-in-1 cable (to connect to DTE devices) will not support modem control for the asynchronous mode. To support DTE devices with modem control, you must use the DTE style cables with a null modem adapter. [CSCdi72371]
- Configuring a bridge group on a port-channel subinterface (fast etherchannel) with ISL encapsulation will prevent routing IP on any of the subinterfaces in that port-channel interface. This was observed in IOS Release 11.1(15)CA. The workaround is to remove the bridge group from the subinterface. [CSCdj69528]

Wide-Area Networking

- In RSP systems that have a 4R interface on the VIP, fast switching does not work, and the RSP has errors. However, process switching still works. The workaround is to upgrade to Cisco IOS Release 11.1(5). [CSCdi51744]
- Packet corruption in the AIP causes packet errors and loss. In some non-reproducible and rare circumstances, an AIP on a Cisco 7000 router reports excessive input errors (like 1%) and displays the following message when the **debug atm error** command is issued:

```
atm_parse_packet(ATM4/0):Invalid VC(0) received, type=AAAA
```

Use the **microcode reload** command as a workaround to return the AIP to a normal state. [CSCdi77244]
- The version 3 PLIM on the Cisco 4500 router causes CRC errors. A high number of CRC errors have resulted between the Cisco 4500 router and LightStream 1010 ATM switch. [CSCdj02665]
- A router can sometimes crash showing a message like this:

```
LIF_Fatal called from CCPRI 0x600B578C, func =3D CCPRI_Mail, string Couldn't send
a package to the HOST: 6
ExecExit called from 0x6008BC0C
%SYS-6-STACKLOW: Stack for process ISDN running low, 0/6000(GDB)
```

Stack contains : process_run_degraded_or_crash

The problem seems to be caused by overburdened ISDN lines. There is currently no workaround available. [CSCdj73619]

- When a dial-in customer uses authentication, this error message appears on the router:

```
%SCHED-3-PAGEZERO: Low memory modified by Net Background (0x40 = 0x4AFC4AFB).
-Traceback= 3128CD6 30D957C.
```

The workaround is to use the terminal window. [CSCdk25156]

Caveats for Release 11.1(1) through 11.1(23)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(23). Since Release 11.1 changed from a seven-week to a fourteen-week maintenance schedule after Release 11.1(18), Release 11.1(23) was only released as an interim version. These caveats also apply to Releases 11.1(1) through 11.1(22) (unless otherwise noted).

For more caveats of Release 11.1(23) and earlier 11.1 releases, see the preceding section, “Caveats for Release 11.1(1) through 11.1(24).”

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(24).

Basic System Services

- Route/switch processor (RSP) range registers set correctly to enforce 2MB limit on MEMD access. [CSCdk64322]

IBM Connectivity

- APPN DLUR make depend fails due to compiler retirement. All APPN images are affected. As a fix, you can try updating your compiler. [CSCdk69202]

Interfaces and Bridging

- Ethernet interface processor (EIP) interfaces on a Cisco 7500 series router running IOS Release 11.2(13) changes between up and down state. A typical **shut** command, then **no shut** command does not bring them back. You must either reload the system, or a microcode reload to stabilize the system to normalize the status. [CSCdk36767]
- The Token Ring interface changes between up and down state when transparent bridging is configured. There is no workaround. [CSCdk60152]

Miscellaneous

- Redundant ARP servers do not implement a backoff mechanism. When the link between the redundant ATM ARP-servers breaks, they continue to try and contact each other in an effort to repopulate the ARP cache. Due to excessive signalling the CPU load on the routers and ATM switches rapidly overloads. The workaround is to use only one ARP server or put them on very stable links [CSCdk40947]
- Several map-list protocol statements cause memory leak. This problem only exists if ALL the following conditions are TRUE:
 - 1. Multiple static maps are configured in a map list.
 - 2. The static maps have broadcast enabled.
 - 3. The static maps have map-class attached.
 - 4. SVCs can not be established due to network or remote problems.

Since PVC is always active in Cisco IOS Release 11.1, it should not have this problem. OSPF hello will always be sent down the PVC without being rejected. Once the memory leak has started it can be stopped by unconfiguring the IP OS network broadcast on the interface or making the interface become passive. [CSCdk62702]

Wide-Area Networking

- A signalling interoperability problem occurs between a Cisco 7500 series router and Bay Centillian switch, resulting in the LEC on the router going down every 15 minutes. The switch sends a "statusEnq" message for the control virtual circuits (VCs) on the router with endpointRef 0. Cisco IOS Release 11.1 or 11.2 software does not handle this properly and fails to respond to **statusEnq** in time, prompting the switch to release the control VCs, resulting in the LEC going down on the router. [CSCdk54181]

Caveats for Release 11.1(1) through 11.1(22)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(22). These caveats also apply to Releases 11.1(1) through 11.1(22) (unless otherwise noted).

For more caveats of Release 11.1(22) and earlier 11.1 releases, see the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections "Cisco Connection Online" and "Documentation CD-ROM" at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(23).

Basic System Services

- When the router is running low on memory and a 'write memory' or configuration is attempted, there is a chance the NVRAM becomes corrupted and the router crashes. This problem can be avoided by first checking that there is enough memory to write the configuration. [CSCdk32125]
- From the login prompt, it is possible to recover fragments of lines typed by the previous user of the same physical or virtual terminal line. This may represent a security exposure. A complete description can be found at the following location:
<http://www.cisco.com/warp/public/770/ioshist-pub.shtml>. [CSCdk43920]

Interfaces and Bridging

- A bus error occurs with bridging enabled on the ATM interface. When bridging is removed from the ATM interface the router stays up. It also causes the router at the other end of the PVC to reload with a software-forced crash. Bridging on the ATM interface using 11.1(14)CA works. [CSCdk18176]

IP Routing Protocols

- There is inconsistent OSPF metric behavior in Cisco IOS Release 11.1. OSPF will not install intra area routes with a total metric greater than 65535. One exception is that an intra area route to a stub network with metric greater than 65535 will be installed the first time the route is calculated. Issuing the **clear ip route** command removes this route. This bug fix ensures that stub routes with metrics greater than 65535 are never installed. Note that the intra area path metric limit has been increased to 16777214 in Cisco IOS Release 11.2 (CSCdi45519). [CSCdk29964]

Miscellaneous

- DNS queries are sent to ports lower than 1024 on devices running Cisco IOS Release 11.1(18) or earlier. It then becomes a problem for returning UDP packets to define access lists. [CSCdk07961]

Wide-Area Networking

- When 'mroute-cache' is configured, multicast packets cannot tunnel through to a router being routed via LANE. This is due to the AIP failing to pad LANE packets. [CSCdj82421]

Caveats for Release 11.1(1) through 11.1(21)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(21). Since Release 11.1 changed from a seven-week to a fourteen-week maintenance schedule after Release 11.1(18), Release 11.1(21) was only released as an interim version. These caveats also apply to Releases 11.1(1) through 11.1(20) (unless otherwise noted).

For more caveats of Release 11.1(21) and earlier 11.1 releases, see the preceding section, "Caveats for Release 11.1(1) through 11.1(22)."

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections "Cisco Connection Online" and "Documentation CD-ROM" at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(22).

IBM Connectivity

- A router may reload if the Token Ring interface has SRB configured. This can happen if a router with SRB configured receives a frame for LNM with a RIF length greater than 7 hops. A workaround is to issue the command **no lnm rem**. All platforms are affected. [CSCdk30604]

Interfaces and Bridging

- A router will become very busy and seem to fail because the Token Ring does not filter forwarded DECnet multicast frames when permanent bridging entry and DECnet are configured. There is no workaround. [CSCdk27418]

IP Routing Protocols

- For a Cisco 7000 router running Cisco IOS Release 11.1(15)/11.2(8), CPU utilization stays at 87 percent due to the IP-RT background process. This problem occurs when a static route is configured for a down or non-existent interface. A workaround is to remove the static route. [CSCdj54602]
- Issuing a **show ip eigrp event**, a **show ipx eigrp event**, a **show appletalk eigrp event** command, or enabling Enhanced IGRP event logging for IP, IPX, or AppleTalk may cause the following platforms to reload with a bus error or segv: 1000, 2500, 2600, 3800, 4000, 5200, and 7000 (RP/SP). Other platforms, including the Cisco 3600, 4500, 4700, 5300, 7000 (RSP), 7200, 7500, 8500, and RSM may display the record of a spurious memory access.

The Enhanced IGRP event log is invalid on all platforms.

The workaround to this problem is not to display the event log or enable Enhanced IGRP event-logging. Additionally, the event log can be disabled by issuing one of the following configuration commands:

For IP: **router eigrp as eigrp event-log-size 0**

For IPX: **ipx router eigrp as event-log-size 0**

For AppleTalk: **appletalk eigrp event-log-size 0** [CSCdk33475]

Wide-Area Networking

- It is possible for a system to encounter problems when an online insertion and removal (OIR) occurs. One of the symptoms of this problem is for the VIP CPU load to remain near 99 percent. This problem occurs because the VIP continues to transmit packets to the removed interface using distributed fast switching. Only a system reload or micro reload would clear the problem. [CSCdj35436]

Caveats for Release 11.1(1) through 11.1(20)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(20). These caveats also apply to Releases 11.1(1) through 11.1(19) (unless otherwise noted).

For more caveats of Release 11.1(20) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(21).

Basic System Services

- In a RSP system it is possible to get a software forced failure due to redzone corruption if the following is configured on the router:
 - HSA and large configurations, or configuration compression and large configurations, or all three, and the configuration file is the size of “boot buffersize” in the configuration (boot buffersize defaults to approximately 126K bytes).

A workaround for this problem is to make the “boot buffersize” in the config larger. We suggest 100K bytes larger than the configuration to allow room for configuration changes. [CSCdk14608]
- A Cisco 7000 with a Silicon Switch Processor may discover an additional Ethernet Interface, E0/8, which doesn't exist. This may be followed by “CBUS-3-INITERR” errors and other strange behavior including the router reloading.

This issue is due to corrupted SSP microcode which got incorporated into the release. The solution is to load a newer image which has uncorrupt SSP microcode or to load the uncorrupt SSP microcode directly. The Cisco IOS 11.1(20) release image contains the correct microcode. [CSCdk14917]
- The accounting code should be executed only when **aaa new-model** is enabled. [CSCdk17943]

Interfaces and Bridging

- Vines and CLNS routing paths are not learned when bridging over HDLC-SMDS. [CSCdj40742]
- Transparently bridging IP over FDDI may fail. [CSCdk04111]
- This caveat applies to HDLC, Frame Relay, and LAPB stac-compressed links. Some packets sized near a link's MTU are erroneously rejected. This caveat manifests slightly differently on all of these encapsulations. [CSCdk12078]
- Transparent bridging may fail on an FDDI interface on a Cisco 7200 platform. [CSCdk24341]

IP Routing Protocols

- Enhanced IGRP may crash when receiving updates in a network that has a major topology change in conjunction with an Enhanced IGRP topology database with neighbor counts exceeding 100 and route counts exceeding 4000. Routers in topologies which are borderline may experience CPUHOG messages in addition to or instead of a failure. Routers which greatly exceed these numbers are more likely to fail. [CSCdj54728]

ISO CLNS

- If IS-IS routing for IP is configured then unconfigured multiple times, the router may reload when an IP address is removed from an interface. [CSCdk24547]

TCP/IP Host-Mode Services

- TCP uncompress code may discard a bad frame without releasing the packet memory associated with it. This causes a memory leak and an interface may become wedged if the number of bad frames received reaches the input queue limit. [CSCdj77906]

Wide-Area Networking

- A Cisco 4700 router may constantly display the following error message:

```
%SYS-2-INPUTQ: INPUTQ set, but no idb, ptr=60C43314  
-Traceback= 60037A78 60039F6C 6003EF98
```

[CSCdi87914]

- A race condition existing in the current SSCOP code can sometimes lead to a system failure. The workaround is to disable the SSCOP quick polling scheme. [CSCdj93988]
- The SSCOP quick polling scheme which was made the default scheme in router images can sometimes result in SSCOP resets. This quick polling can reorder the poll PDUs sent from the router thereby leading to sequencing errors. [CSCdk08643]

Caveats for Release 11.1(1) through 11.1(19)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(19). Since Release 11.1 changed from a seven-week to a fourteen-week maintenance schedule after Release 11.1(18), Release 11.1(19) was only released as an interim version. These caveats also apply to Releases 11.1(1) through 11.1(18) (unless otherwise noted).

For more caveats of Release 11.1(18) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(20).

IBM Connectivity

- In some situations WFQ might drop OSPF and EIGRP HELLO messages causing the protocol to go down. Work around to this problem is to disable WFQ on the interface. [CSCdj95348]
- Cisco 2523 routers running Cisco IOS Release 11.1(18.1) will not pass non activation XIDs when configured for XID pass-thru. The impact of this is not serious unless you require PU 2.1's to remain active while Vtam is down. [CSCdk01631]
- The -r parameter for the APPN ping command is broken. Issuing the command with this parameter will cause the box to stop responding to network control traffic, and new sessions will be unable to start. A router reload will be required. [CSCdk05802]
- The maximum memory access for APPN is adjusted as the maximum memory capacity of Cisco routers increased to 256 MB. With this fix, the APPN subsystem can use the full 256 MB of main memory of the router. [CSCdk08186]

Interfaces and Bridging

- An online insertion and removal (OIR) of any interface processor in an RSP-based Cisco 7000 or 7500 router that contains a Fast Ethernet Interface Processor (FEIP) may result in disruption of the system if the interface processor is inserted or removed while the FEIP is busy switching data. Symptoms following the OIR include CyBus errors or MEMD errors which may be accompanied by CBus complex restarts. In severe cases the router may reload due to a Cache Parity Exception. [CSCdj89682]

- While receiving bridged input from a virtual device on a Cisco 7500 series router with FDDI interface(s) in the bridge group, the software could attempt to send an interface processor command to the virtual device, thereby causing the router to fail. [CSCdk00164]
- Ethernet collisions on the Cisco 7513 PA-8E port adapter are not counted correctly. Collisions are zero for over 2 million packets. There is no workaround. [CSCdk01150]
- When a router is configured with a mixture of compressed and uncompressed Frame Relay interfaces, sub-interfaces, or DLCIs, some packets are inappropriately compressed. The symptoms vary widely, in some cases NLSP neighbors will flap, in other cases LMI messages may be misdelivered. [CSCdk05157]

IP Routing Protocols

- Issuing the command **ospf ignore lsa mospf** does not suppress all error messages related to MOSPF. In particular, error messages about receiving MOSPF LSA in link state acknowledgment packet are still generated. These error messages will appear if there are more than two MOSPF routers on the same LAN as the Cisco router. [CSCdj66792]
- A router configured for Enhanced IGRP, under unusual circumstances, may lose routes from the routing table. Examination of the Enhanced IGRP topology entry for the lost route will reveal the feasible distance as infinity (4294967295) even though the metric for that route is good.

The loss of the route is due to sporadic line congestion (packet drops) and/or an SIA event on the same link as the neighbor occurring while a route is active. On very rare occasions, this can result in a lost acknowledge packet and a retransmission of the reply packet. For the failure to occur the retransmitted reply must have a valid metric.

A workaround is to issue the command **clear ip route ***. [CSCdj73617]

- If a Cisco router is attached to a network that includes a Proteon router, free processor memory in the Cisco router can very slowly decline. This is due to a memory leak in the OSPF process. [CSCdj78467]
- On a Cisco 7206 router, with a large number of redundant connections and Enhanced IGRP configured, the router may fail if the interfaces are changed from passive to active or from active to passive. A workaround is to set some of the interfaces passive and not change them to active. [CSCdj81611]
- The fix to caveat CSCdj64479 caused a memory leak for routers running Enhanced IGRP. Depending on the amount of free memory and the number of route changes, the router will eventually become unstable. Additionally, a separate issue was uncovered; as a network is deleted, Enhanced IGRP may record spurious accesses. The spurious accesses do not seriously affect router operations. [CSCdk03200]

ISO CLNS

- If an external route is known to IS-IS by multiple optimal paths, and one or more backup paths, the backup path information may be lost temporarily under certain circumstances. When this happens, the route may appear to be unreachable for a period of time.

Specifically, this can happen when the external route is known via the backup path, then becomes known via multiple optimal paths at about the same time, followed later by the loss of the optimal paths. The problem disappears when an SPF is run for any reason.

A workaround is to force an immediate SPF on the router (for example, by issuing the commands **shutdown, no shutdown** on a loopback interface running ISIS). Note that this can be done on any router in the same area. [CSCdk05616]

Miscellaneous

- An online insertion or removal (OIR) of an interface processor in an RSP-based 7000 or 7500 series router may result in multiple interfaces dropping very large numbers of incoming packets after the OIR. This problem may be seen on interfaces of other boards, as well as the interfaces on the board that was inserted or removed. The problem can be observed by a large and increasing number of packets reported in the “ignore” counter in the output of the **show interfaces** command. Communication through these interfaces will be severely impacted. This problem is most likely to occur in routers that have many active interfaces, and some interfaces with moderate to high traffic load. The problem is rare in routers that have few active interfaces and lightly loaded interfaces. The workaround is to reload the controller microcode using the **microcode reload** configuration command after the OIR event or power down the router to remove and insert cards. [CSCdk07259]

Novell IPX, XNS, and Apollo Domain

- Fast switching to some servers may appear to stop working if the server is brought down and then brought back up, while the default route is known.

A workaround is to run with fast switching disabled or clear the IPX route cache when this is noticed. [CSCdj59732]

Wide-Area Networking

- Processor memory parity errors are not being reported correctly on the VIP2 (10/15/20/40/50) product family.

When running an image that has CSCdj93505 integrated into it, crash output for VIP2 products with a signal value of 20 indicates that a cache parity error condition was detected.


```
%VIP2 R5K-1-MSG: slot3 System Reload called from 0x..., context=0x...  
%VIP2 R5K-1-MSG: slot3 System exception: sig=20, code=0x..., context=0x...
```


When this signal is present, the contents of the VIP crashinfo file are required for proper analysis.

When running an image that does not have CSCdj93505 integrated into it, the parity error may manifest in different ways. CSCdj20187 documents one such example. [CSCdj93505]
- The router attempts to display “unknown sub-interface type 0x2” when Frame Relay subinterfaces are configured on Frame Relay NNI. This display may either cause a system reload or a kernel error message like “SYS-2-NOBLOCK messages.” [CSCdk05107]
- Unsolicited drop parties/releases are sent on multipoint SVCs. In a LANE environment this might lead to random LEC failures. The root cause for this problem has been identified and fixed. [CSCdk06968]

Caveats for Release 11.1(1) through 11.1(18)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(18). These caveats also apply to Releases 11.1(1) through 11.1(17) (unless otherwise noted).

For more caveats of Release 11.1(18) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(19).

Basic System Services

- When a Cisco 4500 router is booted using 11.1(11) boot-flash with PRI-NPM, the following error message comes up:

```
%SYS-3-SUPNONE: Registry 23 doesn't exist
[CSCdj19276]
```

- The console/virtual-terminal exec on Cisco 7500 HSA systems may become unresponsive with the **write memory** command and configurations larger than 128K and **service compress-config**.

If this problem occurs, the configuration NVRAM of both the master and slave RSP will be invalid after a reboot and must be recovered manually as follows:

1. Send an RS-232 break to the console of both the master and slave.
2. Issue the ROM monitor **confreg** command on the master and slave to ignore the system configuration.
3. Issue the ROM monitor **reset** command on the master and slave to boot a slave-capable image.
4. On the master console, copy a good configuration file from Flash memory or TFTP into running-config.
5. Turn off the 0x40 bit in the configuration register by issuing the **show version EXEC** command and the **config-register** configuration command.
6. Issue the **reload** command to reload the master.

A workaround is to store the configuration in Flash memory. For example, issue the **copy running slot0:config** or **write memory** commands while configured with **boot config slot0:config**, **service compress**, and **boot buffersize n**, where *n* is at least three times the configuration size in bytes. In this case, the **write memory** command will work slowly - 10 minutes elapsed time for each 128k block of configuration text. [CSCdj63926]

- A corrupt buffer header is causing Cisco 7500 routers running Cisco IOS Release 11.1.(15.05)CA to restart with a bus error. [CSCdj80564]
- In some network conditions it is possible for Frame Relay LMI Status Enquiry packets to be delayed before transmission in the router by other routing or control packets and then appear on the wire out of order. This can cause some instability of the Frame Relay circuit during the time the Status Enquiries are delayed by the other packets. The instability is seen as the Frame Relay PVC being declared Inactive at the remote end and then Active again about 1 minute later. The Frame Relay switch at the local end will report LMI Timeouts and Sequence Number Mismatches.

It is also possible for this problem to occur on HDLC serial lines and cause instability due to HDLC keepalive packets being delayed.

This is a rare occurrence and has only been seen with very large IPX SAP updates sent over a slow-speed circuit. The size of updates necessary to cause this problem on a 56 kbps circuit is around 3000 SAPs. The problem is more likely to occur when there is data traffic at near-line capacity on the circuit.

It is theoretically possible for other routing or control packets such as OSPF Link State Advertisements (LSAs) or NLSP Link State Packets (LSPs) to cause the same effect in a period of severe routing instability in a large network with many Frame Relay subinterfaces. The issue is less likely to be seen when Weighted Fair Queuing is used on the serial interface rather than First In First Out (FIFO) queuing. Please note that there are many other possible causes of instability of Frame Relay or serial circuits and the manifestation of this particular caveat in operating networks is unlikely.

If the issue is seen because of very large IPX SAP updates, the workaround is to configure an **ipx output-sap-delay** and **ipx output-rip-delay** that is larger than the propagation delay of a SAP packet across the circuit. A delay of 110 ms is sufficient for a 56K circuit. The possibility of seeing this caveat with very large IPX SAP updates was introduced by CSCdj18092. [CSCdj91667]

IBM Connectivity

- Under certain stress conditions where a router's buffer is depleting (when processing DLUR pipe traffic, gds 1500 variables), the router sends an unsolicited reset IPM request to VTAM. VTAM immediately sends a reset IPM acknowledgment. Upon receiving this reset IPM acknowledgment, the router unbinds its cpsvrMgr (DLUR pipe) and cpsvrMgr (CP-CP) sessions. [CSCdj44512]

- A router configured for APPN may crash due to a bus error at PC 0x902FA6 (asm_mainline). The stack trace may not show the routines called prior to the crash. In that case, the router needs to be set up for a core dump

There is currently no known workaround [CSCdj77914]

- When a router is configured for DLSw/QLLC and the first SNA XID is from the LAN through the router to X.25, then the router sets the ABM bit in the SNA XID to 1 (byte 19, bit 1). This is not supported by all QLLC devices. [CSCdj81191]

- A router running RSRB might crash when a badly formed LNM packet is received.

A workaround for this is to disable LNM on the router by issuing the command **lnm disable**. [CSCdj82340]

- APPN/DLUR: A router reload can occur when DLUR processes a flow on the DLUS/DLUR connect which must be responded to negatively because the PU has disconnected. This is a regression defect introduced by CSCdj59639. [CSCdj84659]
- The APPN router may reload due to a spurious memory access in recreate_small_fid2_mu. The following messages are displayed on the router console before the reload:

```
%APPN-7-APPNETERROR: Insufficient available buffer supply
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x606F5A4C reading 0x50
```

The **show stack** command displays the following backtrace:

```
#0 0x606F5A4C in recreate_small_fid2_mu
#1 0x606fdbd4 in transfer_to_dynamic_and_send
#2 0x606fce90 in sc_process_mu
#3 0x606f6900 in e
#4 0x606f6ed8 in fsm_receive_router
#5 0x606d6b20 in upchuck
```


- If a Cisco router is attached to a network that includes a Proteon router, free processor memory in the Cisco router can very slowly decline. This is due to a memory leak in the OSPF process. [CSCdj78467]
- On a Cisco 7206 router, with a large number of redundant connections and Enhanced IGRP configured, the router may crashed if interfaces are changed from passive.
Workaround is to set some of the interfaces passive and not change them to active. [CSCdj81611]
- Enhanced IGRP redistribution between different AS is broken when interface flaps. This is a regression from the fix for CSCdj62406 [CSCdj85316]
- Intermittently, an FDDI Forward/Dense entry is not added to the outgoing interface list (olist) of a Source-Group (SG) routing table. The end result is that the FDDI interface does not forward mpackets as it should until the **clear ip mroute** command is executed. This problem may occur when multiple Cisco 7513 routers run Release 11.1(16)CA with FDDI, FastEthernet, and Ethernet interfaces. [CSCdj92400]

Novell IPX, XNS, and Apollo Domain

- Fastswitching to some servers may appear to stop working if the server is brought down and then brought back up, while the default route is known.
A workaround is to run with fastswitching disabled or clear the IPX route cache when this is noticed. [CSCdj59732]

Wide-Area Networking

- Some PPP implementations erroneously send PPP packets that exceed the negotiated Maximum Receive Unit. If these packets are also larger than 1500 bytes (which all RFC 1661 compliant implementations are capable of receiving), Cisco IOS software with the CSCdi92482 patch applied will silently discard them. This is the correct behavior per the RFC.

It may be possible to work around the problem by using the **mtu** command to select a smaller MTU/MRU value for the interface, but this will only work if the remote peer agrees to negotiate the smaller value. Another workaround is to downgrade to a version of software that does not contain the CSCdi92482 patch.

To verify the problem, issue the **debug ppp error** command and search for a debug message of the following form:

```
Se6/0/0:23 PPP: Packet too large, size = 1509, maxsize = 4, protocol = 0x003D  
[CSCdj82427]
```

- When loading a configuration at boot up, from Flash memory, or from the network, a router will fail if the configuration contains the following commands:

```
lane fixed-config-atm-address  
lane auto-config-atm-address
```

A message of the following form will be generated:

```
%LANE-4-LECS_WARN: ATM1/0: can't register  
47.0079000000000000 000000.00A03E000001.00 with signalling  
(duplicate address ?)
```

As a workaround, use only a single LECS address configuration or do not enable logging timestamps if multiple LECS addresses are required. [CSCdj83816]

- Following a CyBus error on an RSP, the following messages may be present:

```
%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
-Traceback= 6014B948 6014BEDC 6020BEB0 6020BFB0 60207048 60217C0C 6021A53C
6020BC20 601C0454 601C054C 601C0CBC 601BF650
%SYS-2-MALLOCFAIL: Memory allocation of 352 bytes failed from 0x6014BED4, pool
Processor, alignment 0
-Process= "<interrupt level>", ipl= 6
-Traceback= 6014A2D8 6014BB64 6014BEDC 6020BEB0 6020BFB0 60207048 60217C0C
6021A53C 6020BC20 601C0454 601C054C 601C0CBC 601BF650
```

These messages may repeat, and the RSP may also hang as a result. An image with CSCdj85257 integrated in will resolve these secondary problems and the RSP will recover normally. CSCdj85257 will not resolve the original CyBus error, however. [CSCdj85257]

- Processor memory parity errors are not being reported correctly on the VIP2 (10/15/20/40/50) product family.

When running an image that has CSCdj93505 integrated into it, crash output for VIP2 products with a signal value of 20 indicates that a cache parity error condition was detected.

```
%VIP2 R5K-1-MSG: slot3 System Reload called from 0x..., context=0x...
%VIP2 R5K-1-MSG: slot3 System exception: sig=20, code=0x..., context=0x...
```

When this signal is present, the contents of the VIP crashinfo file are required for proper analysis.

When running an image that does not have CSCdj93505 integrated into it, the parity error may manifest in different ways. CSCdj20187 documents one such example. [CSCdj93505]

- The router attempts to display “unknown sub-interface type 0x2” when Frame Relay subinterfaces are configured on Frame Relay NNI. This display may either cause a system reload or a kernel error message like “SYS-2-NOBLOCK messages.” [CSCdk05107]
- Unsolicited drop parties/releases are sent on multipoint SVCs. In a LANE environment this might lead to random LEC failures. The root cause for this problem has been identified and fixed. [CSCdk06968]

Caveats for Release 11.1(1) through 11.1(17)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(17). These caveats also apply to Releases 11.1(1) through 11.1(16) (unless otherwise noted).

For more caveats of Release 11.1(17) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(18).

Basic System Services

- A new configuration command now exists for RSP routers to control caching policies for memory regions. A user can now configure MEMD to be accessed uncached by issuing the **memory cache-policy io uncached** configuration command.

This method is better than having to enter the **test rsp cache memd uncached EXEC** command every time the router is booted.

This configuration command can be used as a workaround for problems like CSCdj52309 and CSCdj70296.

To restore the MEMD caching policy to the original write-through policy, issue the **memory cache-policy io write-through** command. To determine what memory cache policies are currently configured on your router, use the **show rsp** command. [CSCdj33812]

- When running Cisco IOS Release 11.2(11) with Kerberos authentication, the main memory will decrease. The Access Server will run slow, but it will not crash. The access server will need to be reloaded to reset the memory. There is no work around yet. An alternate IOS image is not an option for this access server. [CSCdj76071]

IBM Connectivity

- Timers are not cleaned up properly in LLC2. This may result in crashes when RSRB local acknowledgment is used under a high load. [CSCdj42474]
- In a rare timing situation, an APPN/DLUR router may reload due to a bus error/segV exception at ndr_sndtp_encap_mu. [CSCdj59639]
- Memory leaks may be observed in routers running LNM especially at a burst. [CSCdj66894]

Interfaces and Bridging

- A TRIP interface configured for transparent bridging but not configured for source route bridging may silently drop some incoming frames. Specifically, if the interface receives a frame with length less than 120 bytes and the RII bit is set (indicating a source route bridging frame) it may drop the next frame received. This can cause the interface's keepalive processing to fail and can lead to sporadic resets on the interface. [CSCdi88756]
- A Cisco 4000 router connected to a FDDI ring and a Token Ring can cause corruption of data in packets going from the FDDI ring to the Token Ring. This is strictly data corruption, there is no corruption of the protocol or the checksum. Packets going from the Token Ring to the FDDI ring are unaffected. [CSCdj05331]
- A Cisco 7000 router with a FIP will not boot properly if the command **microcode reload** is in the configuration. [CSCdj32533]
- For Fast Ethernet interfaces on Cisco 7500 series, 7200 series, 4000 series, or 3600 series routers, the regular Fast Ethernet PA **media-type** configuration command is missing the RJ45 option; only the MII option is available.

For example, on a Cisco 7200 series router with Fast Ethernet port adapter 6/0, the problem looks like the following:

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
int f 6/0
media ?
MII Use MII connector <--- Only MII, no RJ45
```

This problem appears on the following platforms in the specified Cisco IOS releases:

- Cisco 7200 series: Cisco IOS Releases 11.1, 11.1 CA, 11.2, 11.2 P, 11.3, and 11.3 T.
- Cisco 7500 series: Cisco IOS Releases 11.1, 11.1 CA, 11.2, 11.2 P, 11.3, and 11.3 T.
- Cisco 4000 series: Cisco IOS Releases 11.1, 11.1 CA, 11.2, 11.2 P, 11.3, and 11.3 T.
- Cisco 3600 series: Cisco IOS Releases 11.2, 11.2 P, 11.3, and 11.3 T. (The Cisco 3600 series does not support Releases 11.1 and 11.1 CA.)

A workaround is available on most of the platforms and Cisco IOS images; to configure for RJ45, use the **no media-type MII** command. The following is an example of the workaround on a Cisco 7500 series router with Fast Ethernet port adapter 0/0/0:

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
int f 0/0/0
no media MII <--- switch to RJ45
```

This workaround is available on the following platforms running the specified Cisco IOS releases:

- Cisco 7200 series: Cisco IOS Releases 11.2, 11.2 P, 11.3 and 11.3 T.
- Cisco 7500 series: Cisco IOS Releases 11.1, 11.1 CA, 11.2, 11.2 P, 11.3 and 11.3 T.
- Cisco 4000 series: None.
- Cisco 3600 series: Cisco IOS Releases 11.2, 11.2 P, and 11.3

Platform defaults are correctly preserved for all platforms and images that default to RJ45. The following platforms running the specified releases default to RJ45:

- Cisco 7200 series: Cisco IOS Releases 11.1, 11.1 CA, 11.2, 11.2 P, 11.3 and 11.3 T.
- Cisco 7500 series: Cisco IOS Releases 11.1, 11.1 CA, 11.2, 11.2 P, 11.3 and 11.3 T.
- Cisco 4000 series: Cisco IOS Releases 11.1, 11.1 CA, 11.2, 11.2 P, 11.3 and 11.3 T.
- Cisco 3600 series: Cisco IOS Releases 11.2, 11.2 P, 11.3 and 11.3 T. (The Cisco 3600 series does not default to RJ45 media for Fast Ethernet interfaces on Release 11.3 T. The RJ45 port on the Cisco 3600 FE ports will not be usable in images with this problem.)

This problem first appeared in the following releases: 11.1(16.2), 11.1(15.3)CA, 11.2(10.4), 11.2(10.4)P, 11.3(1.2), and 11.3(1.2)T.

This problem was fixed in the following releases: 11.1(17.1), 11.1(17)CA, 11.2(11.4), 11.2(11.4)P, 11.3(1.5), and 11.3(1.5)T. [CSCdj75983]

- Cisco 7200 series routers configured with ISL on the C7200-I/O-FE Fast Ethernet port fail to transmit ISL encapsulated packets. There is no problem with native (non-ISL) packets going out on the same interface. This problem does not occur on the PA-FE-TX and PA-FE-FX, or while running Cisco IOS Release 11.3(1) or 11.3(1)T.

As a workaround, use the PA-FE-TX or PA-FE-FX interfaces for ISL traffic or use Releases 11.3(1) or 11.3(1)T. [CSCdj79992]

IP Routing Protocols

- The output of the **debug ip routing** command indicates that the route to 0.0.0.0 is removed and reinstalled into the routing table with the same metric. [CSCdj06220]

TCP/IP Host-Mode Services

- Under rare circumstances, a router reload may occur while running TCP to X.25 protocol translation. [CSCdj23230]

Wide-Area Networking

- When all existing AIPs are extracted and hot swapped, SVCs can no longer be established.
In the case of multiple AIPs, change them one at a time. In the case of only one AIP, insert the new AIP before extracting the existing AIP. [CSCdj71438]
- When using ARA version 3.0, a Cisco router allocates an AppleTalk node address of 0 and PPP negotiation fails. [CSCdj77846]

Caveats for Release 11.1(1) through 11.1(16)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(16). These caveats also apply to Releases 11.1(1) through 11.1(15) (unless otherwise noted).

For more caveats of Release 11.1(16) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(17).

Basic System Services

- The Cisco 7500 series may not correctly allocate the right number of packet memory (memd) buffers to some network interfaces. This problem requires a large number of interfaces whose collective bandwidth is high, but their MTU is smaller than another buffer pool.

For example, a problem was found with a Cisco 7500 series using a large number of Fast Ethernet and/or Ethernet interfaces and one or more FDDI interfaces. The pool of packet memory should have allocated 80 percent of the memory to the Ethernet and Fast Ethernet interfaces, which use an MTU of 1536. Instead it received 20 percent of the memory, and the lone FDDI interface with MTU 4512 got 80 percent of the packet memory.

The problem occurred with 55 Ethernet, 6 Fast Ethernet, and 1 FDDI network interfaces. The problem did not occur with fewer interfaces, specifically 36 Ethernet, 5 Fast Ethernet, and 1 FDDI interfaces.

The problem may show up as a high number of input drops on some router interfaces. [CSCdj55428]

IBM Connectivity

- A router may restart unexpectedly with SegV exception, PC 0x0, when the router is configured for DLSw. [CSCdj16559]
- When running proxy explorer and NetBIOS name caching on a Token Ring interface of a Cisco 7200 router, alignment errors will occur. [CSCdj52522]
- When an actpu is followed by a dactpu from VTAM and there has been no response from the downstream device to either flow, after a disconnect is received from the downstream device, DLUR will send a -rsp(actpu) upstream instead of the proper flow, +rsp(dactpu). This can cause the PU from the DLUS perspective to hang in PDACP state. [CSCdj61872]
- It is rare, but possible, for DLUS to send a -rsp(REQDACTPU). When this happens, it indicates that VTAM has already cleaned up the PU in question. When receiving this response, DLUR must clean up the PU to avoid the PU from being stuck in “stopping” state. [CSCdj61879]

- When using APPN/DLUR with a large number of LUs (over 1000), a memory spike can occur during the processing of a downstream PU outage. In extreme cases, this memory spike can be large enough to exhaust memory in the APPN/DLUR router and cause a reload. [CSCdj61908]
- If an RSRB session is disconnected by the local LAN side at exactly the same time as a data message is received from a remote host, a situation can occur that will lead to a crash in `llc_get_queue_status()`. There is no workaround. [CSCdj62026]
- Session attempts fail with DLUR generating a sense 08060000 in a rare case where the LU name list gets corrupted. This problem is easily identified by the VTAM LU showing “active” state, while the **show appn dlur-lu name** display does not show the LU. [CSCdj62172]
- When source-route translational bridging is used, LLC sessions that are initiated from the transparent domain will result in the source-route largest frame to be incorrectly set to 4472 instead of 1500. The result is that SNA and NetBIOS sessions may fail if the source-route station sends a frame with a payload that exceeds the maximum allowable size of 1500 for Ethernet media.

The problem typically occurs when NetBIOS is utilized to allow workstations to communicate between Ethernet and Token Ring. It will also occur when SNA is used.

The workaround is to disable fast switching by using the command **no source-bridge transparent fastswitch** or configure the end stations to use frames with a payload of less than or equal to 1500 bytes. [CSCdj62385]

- Any DLUR installation with over 800-1000 downstream PUs may experience a reload with the following backtrace:

```
[abort(0x601f2c3c)+0x8]
[crashdump(0x601f0b20)+0x94]
[process_handle_watchdog(0x601c2f08)+0xb4]
[signal_receive(0x601b7d58)+0xa8]
[process_forced_here(0x60169424)+0x68]
[locate_node_index(0x607dbcc0)+0x64]
[etext(0x60849e00)+0xcbee04]
```

[CSCdj67966]

- APPN router may reload in rare situations with the following backtrace:

```
RA: 0x607E1724[find_matching_row(0x607e16ec)+0x38] RA:
0x607E1B9C[Tfind_next(0x607e1b70)+0x2c] RA:
0x6071182C[DBfind_next_directory_entry(0x60711814)+0x18] RA:
0x6070BAD8[CPdelete_men(0x6070ba90)+0x48] RA:
0x6070BA78[CPupdate_cp_status(0x6070b9c0)+0xb8] RA:
0x6070B40C[CPmain(0x6070b300)+0x10c] RA: 0x6070AC2C[newdss00(0x6070ab60)+0xcc]
RA: 0x60183F80[r4k_process_dispatch(0x60183f6c)+0x14]
```

[CSCdj70817]

- APPN leaks memory when directory services processing unknown locate replies. [CSCdj70886]

Interfaces and Bridging

- When adding or removing a subinterface to a Frame Relay interface, all DLCIs are brought down until the Frame Relay switch sends the PVC information again. Two problems are associated with this caveat. One problem is that the whole interface will be reset when a user tries to add the **ip address** command. Caveat CSCdj02488 (integrated into 11.1(11) and 11.2(5.1)) fixed this problem.

A workaround for the second problem is to turn off CDP globally or on individual interfaces. In this case, the user can turn off CDP on the serial interface before adding or removing subinterfaces. [CSCdj07291]

- Under certain conditions, packets may stay on the input queue. [CSCdj30087]
- A Cisco 2520 low-speed port may sometimes ignore group polls. This problem occurs on average once per minute and appears to occur only when the router is configured for half duplex and is using a DTE cable.

This problem should have minimal impact on the performance of a multidrop line because a FEP usually resorts to individual polling. [CSCdj33392]

- When transparent bridging to a Token Ring interface, it is possible for the interface to read in a frame it has forwarded onto the Token Ring interface. This will cause the bridge table to be incorrect.

The problem only affects the mid-range and low-end platforms. [CSCdj41666]

- A Cisco 4700 with a Fast Ethernet interface may freeze for a few seconds with Receive FIFO overflow messages. [CSCdj45097]
- Fast Ethernet might hang when process switching 1518 byte frames. The workaround for this problem is to configure the following buffer allocation commands:

buffers big min-free 5 buffers large max-free 10 buffers huge max-free 4 [CSCdj50120]

IP Routing Protocols

- If OSPF external routes are summarized using the **summary-address** command, and the number of external routes being covered by this summary address drops to zero, the external summary will be flushed, but the router originating the summary will not install any matching external or NSSA routes that may be present in its database.

The router can be forced to install the matching route by using the **clear ip route *** command. [CSCdj32471]

- Some Cisco and Proteon routers have an interoperability issue. The Cisco router will install the latest “learned” route into the Proteon’s Internal Address, which may not be the shortest path.

This issue occurs when the Proteon router’s Internal Address is advertised as a Host Route, not a network, in the router’s LSA. A Host Route is represented as a Type 3 link (Stub Network) whose link ID is the host’s IP address and whose Link Data is a mask of all ones (0xffffffff). This Host Route is advertised into all OSPF areas. [CSCdj56079]

- With EIGRP routing configured, redistribution of the following type of routes into the EIGRP process will not work correctly:
 - A directly connected route
 - A static route with the next hop set to an interface
 - A static route with the next hop set to a dynamically learned route

The nature of the defect is that it will only occur after a dynamic event. If redistribution is manually configured, EIGRP will initially reflect correct information in the topology table; however, after any sort of dynamic event, the topology table becomes invalid and routing updates sent are inaccurate. [CSCdj58676]

- When the IP multicast tunnels (DVMRP, GRE) from a serial interface are moved to an ATM interface on a Cisco 4700 router, the packets become process switched instead of fast switched, which causes a lot of CPU (IP INPUT).

Incoming packets on the ATM interface and outgoing packets on the serial interface also experience this problem. However, incoming packets on the serial interface and outgoing packets on the ATM interface do not experience this problem.

It seems that incoming packets are not fast switched. [CSCdj59076]

- Dynamic redistribution into EIGRP from another routing protocol fails if the routes being redistributed fall within the same major network as EIGRP. A temporary workaround is to remove the redistribution statement from the EIGRP configuration, then re-insert the redistribution statement. [CSCdj65737]

TCP/IP Host-Mode Services

- The program land.c, which can be used to launch denial of service attacks against various TCP implementations, sends a TCP SYN packet (a connection initiation), giving the target host's address as both source and destination, and using the same port on the target host as both source and destination.

For in-depth information including workarounds and information on other Cisco product vulnerabilities, refer to the following URL:

<http://www.cisco.com/warp/customer/770/land-pub.shtml> [CSCdj61324]

Wide-Area Networking

- When using DLCI prioritization on a point-to-point Frame Relay subinterface and one of the DLCIs fail, the subinterface may bounce once or continually bounce during LMI full status reports, depending on whether LMI reports the DLCI as being DELETED or INACTIVE. This behavior is the same for every DLCI defined in the **priority-dlci-group**.

During normal behavior, the point-to-point subinterface should go down when the primary DLCI fails. If a secondary DLCI fails, the subinterface stays up, but traffic destined for that DLCI only will fail. [CSCdj11056]

- Running Cisco IOS Release 11.1(11) on a Cisco 4700 router might cause memory corruption, which will cause the router to reload. [CSCdj24418]
- The SSCOP layer sequence number wraparound conditions lead to memory leaks and memory fragmentation problems. The problem occurs when the SSCOPs send sequence number reaches a maximum value of 16777215. The switch needs to be reset to continue normal functionality. [CSCdj45157]
- When the commands **ip tcp header-compression** and **ppp multilink** are configured together on the same interface, it can cause the router to crash.

The workaround is to remove the **ip tcp header-compression** or **ppp multilink** command. [CSCdj53093]

- RSP crashes at `rsp_fs_free_memd_pack` may be caused by previous releases of AIP microcode in the router that is crashing or in routers that are feeding this router in the same network. [CSCdj59745]

Caveats for Release 11.1(1) through 11.1(15)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(15). These caveats also apply to Releases 11.1(1) through 11.1(14) (unless otherwise noted).

For more caveats of Release 11.1(15) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(16).

Basic System Services

- A timing conflict between the HTTP server and TACACS+ code can cause the HTTP process to hang when configured to use TACACS+ for authentication. Since the HTTP server uses a tty to handle I/O for the request, these hung processes can tie up all available ttys. [CSCdi84657]
- If the **map-list** command is configured, issuing the **show running** command may cause the router to crash if the “Last configuration change at...” informational string exceeds a total length of 80 characters. [CSCdj13986]
- When custom or priority queuing is turned off on an interface that does not support fair queuing, the queuing data structures associated with the interface are left in an inconsistent state.

In particular, the enqueue and the dequeue routines are not reset and this causes the box to crash when the routines are invoked the next time. Once the box is rebooted, the inconsistency is cleared. [CSCdj29439]

- The input queue may be wedged with IP packets if the **exception dump** command is configured.

The following are known workarounds:

- Increase the input queue to 175. ([75]Original Queue amount+[100] per **exception dump** *x.x.x.x* command)

- Remove the **exception dump** *x.x.x.x* command.

[CSCdj58035]

EXEC and Configuration Parser

- Entering the **privilege route-map level** *x* **set as-path prepend** *x* command in configure mode may cause the router to reload, even though the number after **prepend** is not necessary. The workaround is to not enter a number after **prepend**. [CSCdj37035]

IBM Connectivity

- A small window exists in which it is possible after a transmission group reinitialization that only one CP-CP session is established between the router and a neighboring node. In this case, the contention winner session from the perspective of the router is not activated. Once this occurs, the CP-CP contention winner session will only activate if the APPN subsystem is stopped and started.

There is no known workaround. [CSCdj25859]

- An APPN router may crash during an SNMP access to the APPN MIB. This problem only occurs after an unused APPN node is garbage collected. The crash has the following stack trace:

```
System was restarted by bus error at PC 0x8B5902, address 0x4AFC4AFC PC:
process_snmp_trs_tg_inc
```

```
0x8B5CAC: _process_ms_data_req_trs(0x8b5aaa)+0x202
0x87E5FE: _xxxtos00(0x87d6b0)+0xf4e 0x180E5C: _process_hari_kari(0x180e5c)+0x0
[CSCdj36824]
```

- On RSP-based routers the pseudo MAC address assigned to a bridge port on a source route bridge virtual ring group is incorrectly formatted to Ethernet format during Cisco IOS start up. This MAC address is used to establish a bridge link from IBM LAN Network Manager and can be shown by using the **show lnm config EXEC** command. [CSCdj38360]
- DLSw FST may corrupt the frame header if the riflen is different on both sides. [CSCdj40582]
- An APPN router may crash with a bus error if a race condition is experienced during cleanup processing. The stacktrace shows the crash occurred in Qfind_front while executing a psp00 function. An example stacktrace for this problem follows:

```
System was restarted by bus error at PC 0x3784864, address 0xF0110208 PC
0x3784864[_Qfind_front(0x3040a04+0x743e44)+0x1c] RA:
0x36C1F2E[_queue_find_front(0x3040a04+0x68151c)+0xe] RA:
0x36CC554[_psbfrm(0x3040a04+0x68bb30)+0x20] RA:
0x36CDAF6[_psp00(0x3040a04+0x68cfd4)+0x11e] RA:
0x314BD78[_process_hari_kari(0x3040a04+0x10b374)+0x0]
```

[CSCdj44198]

- When RSRB with TCP encapsulation is configured with priority peers and some of the priority peers are closed/dead, an explorer packet may continuously try to open the closed/dead priority peer. After several tries, the router may crash with memory corruption. [CSCdj47493]
 - A router will not pass SRB directed frames if the SRB proxy-explorer feature is configured. SRB proxy-explorer is used with NetBIOS name caching. [CSCdj47797]
 - Some 68K-based routers, such as the Cisco 7000, Cisco 4000, and Cisco 2500 routers, may crash while running APPN. This memory corruption may occur after a rare combination of APPN detail displays, followed by a **show appn stat** display.
- [CSCdj47941]
- An APPN router may fail the ACT_ROUTE if using parallel transmission groups (TGs). This problem may occur when an APPN router has two parallel links defined with the adjacent node. If the adjacent node activated a link to the network node (NN) requesting a TG number that had previously been used for a different defined link activation, the NN may fail the ACTIVATE_ROUTE. The APPN router sometimes tried to incorrectly activate the route using the other inactive link, which still had the same TG number. [CSCdj49814]
 - Executing a **show source** command may cause the router to restart unexpectedly if a virtual ring group or remote peer is deconfigured when the **source-bridge** command output is waiting at the **-- more --** prompt.

The workaround is not to reconfigure virtual rings or remote peers while executing a **show source** command. [CSCdj49973]

- Normal nonextended unbind (0x3201) was extended with corrupted information which caused rejection by the host. As far as the host is concerned, the session is still active. A user cannot clean up this session without bringing down the link. [CSCdj50581]

Interfaces and Bridging

- In certain cases, a router may bring Layer 1 down without an apparent reason. Hereafter, a new TEI is negotiated with the switch. The latter still keeps all call references belonging to the previous TEI, since no DISCONNECT was seen on L3. [CSCdj11840]
- The PA-4R may incorrectly adjust the datagram size of an incoming packet to include extra padding at the end of the packet. This problem only occurs under moderate/heavy traffic load where multiple PA-4R interfaces are consuming many particle buffers. The problem also only occurs on packets with a packet length that is a multiple of 512 bytes, 513 bytes, 514 bytes or 515 bytes. On Cisco 7000 series VIP PA-4R systems any type of packet may be subject to this corruption. On Cisco 7200 series systems with PA-4R, only source route bridging packets are subject to this corruption. The only workaround is to reduce the Token Ring interface's MTU to 508 bytes or less. [CSCdj48183]
- In Cisco 7500 series routers, the **show dialer** command is not working. The workaround is to use the **show dialer interface serial x/y** command. [CSCdj51612]

IP Routing Protocols

- A router may crash with a "System restarted by bus error at PC 0x60394488, address 0xD0D0D0D" message when running Cisco IOS Release 11.1(9) RSP with a heavy load of EIGRP and CSNA traffic. [CSCdj29447]
- BOOTP requests being sent to 0.0.0.0 get forwarded to the gateway of last resort when there is one. [CSCdj33809]
- A Cisco 7513 router running EIGRP reloads with the following message:

```
System restarted by error - an arithmetic exception, PC 0x60286234
```

The program counter value points to an EIGRP IOS routine. [CSCdj38361]
- ICMP unreachable are wrongly sent out for multicast packets. [CSCdj43447]
- If the OSPF summary host route is overwritten by a route from another routing process that has a lower administrative distance, it is possible that the OSPF summary host route will not be reinstalled after the latter route is removed. In particular, it only happens if the host route address is also the router ID of some ASBR. [CSCdj49161]
- When one of the routers on a broadcast network has been partitioned in which at least one partition has only one router, OSPF will generate a stub advertisement for this network in the isolated router's router LSA. This stub route will overwrite the normal network route calculated using the network LSA, regardless of the path cost.

This problem exists in all Cisco IOS releases starting at Release 10.3. The problem will be fixed in Release 11.1 and newer releases. [CSCdj53804]
- If a router is running out of memory while running OSPF, OSPF does not check to see if one of its structures has been properly allocated. This may result in a SegV exception, thus causing the router to reload. [CSCdj54524]

ISO CLNS

- Under certain circumstances, a Cisco 7505 router running Cisco Release 11.1(13a)CA1 will reload if the netID is changed under the IS-IS routing process. [CSCdj49485]

Novell IPX, XNS, and Apollo Domain

- Using any of the **xns flooding** commands may cause the router to reload, give alignment, bad pool, or buffer warnings. [CSCdj23479]
- If a route goes away via aging (180 seconds) and the default route is known, a cache entry may be installed for the network using the default route path. If the network comes back within the next 60 seconds, a new cache entry pointing to the now valid path may not be installed and the cache will still point to the default route path for the network. A workaround is to issue the **clear ipx route** and **clear ipx cache** commands, or run without using the default route. [CSCdj47705]

TCP/IP Host-Mode Services

- A router may restart with a bus error at address 0xD0D0D5D in module tcpdriver_del. [CSCdj26703]
- Sometimes a TCP control block structure is mistakenly freed during timeout processing, and the next reference to the structure will cause the router to crash. [CSCdj55793]

Wide-Area Networking

- On RSP platforms, if the load on a LEX interface increases to the point where the fast switching code decides to put packets on the process-level output queue, the system will crash. [CSCdj26184]
- Using NetBIOS over PPP may result in traceback messages complaining about invalid memory action at interrupt with traceback information appended:

```
%SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
```

[CSCdj42341]
- This patch prevents the use of an invalid pak-info_start pointer when doing payload compression on RSP platforms, thus avoiding a crash. [CSCdj43332]
- A remote DLSw peering router may send a DM response just after the LLC2 connection is established if the router is very busy and the PC station responds immediately to the UA with a RR. The client will need to reestablish the connection. [CSCdj47782]
- A boot image without a subsystem containing IPCP will restart the router. There is no workaround. [CSCdj48085]
- The **show x25 vc** command will cause the router to unexpectedly restart if there is a combination of locally switched virtual circuits and other virtual circuits. [CSCdj50405]

Caveats for Release 11.1(1) through 11.1(14)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(14). These caveats also apply to Releases 11.1(1) through 11.1(13) (unless otherwise noted).

For more caveats of Release 11.1(14) and earlier 11.1 releases, see the preceding section, “Caveats for Release 11.1(1) through 11.1(18).”

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(15).

AppleTalk

- ATCP may cause AppleTalk to trash memory and reload the router. There is no workaround. [CSCdj23355]

Basic System Services

- On Single Flash Bank 2500 devices running from the image on Flash (RFF), copying to flash using CISCO-FLASH-MIB does not work.

The workaround is to use the **copy tftp flash** command line interface command. This CLI command invokes the FLH interface and the file is copied successfully to the device. [CSCdj27438]

- RMON alarms will not work properly on a number of MIBs that use internal MIB caching to speed up MIB object value retrieval. The only possible workaround is to set up an SNMP get poll on these objects to force an update to the MIB cache, with a poll period within the alarmInterval time. The following MIBs have this problem:

APPN-DLUR-MIB
IBM-6611-APPN-MIB
CISCO-CIPCSNA-MIB
CISCO-CIPLAN-MIB
CISCO-CIPTCPIP-MIB
CISCO-SNA-LLC-MIB
SNA-NAU-MIB
CISCO-TN3270SERVER-MIB
OLD-CISCO-IP-MIB
BGP4-MIB
LAN-EMULATION-CLIENT-MIB
RFC1406-MIB
RMON-MIB
IF-MIB
RFC1398-MIB
OLD-CISCO-INTERFACES-MIB
CISCO-PING-MIB
CISCO-QLLC01-MIB [CSCdj34766]

- An SNMP Get of an individual instance from the ipNetToMediaTable may fail, even though an SNMP Get-next will successfully retrieve the instance. This is likely to be seen on table entries referring to software interfaces (for example, subinterfaces, loopbacks or tunnels) or hardware interfaces that have been hot-swapped in. There is no known workaround. [CSCdj43639]
- A Cisco 4500 running Cisco IOS Release 11.0(13) crashes in fr_fair_queue_flow_id. [CSCdj45516]

IBM Connectivity

- A 1500-byte frame sent to the SR/TLB code is dropped because the SR/TLB MTU is set to 1492 bytes. [CSCdj18838]
- A router configured for DLSw has a buffer leak in the middle and big buffers. Eventually, the router runs out of I/O memory.

The problem is related to the way DLSw backup peers are configured. This problem only occurs if the local router is configured with backup peer commands and the remote router also has a configured peer and is not promiscuous.

The workaround is to remove the DLSw backup peer configuration. [CSCdj21664]

- On a Cisco 7200 series router, duplicate ring entries may be seen in the RIF cache and when using the **debug source bridge** command. The duplicate ring entries lead to connectivity problems for end systems. [CSCdj21876]
- A DLUR router may reject unbind requests from the host if it has not received a bind response from the downstream LU.

If the downstream device never responds to the outstanding bind, the DLUR router will wait indefinitely and not free the local-form session ID (lfsid). This may cause a situation in which the host tries to reuse a lfsid after it has sent an unbind request, but the DLUR rejects the new bind request because it believes that this lfsid is in use. If the host continuously tries to use this lfsid which the DLUR believes is in use, then no new sessions can be established. This problem occurs only when the downstream device does not respond to a bind request. [CSCdj30386]

- An APPN router may display the following “Unanticipated CP_STATUS” message when the contention loser CP-CP session goes down and comes back up without the contention winner session being deactivated:

```
%APPN-6-APPNSENDMSG: Ended DLUR connection with DLUS NETA.SJMVS1
%APPN-7-MSALERT: Alert LU62004 issued with sense code 0x8A00008 by XXXSMPUN
%APPN-6-APPNSENDMSG: Starting DLUR connection with DLUS NETA.SJMVS4
%APPN-7-APPNETERROR: CP_STATUS FSM: Unanticipated CP_STATUS message received
```

Each subsequent broadcast locate received by the router causes the following messages to be displayed and about 1920 bytes of APPN memory to be leaked:

```
%APPN-7-APPNETERROR: MAP_INPUT_SET_TO_ROW: invalid input value=0x80200080
%APPN-7-APPNETERROR: State Error lcb: 60C05CC0 pcid: DA839C70FB1548CB row: 22
col: 0
```

This problem occurs when two links are active to the same node, the CP-CP sessions are split between these two links, and the link with contention loser is stopped.

The APPN subsystem should be stopped and restarted to clear this problem. If the CP-CP sessions are between the router and the host, terminating either CP-CP session on the host will also clear this problem. [CSCdj33718]

- Intermittent failures may occur when trying to link to bridges over the DLSw remote peers when running LNM over DLSw. The workaround is to reload the router that is directly attached to the LNM device. [CSCdj34112]
- When an LLC2 connection is configured to work over ATM LANE for DLSw, the connection succeeds until a retransmission is required, at which time it fails. [CSCdj34873]
- If the DLUR router received fixed session-level pacing values on the primary stage, it may modify these pacing values before forwarding the bind to the secondary stage. [CSCdj36195]
- An APPN DLUR router may reload with SegV exception in ndr_sndtp_encap_mu in a timing window where the DLUR supported device disconnects before a request_actpu is sent to the DLUS for that device. [CSCdj37172]
- The problem would appear to be when an LU-node-specific node attempts to start a session with a set of invalid Bind parameters. This results in a locate-find (with the bind in the CDINIT) being sent through the Cisco APPN network to the end VTAM CP, which rejects the locate-find with a 0835003A sense and sends it back with a control vector CV35 of minimum length 8 bytes to the originator via the Cisco APPN NN. The APPN NN then rejects the frame with a 08953500 sense and drops the CP-CP session between the Cisco and VTAM CP. [CSCdj37479]
- APPN enforces the maximum size of a CV10 (product set identifier) on XID to not exceed 60 bytes. Some products include a CV10 that is larger than the 60 byte value. These products will fail XID negotiation with APPN. [CSCdj40144]
- In the event that APPN/DLUR has processed and sent a bind request to a downstream device, and that device has not responded to the bind, issuing a **vary inact** command on the host for the LU name that the bind is destined for will not completely clean up the session as it should. [CSCdj40147]
- When a connection is attempted over a port defined with the len-connection operand, APPN can lose 128 bytes of memory for each connection attempt. [CSCdj40190]
- Memory leaks occur when APPN TPsnd_search is sending locate search requests to adjacent nodes when a link failure occurs. [CSCdj40915]
- When RSRB with TCP encapsulation is configured and remwait/dead peers exist, an explorer packet may continuously try to open the remwait/dead peer. After several tries, the router may crash with memory corruption.
A workaround is to remove any remwait/dead peer statements. [CSCdj42427]
- A Cisco 7206 router running Cisco IOS 11.1(13.5)CA restarts with the following message:
System was restarted by error - a Software forced crash, PC 0x60278214
The protocols running on the router are RSRB, DLSw, DECnet, and IPX. [CSCdj42431]
- A Cisco 3640 router crashes when a UI LLC frame is received on the Token Ring interface. [CSCdj43755]
- An APPN router may crash with a bus error if a race condition is experienced during cleanup processing. The stacktrace shows the crash occurred in Qfind_front while executing a psp00 function. An example stacktrace for this problem is shown below.
System was restarted by bus error at PC 0x3784864, address 0xF0110208 PC
0x3784864[_Qfind_front(0x3040a04+0x743e44)+0x1c] RA:
0x36C1F2E[_queue_find_front(0x3040a04+0x68151c)+0xe] RA:
0x36CC554[_psbfrm(0x3040a04+0x68bb30)+0x20] RA:
0x36CDAF6[_psp00(0x3040a04+0x68cfd4)+0x11e] RA:
0x314BD78[_process_hari_kari(0x3040a04+0x10b374)+0x0] [CSCdj44198]

- APPN crashed when it received a CV35 without the Termination Procedure Origin Name (TPON) field. [CSCdj44661]
- DLUR bind processing may cause stack corruption, resulting in a reload with PC 0x0. This problem is caused by attempting to parse the user data subfields beyond the location where the subfields exist. The reload will only occur if the byte two bytes beyond the end of the user data area is 0x3 or 0x4. This is a very rare occurrence. [CSCdj45676]
- In large APPN network environments over 200 NNs, numerous broadcast searches could happen during initial start up or intermediate links recovery. The memory usage surge may bring down the entire network. [CSCdj45705]
- The message “%APPN-0-APPNEMERG: Mfreeing bad storage, addr = 60BB7188, header = 60BB6B20, 00000218 -Process= “ndrmain”, ipl= 0, pid= 62” may be issued when a DLUR served PU disconnects. [CSCdj46783]

Interfaces and Bridging

- When connecting a Canary Fast Ethernet transceiver to the MII connector on VIP port adapters, reload the microcode so that the port will function properly. [CSCdi64606]
- The auto-enable feature for packet-by-packet Frame Relay compression is removed and this form of compression is allowed to be manually enabled. [CSCdi85183]
- Bridging from a serial interface to Fast Ethernet interface with ISL encapsulation fails because the serial input queue is not cleaned up. [CSCdj01443]
- Sending a break character to the asynchronous interface while there is data coming down and through the asynchronous interface will cause the asynchronous interface to hang. This problem effects all platforms with asynchronous interfaces. There is no workaround for this problem except having a fix in Cirrus microcode version A5. [CSCdj02282]
- In bridging, a router fails to translate from a IEEE 802.10 FDDI packet to a native Ethernet packet. The failure is that router fails to de-encapsulate “SDE information” before sending the packet out on an Ethernet interface.

As a result, the first ICMP ARP broadcast message fails to reach the destination when ping is used. [CSCdj21365]

- An SNMP agent was returning erroneous values. Under some conditions, the ifInUcastPkts counter was observed returning decreasing values, which is incorrect. [CSCdj23790]
- Setting **encapsulation fddi** without bridging enabled on VIP2/FDDI and FIP in RSP causes the interface to bridge transparently.

The **encapsulation fddi** command should only be used with bridging enabled.

A workaround is to use the **no bridge-group 1** command to disable bridging. [CSCdj24479]

- PPP compression and custom queuing are incompatible features and may cause the router to crash. To work around this problem, turn off all fancy queuing. [CSCdj25503]
- Under certain circumstances, the Fast Ethernet interface could stop passing traffic. Resetting the interface in this condition with the **shut** and **no shut** commands could cause the router to reload. [CSCdj33727]
- On an experimental image corresponding to Release 11.1(12.5)CA, when using a point-to-point subinterface on the ATM interface of the CES card of the Cisco 7200, the IP connectivity will break if transparent bridging is configured on the subinterface via the **bridge-group** command. IP connectivity can be restored by unconfiguring transparent bridging.

The workaround is to use RFC1483 over a PVC using a multipoint subinterface with a map list defined. Using the **map-group** command on a multipoint subinterface does not exhibit breakage.

To determine if you have this bug, enter the **show arp** command. If there is an entry for the other end of the PVC showing “incomplete” for the MAC address, then you are affected by this caveat. [CSCdj34217]

- NFS transmission problems and FDDI corruption occur after installing Releases 10.3(9), 11.1(9) or 11.2(1). [CSCdj38715]

IP Routing Protocols

- A router crashes after receiving multicast packets with the illegal source address 0.0.0.0. The workaround is to configure the access list to filter out packets with a source IP address of 0.0.0.0. [CSCdj32995]
- The old incoming interface is not populated in the OIF during RPF transitions. [CSCdj34457]
- When the OSPF interface command **ip ospf authentication-key** *key* is configured with key length longer than 19 characters, including any trailing space, then the OSPF internal data will be corrupted. The **write terminal** command could reload the router.

The workaround is not to enter a key longer than 19 characters, either encrypted or not.

The same problem happens with the **ip ospf message-digest** *key-id* **md5** *key* command. In this case, the key length should not be longer than 36 characters. [CSCdj37583]

- In some instances, a configured bgp router-id is not used after the router reloads. Instead, the router uses the highest IP interface address as its router ID, until the **clear ip bgp** command is performed.

A workaround is to configure the loopback interface, whose address is greater than any other address on the router. [CSCdj37962]

LAT

- The following message may be erroneously displayed:

```
%LAT-3-BADDATA: Tty124, Data pointer does not correspond to current packet
```

When many LAT sessions are active, and a received data slot starts in the last 14 bytes of a full Ethernet frame, data for that slot is discarded. [CSCdi82343]

Novell IPX, XNS, and Apollo Domain

- A problem may exist where static routes age in the table when they should not age. [CSCdj45340]
- Running IPX EIGRP with maximum path set greater than one, the router may not remove the SAP after the interface is down if it is learned via more than one path. [CSCdj45364]

TCP/IP Host-Mode Services

- In Cisco IOS Release 11.1(10), forwarding UDP broadcast packets to the helpred addresses seems to be broken. Cisco IOS Release 11.1(4) is not affected. [CSCdj13548]

VINES

- A router may unexpectedly reload when VINES SRTP routing is configured. The workaround is to remove the **vines srtp-enabled** command. [CSCdj37888]

Wide-Area Networking

- CMNS connections may suffer spurious X.25 resets under traffic load. [CSCdi40875]
- PPP IPCP negotiation will be changed after Cisco IOS Release 11.0(11).

In Cisco IOS Release 11.0(11) the software accepts the remote peer's "Her" proposed address regardless, and the "Her" address is subsequently added to the IP routing table as a host route.

With Cisco IOS releases later than 11.0(11) the software will check the "Her" address against the corresponding dialer map and if the address is different than the IP address detailed within the dialer map, a NAK will be sent and the dialer map IP address will be added as a host route in the IP routing table.

It is possible to revert to the previous operation using the hidden interface command **ppp ipcp accept-address**. When enabled the peer IP address will be accepted but is still subject to AAA verification, it will have precedence over any local address pool however. [CSCdj04128]

- On a Cisco 4500 running Cisco IOS Release 11.0(11) and RSRB, there may be a crash in the "llc2_timer" routine causing a system reload. [CSCdj13175]
- ATCP negotiation fails when an ARAP 3.0f1c4 client attempts to connect to a Cisco IOS access server. This was found during Beta testing of the ARAP 3.0 software. The actual ARAP protocol works fine: It is only ATCP that is failing. [CSCdj31323]
- A router may crash in the fr_lmi_tx_process. There is no workaround other than to disable LMI (no keepalive). [CSCdj36899]

Caveats for Release 11.1(1) through 11.1(13)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(13). These caveats also apply to Releases 11.1(1) through 11.1(12) (unless otherwise noted).

For more caveats of Release 11.1(13) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections "Cisco Connection Online" and "Documentation CD-ROM" at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(14).

AppleTalk

- A special character in an AppleTalk zone name does not work correctly when using the **appletalk static** command. If the special character is between :80 and :ff, it will be changed in running-config. This change only occurs when using the **appletalk static** command. [CSCdj25241]

Basic System Services

- When using AAA, it is not possible to duplicate the precise sequence of prompts that dialup users have become accustomed to from using XTACACS. This makes moving from XTACACS to AAA problematic for users who do not wish to rewrite their dial-in scripts. [CSCdi42842]
- Connected routes stay in the routing table when a card is disabled and in an analyzed wedged state. There is no workaround. [CSCdj08355]
- This problem is seen only for asynchronous interfaces and may be caused by the following situations:
 - The configuration is read after a reload.
 - Asynchronous interfaces are configured via Group-Async commands, but **snmp-server** is not yet running.

To work around this problem, do one of the following:

- For scenario 1 above, reread the configuration, or go to the Group-Async interface command line and configure **no snmp trap link-status** again.
- For scenario 2, start **snmp-server** before configuring the **no snmp trap link-status** command. [CSCdj13769]

- The error “System restarted by bus error at invalid address” is caused by intermittent Telnet sessions on a Cisco AS500 platform running Cisco IOS Release 11.1(10)AA.

This problem occurs because of a race condition when doing DNS name query and DNS name cache is removed in the middle of the process.

There is no workaround on the router side. On the DNS server side, configuring DNS TTL to be one minute or longer may work around this problem. However, this workaround may not be acceptable for some applications. [CSCdj16824]

- During a boot Flash format, systems with earlier release images will not recognize Intel boot Flash SIMMs 28F004S5 (device code A7), 28F008S5 (device code A6), and 28F016S5 (device code AA).

To run type A7, A6, or AA boot Flash devices and use images prior to this bug fix, format boot Flash with an image containing this bug fix. Then load an older image onto the newly formatted boot Flash SIMM. [CSCdj20681]

- An ARAP session attempt causes NAS to reload when running AAA accounting with ARAP. [CSCdj21751]

IBM Connectivity

- QLLC/RSRB forwards IEEE XID frames like other XID frames to VTAM. Some devices use IEEE XID frames (format 8, type 1) instead of test frames. [CSCdi86682]
- When an LNM queries the router with a report station address, the router answers correctly with a report station address. However, 0.001 seconds later, the router sends a second report station address to the LNM with all zeros in the frame. This causes the LNM to work incorrectly. [CSCdj04559]
- A memory corruption causes the router to crash when a NetBIOS datagram explorer is received by a Cisco 7200 series router. This problem can occur for any non-explorer frame also. There is no workaround for this problem. [CSCdj04944]
- Issuing the **show lnm station** command may cause the routers to reload, especially when the stations are getting in and out of the ring. [CSCdj09905]

- When SRB and transparent bridging are both configured on two interfaces, SR frames with an Ethernet type of 0x600 or 0x800 will not be forwarded and do not show up as source errors. This problem first appeared in Cisco IOS Release 11.1(12). [CSCdj18483]
- Continuously issuing the **appn ping** command causes the router to hang indefinitely. [CSCdj19525]
- When using RSRB local acknowledgment with priority queuing on a Cisco 7200 platform running Cisco IOS Release 11.1, a severe performance degradation has been seen. The root cause is an alignment error in the priority module. [CSCdj22593]
- When RSRB with TCP encapsulation is configured and there are dead peers, an explorer packet may continuously try to open the dead peer. After several tries, the router may crash with memory corruption. The workaround is to remove any dead peer statements. [CSCdj24658]
- During certain race conditions, an APPN router may crash with the following stack trace:

```
PC= 0x606079a4 [psbmfsm(0x60607930)+0x74], 32 bytes
```

```
PC= 0x606094d0 [psp00(0x60609380)+0x150], 320 bytes [CSCdj25484]
```

- ReqActPU continuously fails with sense 8170001. This problem may occur when there are two parallel links to the same adjacent CP and the links are frequently stopped and started. The reason this may occur is because someone could try to activate a route over an inactive link. [CSCdj26027]
- When promiscuous or peer-on-demand peers are used and there are more than 100 circuits connected, a memory corruption crash may result when the promiscuous or peer-on-demand peers disconnect. The corruption occurs when circuit cleanup is delayed due to end station delay, LAN network delay, or high router CPU usage. [CSCdj26284]
- When a Cisco DLSw router starts a circuit (by sending CUR_cs) to another vendor's DLSw implementation, the Cisco DLSw incorrectly sets the largest frame (lf) bits in the CUR_cs header. [CSCdj26402]
- An APPN router may crash with the following stack trace:

```
606CD174 [Qfind_front+0x24]
```

```
606C7D80 [timer_process+0x300]
```

```
606C8070 [csweotsk+0x1d0]
```

A router may experience this problem after displaying several messages when the output buffer was full. If the crash was related to displaying "incomplete definition in configuration" warnings, the workaround is to remove these incomplete definitions. [CSCdj26701]

- The timer that controls the daily cleanup of APPN topology and the 5-day rebroadcast of topology resources owned by this APPN node can fail after 45 days. At this time, other nodes where the timer is still functioning properly may age out the topology of the node with the failed timer after 15 days. Thus, after a total of 60 days, APPN routing failures and failed CP-CP sessions may result between APPN network nodes.

Because other network events (link outages, and so forth) can trigger a node to send a TDU, this problem will not necessarily appear exactly after a 60-day uptime -- it may occur much later or not at all. However, any APPN router running in the network for over 60 days is at risk for seeing this problem.

Stopping and restarting APPN will work around this problem until the next timer wrap, which can be up to 45 days, but may be less depending on the current value of the timer. Reloading the router will reset the timer and avoid the problem for an additional 60 days. [CSCdj29014]

- A router configured for RSRB may crash with a watchdog timeout during low memory conditions and/or continual peer state changes. [CSCdj30381]

- Sometimes the linkstations may get stuck in a XIDSENT state when an APPN linkstation fails and recovery is attempted.

Caveat CSCdi77040 provides a fix for this problem in the system side. This caveat provides the corresponding fix for APPN. [CSCdj30552]

- When using APPN/DLUR with the **prefer-active-dlus** configuration command specified on the APPN control point, DLUR may not properly connect to a backup DLUS in cases where the primary DLUS is available in the network but has the served PUs varied inactive. [CSCdj31261]
- When using the **len-connection** configuration command on the APPN port and there are at least 30 XID3 devices connecting in through that port, a rare sequence of events of devices connecting and reconnecting can cause a reload. [CSCdj31264]
- Any device connecting to APPN/DLUR that does not carry a cv0E with a CPname specified on XID (any PU2.0 and some older PU2.1 implementations) causes APPN to fail to release 536 bytes of memory each time the device disconnects and reconnects. Any device connecting on a port with LEN-connection defined also exhibits this behavior.

When memory is exhausted, the APPN subsystem may stop or the router may reload. [CSCdj33429]

Interfaces and Bridging

- A Cisco 4700 router crashed in ip_input because of a bad packet on the IP input queue. [CSCdi46479]
- In some cases, a Cisco 4000 router with Token Ring NIM and running xx-p-mz image displays the “%SYS-3-SUPNONE: Registry 6 doesn’t exist” error message repeatedly on the console after bootup. [CSCdi70834]
- On Cisco 7500 RSP platforms, FSIP serial interfaces may display the following panic messages on the RSP console:

```
%RSP-3-IP_PANIC: Panic: Serial12/2 800003E8 00000120 0000800D 0000534C
%DBUS-3-CXBUSERR: Slot 12, CBus Error
%RSP-3-RESTART: cbus complex
```

If the string “0000800D” is included in the panic message, the problem is related to this bug. The workaround is to load a new image that contains the fix for this bug. [CSCdi78086]

- On Cisco 2500 series routers, the Token Ring interfaces run Fastened Plus microcode version 1.28, even though the latest microcode version available is 1.61. [CSCdi93243]
- When using Token Ring Adapter in a Cisco 7200 series router, a very large number of receive errors on the Token Ring interface may cause the router to reload. [CSCdj16191]
- Routers running RSRB from a Cisco 7200 or 7500 series router with a PA-4R Token Ring insert an invalid Token Ring frame check sequence (FCS) in frames sent to remote peers. The invalid FCS will cause data frames to be dropped on some remote peer routers. Affected remote peer routers are Cisco 2500 series, Cisco 4000 series, Cisco 4500 series, and Cisco 4700 series routers running Cisco IOS Release 10.2 or earlier. Other router models and routers running Cisco IOS Release 10.3 or later are not affected. [CSCdj21539]
- When bridging IP and routing AppleTalk, assigning the bridge-group to the LEX interface causes AARP entries to disappear and become no longer resolved. [CSCdj22825]
- When PIM is configured on a Fast Ethernet PA on a Cisco 7200 series router, the interface enters promiscuous mode and receives all packets on the LAN, possibly interrupting unicast traffic between other stations on the LAN. [CSCdj28007]

IP Routing Protocols

- Under unusual circumstances, EIGRP may reinitialize multiple peers when a stuck-in-active condition occurs, instead of just the peer through which the route was stuck. [CSCdi83660]
- In bgp/ospf/rip, a crash can occur when using an extended access list with the command **default-originate route-map** or **default-information originate route-map**.
By design, an extended access list can not be used as a condition to originate a default.
A workaround (the right approach) is to use a standard access list in default origination. [CSCdj02583]
- Under certain circumstances, if the Cisco router received a route with a lower rip2 metric, the router may go to hold down with infinite metric. [CSCdj15295]
- A router may crash after the fifth EIGRP process is configured. CSCdi36031 is a related caveat. [CSCdj17508]
- Under certain conditions, the EIGRP **variance** command may not remove routes that have a higher next hop metric. To resolve the problem, issue the **clear ip route** command. [CSCdj19634]
- When a router is no longer the DR, it should not keep a sparse-mode interface in its outgoing interface list, even if a connected group member exists on that LAN. The sparse-mode interface should expire unless it is refreshed by a join message from a downstream router. [CSCdj25373]
- Turning on IP routing after assigning IP addresses to the interfaces does not take effect.
The workaround is to turn on IP routing and then assign the IP addresses to the interfaces. [CSCdj26052]
- IP cache is not being invalidated for destinations which use the default routes even after the next hop is down. A workaround is to enter the **clear ip cache** command. [CSCdj26446]
- Major net summarization is incorrectly done if you have two equal cost direct connect interfaces. The workaround is to issue the **clear ip route *** command. [CSCdj30971]
- Dense mode interfaces are not always populated in the outgoing interfaces of a multicast route. This was introduced by CSCdi25373. [CSCdj32187]

ISO CLNS

- CLNS fast switching is not working between PVCs defined on ATM subinterfaces. [CSCdj23817]

LAT

- When performing protocol translation from X.25 to LAT, spurious memory accesses may be seen in console messages as well as in the output from the **show alignment EXEC** command. [CSCdj18470]

Novell IPX, XNS, and Apollo Domain

- If Cisco IOS Release 11.1(10) is running with IPX NLSP, IPX EIGRP, and IPX RIP, and IPX EIGRP is redistributed into NLSP and vice versa, the router may reload when receiving certain NLSP updates and redistributing them into IPX EIGRP. [CSCdj11870]

- IPX fast switching might fail over a PRI interface, resulting in IPX client connections not being established over the PRI even though the IPX servers are visible. The workaround is to configure **no ipx route-cache** on the PRI interface. [CSCdj29133]
- XNS does not learn the new non-canonical format of Token Ring MAC addresses. It retains the old canonical format address for its node address, causing routing failure. The workaround is to disable and reenables XNS network on all the Token Ring interfaces. This affects only RSP platforms and when you upgrade an XNS configured router from a version that has the caveat CSCdi48110 to a version that has this caveat fixed. [CSCdj29916]

TCP/IP Host-Mode Services

- An interface may become wedged with input queue 76/75. This is caused by both syslog and SNMP traps.
The workaround is to disable both syslog and SNMP traps. The commands to do this are **no snmp-server host ip-address** and **no logging ip-address**. [CSCdj27567]
- New TCP connections may become stuck in SYNSENT state when router is low on memory. [CSCdj30008]

VINES

- Issuing the **write memory** command may cause the system to reload while writing the VINES access list to memory. Issuing the **write terminal** or **show vines access** commands may also halt the system. The workaround is to delete the configuration file and reconfigure the system. [CSCdi49737]

Wide-Area Networking

- A router configured for both inbound and outbound asynchronous dialing using legacy DDR fails to install dynamic dialer maps for the inbound asynchronous PPP peers when the remote peer is authenticated in character mode, then launched into packet mode from the router's EXEC mode.
A workaround for this is to use **ppp authentication** and **autoselect ppp** on the lines. [CSCdj14047]
- Packets that are exactly the size of the MAC encapsulation size are not bridged. This means that TEST and XID frames will not be bridged. Instead, they are passed up to the process level, which responds to them. [CSCdj14748]
- Under a high CPU load, it may be possible for the number of active calls and the number of available B channels displayed by the **show isdn status** command to be incorrect. Duplicate caveats are CSCdj23944, CSCdj27419, CSCdj15811, CSCdi82010 and CSCdj28147. [CSCdj18895]
- A memory allocation error occurs after a large number of modem calls are placed to an AS5200 configured for PRI ISDN. After the AS5200 starts to generate a number of these memory allocation error messages, calls cannot be answered.

The following are indicators that may be used to determine if the AS5200 is encountering this problem:

- When the AS5200 runs out of memory, MALLOC Failure messages similar to the one shown will be displayed:

```
%SYS-2-MALLOCFAIL: Memory allocation of 1056 bytes failed from 0x2214E776,
pool Processor, alignment 0 -Process= "Net Periodic", ipl= 0, pid= 34
-Traceback= 2214D3E0 2214E542 2214E77E 2214BEC6 2214C12A 22159466 2215E86E
22140BDE 2213B688 2213B6E0
```

- If there is no ISDN process in the output from the **show process** command, and you start to see “%SYS-2-MALLOCFAIL” error messages, then the memory leak was caused by this bug.
- If there are more than 46 entries marked “Active” in the output from the **show isdn history** command, then the memory leak was caused by this bug.

[CSCdj21944]

- A Cisco access server may fail to start PPP mode for dialup connections when the line is configured with the **autoselect ppp** command. This results in the dialup connection getting dropped.

To work around this problem, use the **async mode dedicated** command if no login is required. If a login is required, configure the **no flush-at-activation** command, change the q2 register in the modem database, and configure the **modem autoconfigure type** command. [CSCdj25443]

- Routers running with **x25 routing** enabled on releases after 11.0(14.1), 11.1(10.1) and 11.2(4.4) are susceptible to the router processor pausing indefinitely when malformed connections are made to the X.25-Over-TCP (XOT) port. If this occurs, the router must be reloaded to recover.

The following error message can be seen scrolling on the console if the router is in the above state:

```
%X25-4-VCLOSTSYNC: Interface TCP/PVC, VC 0 TCP connection corrupted
```

This does not seem to occur in a normal XOT switching environment. [CSCdj25846]

- When the primary interface goes down, the secondary interface may not come up if there is a specific backup load configured. This problem does not affect backing up for a subinterface, since the **backup load** command does not apply. [CSCdj26048]
- Some PC based PPP clients are not correctly autoselected into PPP mode by the Cisco Access Servers. This results in numerous drop calls. This problem is usually noticed when an automated dialer is used.

The workaround is to configure the asynchronous interfaces using the **async mode dedicated** command. Sometimes, adding a second or two delay in the automated dialer’s script also fixes the problem. [CSCdj26647]

Caveats for Release 11.1(1) through 11.1(12)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(12). These caveats also apply to Releases 11.1(1) through 11.1(11) (unless otherwise noted).

For more caveats of Release 11.1(12) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(13).

AppleTalk

- ATCP and ARAP code will not work with all-router node addresses. NBP lookup to ATCP/ARAP clients may fail. There is no workaround. [CSCdj02390]
- A router may prevent Macintoshes from coming up because of duplicate provisional addresses. A work around is to issue the **clear appletalk arp** command. [CSCdj16510]

Basic System Services

- If a Cisco Catalyst 3000 on an adjacent network does not have a protocol address configured and it sends CDP updates, the router may be reset when the **show cdp neighbor detail** command is used. [CSCdj15708]
- Distributed access lists with a large number of statements may not behave properly when the RSP reloads. A workaround is to issue the **microcode reload** command. [CSCdj17068]
- Control characters in **chat-script** commands that are specified using backslash-octal representation are not accepted and stored properly. [CSCdj18869]

IBM Connectivity

- During IBM-LNAMAN tests, after LAN manager was shutdown the router crashed when the **show buffer** command was issued. The router then crashed with a bus error. This problem occurred on a Cisco 4000 router running Cisco IOS Release 11.2(5.1)F, image c4000-js-mz. [CSCdj09919]
- NetBIOS sessions may not come up in a busy system. [CSCdj11152]
- A system may be restarted by an error caused by LAN Manager. The current workaround is to disable LNM. [CSCdj11711]
- A Cisco 7204 router running Cisco IOS Release 11.2(4) feature RSRB, intermittently reloads itself with a software forced crash due to memory corruption. [CSCdj13017]
- Source-routed frames with a destination address of FFFF.FFFF.FFFF will not be forwarded between Token Rings when SRB is configured on the router. Source-routed frames with destination addresses other than an all Fs broadcast address will be forwarded.

In some application environments, certain 3270 emulators will not direct a test poll to a specific media access control address and will use an all Fs address to create the frame. It is this all Fs frame in an SRB configuration that will not be forwarded by the router. This configuration impacts workstations that are attempting to connect to host devices. The broadcast frame will never leave the local ring.

Most emulators will use the destination media access control address of the host device to create a frame containing the test poll. With some proprietary implementations, the MAC address of the host device does not have to be known by the end device. [CSCdj13563]

- When running Cisco IOS Release 11.1(11) with BSTUN configured, the router may reload under certain conditions. This problem may be minimized by configuring HOSTTIMEOUT to a large value. However, this will have a significant impact in detecting device outages. [CSCdj16888]
- Some circuits may connect using smaller, non-optimal maximum frame sizes when Cisco DLSw is used with other vendors' DLSw implementations. In addition, some circuits may not connect at all. [CSCdj17372]
- Cisco 2522 routers running Cisco IOS Release 11.0(11) may have problems with the SDLC state machine. When a large amount of data is input into the router from a PU (for example, during a file transfer), the router may poll the next PU without receiving a poll final in a frame and without T1 expiring. The router may also expect data from the PU, even though it did not poll the PU.

A workaround is to ensure there are no unnecessary PUs configured on a line that is continually sending SNRMs. [CSCdj17630]

- A Cisco 4500 may crash if it has source-bridge local-route configured. [CSCdj20420]
- Buffers classified as linktype IBMNM may leak in the LNM process. A workaround is to disable the LNM process. [CSCdj20441]
- The router is unable to link with LAN Network Manager. [CSCdj20748]
- When a directory cache entry exists for a resource and a broadcast search arrives for that same resource name, the intermediate node broadcast processing will delete the valid cache entry that previously existed, resulting in excessive locate broadcast traffic. [CSCdj21343]
- Using the **dls w ring-list** or **dls w port-list** configuration commands can cause a SegV exception when executing the **show dls w reachability** command. [CSCdj21894]
- The DLUR router may get into a tight loop continuously retrying to start the DLUR/BLUS pipe to the same DLUS without waiting the specified retry time. This problem could cause the router to crash, or pipe retry messages to be displayed continuously (instead of waiting the specified retry time), or just high CPU utilization. [CSCdj22330]
- When establishing a DLSw session, the circuit priority field in the SSP header of the CUR_cs, ICR_cs, and/or REACH_ACK SSP frames may be set to a reserved value (5, 6, or 7). While this value will not cause problems when sent to a Cisco router peer, it may cause interoperability problems when peering to another vendor's equipment. This problem may manifest itself as an inability to start the circuit. [CSCdj22482]
- When the first attempt to link a Cisco router with the LAN Network Manager fails, it is not possible to link this bridge again because of a hanging LLC2 session in status ADM. To clear this session, reload the router. [CSCdj23142]
- With APPN/DLUR, caveat CSCdj18360 caused a regression in APPN images, which creates thrashing topology updates (topology war) for any topology with more than one CP-CP session. Cisco recommends that an image containing CSCdj18360 should not be used in an APPN network without also having this fix applied. All APPN images containing CSCdj18360 and not this fix have been deferred as production images. [CSCdj23165]
- Under certain circumstances, the router will fail to create a dynamic link station. The workaround is to restart APPN on the router. This is caused by a small buffer leak that occurs for each actpu processed by DLUR. After some time, enough buffers may be lost as to cause session failures and dynamic link station failures due to insufficient buffers. [CSCdj23782]

- The low entry networking (LEN)-connection mode of operation on an APPN port is designed to allow LEN-level connectivity between a DLUR and its downstream devices. Independent session activation (LU6.2) through ports with LEN-connection fails with the message “no route for session.” This problem does not affect dependent session activation (LU 0,1,2 etc.). [CSCdj24777]

Interfaces and Bridging

- In Cisco 7500 series routers, the following error message might be displayed while booting the system image from TFTP or Flash memory:

```
%CBUS-3-CMDTIMEOUT: Cmd timed out, CCB 0x5800FF50, slot x, cmd code 0
```

A possible workaround is to issue a **microcode reload** command or load a new system image that has the fix for this bug. [CSCdj00013]

- The bridge ID may choose a Cisco random address even though the Ethernet interface has a MAC address. It occurs mostly on the first Ethernet interface. [CSCdj13302]
- The VIP PA-4R was bridging frames that were aborted by the sender. The frame is now dropped when the abort is detected. [CSCdj13409]
- An ARP/RARP packet is dropped on a Cisco 7000 ISL subinterface. [CSCdj17002]
- IEEE spanning tree BPDUs are not recognized by a VIP2 with a NP-4R running Cisco IOS Release 11.1(10)CA or 11.1(11a). [CSCdj18696]
- The FDDI PA versions that support CAM are properly recognized before attempting CAM operations. CSCdi51248 must also include CSCdj23259 to avoid problems with old FDDI hardware. [CSCdj23259]

IP Routing Protocols

- Cisco 4500 routers may not correctly policy-route when serial subinterfaces are configured and the fast-switching cache is populated. A workaround is to disable fast switching on all interfaces. [CSCdi86063]
- A router may reload if it receives an ARP request frame from a Token Ring interface and the frame has been incorrectly formatted as a Frame Relay ARP. ARP request frames that are correctly formatted for IEEE LAN media will not cause this problem. The only workaround is to remove the station sending the illegal frame from the network. [CSCdj05170]
- An ICMP redirect will not be sent if there is a destination IP address entry in the fast cache. An ICMP redirect is only sent when the packet is process-switched. [CSCdj16708]

LAT

- Illegal LAT STOP slots may be sent if a line is disconnected immediately after initiating a LAT connection. The illegal slots may cause the LAT virtual circuit to be disconnected, affecting all connections to the host. This problem is more likely to occur when using protocol translation. [CSCdj09876]

Novell IPX, XNS, and Apollo Domain

- IPX cache corruption may occur when two Fast Ethernets in a VIP carrier (one configured for ISL) connect to a single server with dual NICs (different external numbers, same frame type) and IPX max-paths is set to 2. A workaround is to disable fast switching for IPX. [CSCdj17470]

TCP/IP Host-Mode Services

- DLWS incorrectly connects to a down interface on the peer. [CSCdj00448]

Wide-Area Networking

- TCP header compression does not work over Point-to-Point Protocol (PPP), ISDN, and asynchronous dialer interfaces. To work around this problem, turn off TCP/IP header compression. Note that non-dialer asynchronous interfaces used for dial-in PPP access are not affected. [CSCdi19199]
- After a data-direct VCC is created, the ATM-SIG input holding value increases. After it is cleared by a timeout, the ATM-SIG continues to hold onto memory, causing a memory leak. [CSCdj02779]
- When the **shutdown** and **no shutdown** commands are issued on a BRI interface while the primary Frame Relay interface is down, the interface comes back in standby mode. This problem also occurs when the router is reloaded with the BRI in a standby mode and the primary is down. [CSCdj16441]
- Occasionally, an RSP router running Cisco IOS Release 11.1 would crash with invalid pointers. This problem has not been identified on other platforms or other software releases. [CSCdj17033]

- The following console messages may be logged:

```
%AIP-3-AIPREJCMD: Interface ATM3/0, AIP driver rejected Teardown VC command
(error code 0x8000)
```

The workaround is to reload the system. [CSCdj20667]

- Upon bootup, OIR, microcode reload, and cbus complex restarts, the router shows CCBTIMEOUT error messages on VIPs that result in a disabled wedged status.

A possible workaround is to reload the microcode. [CSCdj21639]

- VIP2 packet bus parity errors are not reported. [CSCdj23431]

Caveats for Release 11.1(1) through 11.1(11)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(11). These caveats also apply to Releases 11.1(1) through 11.1(10) (unless otherwise noted).

For more caveats of Release 11.1(11) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(12).

AppleTalk

- The ability to route AppleTalk with Enhanced IGRP on the Cisco 1005 was present in Cisco IOS releases 10.3 and 11.0 but is not in Cisco IOS Release 11.1. [CSCdj09990]
- Memory leak may occur when an ARAP user fails to connect due to initialization failure. [CSCdj14393]

Basic System Services

- When the **ntp broadcast client** command is enabled, packet buffer leaks may occur unexpectedly. Disable the command if this condition occurs. [CSCdj03162]
- On RSP systems, when maximum-size MTU packets are received by serial interface processors (including the FSIP, HIP, MIP, POSIP, and serial port adapters on VIPs that forward data to the RSP to be routed), up to 8 bytes of data might be written into the next datagram’s packet memory. This could result in anomalous system behavior, including software-caused system crashes and dropped datagrams. This problem is only applicable to RSP systems with serial interfaces. [CSCdj08573]
- Customers who have an FDDI interface installed on their router may see some bad input packets with other interfaces that are using the same pool of MEMD buffers. There will be up to one input failure per SMT frame input over each FDDI interface.

A workaround is to enter the command **test rsp cache memd-fastswitchuncache** each time the router is rebooted. [CSCdj10028]
- A reverse Telnet connection to an asynchronous line via a raw TCP port (40xx) may result in a 30-second pause before data is passed. Pressing Return will bypass the pause, as will using a Telnet protocol port number (20xx). [CSCdj11084]
- Under certain circumstances, alignment warnings may appear when fast switching with custom or priority queuing is enabled. These warnings signal that extra CPU cycles are necessary to process the packet. Despite the warnings, the packet is still switched correctly. [CSCdj12269]
- Even if the **rlogin** command has its privilege altered to level 0, it will still be treated as though its privilege level is 1 by AAA command authorization. [CSCdj14206]

IBM Connectivity

- Source-route bridging over FDDI might not pass all frames following the spanning or all-routes explorers. This problem was introduced in Release 11.2(9). [CSCdi92160]
- The DLUR router may tear the downstream link down when it receives a DACTPU “not final use” for the downstream PU. [CSCdi92973]

- When both BNN and BAN sessions are configured on the same SLDC interface, all sessions will come down when the user deconfigures the BAN sessions, disrupting existing BNN sessions. [CSCdj00497]
- If end stations are continually activating and deactivating, a router configured for DSPU may crash with the error “Software forced crash, PC 0x31598BC.” [CSCdj02005]
- When the first connection to an SDLC-attached OS/2 system in a FRAS BNN environment fails, a successful connection can be made only by issuing the **shutdown** and **no shutdown** commands on the router’s SDLC interface. [CSCdj04321]
- IPX SAP packets may be ignored when received from a VIP/4R token ring interface if the SAP packets have a destination MAC address of “all stations broadcast” and a Routing Information Field (RIF). [CSCdj04552]
- The **show appn dlur-lu** and **show appn dlur-pu** commands can fail to filter out the correct LU the user wants to display. No matches will be found even though the filter should find a match. [CSCdj07924]
- When running APPN/DLUR, if the downstream device has a different network ID from the network ID specified on the APPN CP name, the binds for the dependent sessions will fail. [CSCdj08190]
- In some circumstances when DLSw is required to verify the NetBIOS reachability cache entry, there may be a 1-second delay before a NetBIOS FIND_NAME is forwarded to the LAN interface. [CSCdj09865]
- A buffer leak causes a crash when NSP is used over DLUR. [CSCdj10387]
- The DLUR router may send a corrupt APPC frame to a DLUS if a timing window is hit when accessing multiple DLUSs. This problem may occur if there are primary and backup DLUSs configured and at least one inactive PU that cannot get into the primary DLUS while other PUs are active with the primary DLUS.

This problem may cause VTAM to refuse to activate subsequent DLUR/DLUS pipes for all DLUR NNs. “/d net, dlurs” shows the DLUS conwinner state as reset and the conloser state as active.

To prevent the DLUR router from sending this corrupt frame, reconfigure the DLUR routers without coding a backup DLUS. [CSCdj10485]
- Running DLSw and RSRB in the same box with LAN Manager can cause disruption of LAN Manager on the RSRB connections. [CSCdj11691]
- Running DLSw and RSRB in the same box with LAN Manager can cause LAN Manager disruption on the RSRB connections. [CSCdj11691]
- Any existing sessions/circuits over the backup peer will be brought down immediately after the primary peer is up. This problem occurs even though the backup peer linger timer has been configured for a specific value. [CSCdj13159]
- Using QLLC/DLSw+, QLLC connections are not established when nondefault SAPs are used. [CSCdj14080]
- DLSw searching remote and local behavior was observed in Cisco IOS Release 11.1.11. A workaround is to not allow CUR frames to go from hub router to the peered (remote) router. [CSCdj16711]

Interfaces and Bridging

- OIR removal of a FIP from one slot into another will cause the FDDI to permanently remain in DOWN/DOWN. A reload is needed to bring the FDDI back up. Removing the FIP and putting it back into the same slot works fine. [CSCdi87221]
- Under heavy load conditions, it is possible for the keepalive timer to go off and cause resets on the Token Ring interface. [CSCdi88713]
- A problem occurs when the VIP2 FIFO buffers overflow, causing a data write to SRAM to fail silently. This problem may cause a number of protocol-related failures, including, but not limited to, TCP checksum errors and other possible packet data errors. This problem is not limited to any particular network configuration, traffic load, or other specific circumstances. [CSCdj08722]
- When the 90-compatible OUI is used on a “source-bridge transparent” statement, the command is accepted and translational bridging operates correctly. A display of the configuration shows the OUI option as “90compat” instead of “90-compatible.” If the router is reloaded, an error message is generated pointing to the “c” in “90compat” and the resulting configuration does not have the **source-bridge transparent** command included. If the command with the 90-compatible OUI is configured again, normal operation is restored. [CSCdj09688]
- When a serial interface is configured as half-duplex in a Cisco 4000 series router, and the **shutdown** and **no shutdown** commands are entered for another full duplex serial interface, the router may become non-responsive. To correct this condition, turn the router off and then back on. [CSCdj13056]

IP Routing Protocols

- Systems running OSPF might experience a software-forced crash. There is no known workaround. [CSCdi81510]
- Router restarted by unexpected interrupt at ospf_if_get_def_type_cost. [CSCdj08125]
- In a router with a simplex interface configuration, IP route cache is invalidated on the RECEIVE interface only. The IP route cache should also be invalidated for the TRANSMIT interface. [CSCdj11960]
- A multicast boundary on the incoming interface does not stop the router from giving packets to its local process, although these packets cannot be forwarded out any interface due to this boundary. [CSCdj12030]
- When the **ip nhrp map** command is used on a tunnel interface, it may be incorrectly parsed to add an unnecessary IP mask. The workaround is to specify the mask and reenter the **ip nhrp map** command without masks. This problem exists in Cisco IOS Release 11.1(2.0.1) and later releases. [CSCdj13220]

Novell IPX, XNS, and Apollo Domain

- If IPXWAN is configured and the remote router is configured to allow IPXWAN Client mode, the local router will reset the link upon receiving the IPXWAN Timer Request. IPXWAN debugging will show “IPXWAN: Rcv TIMER_REQ reject Router asking for Client mode.” The workaround is to disable IXPWAN Client mode negotiation on the remote router. [CSCdi93285]
- The **distribute-sap-list** command does not work when used to filter SAPs into an IPX routing protocol instance. A workaround is to filter the SAPs when they get redistributed, using the **distribute-sap-list out** command. [CSCdj15889]

Protocol Translation

- Systems doing VTY to asynchronous protocol translation of SLIP or PPP over X.25 may unexpectedly restart when the incoming connection is closed. This problem was introduced in 11.1(10.4) and 11.2(5.1). [CSCdj15471]

TCP/IP Host-Mode Services

- A TCP packet still in use may accidentally get freed in IP when the packet is going out a Frame Relay interface on which TCP header compression is configured. When this happens, the following messages are logged on the console:

```
Mar 19 08:41:23: %TCP-2-BADREFCNT: Tty0: Bad refcnt for packet 0x608F9C2C during
retransmit, 135.135.100.1:1998 to 135.135.105.1:11000, state 4-Traceback= 601EEB7C
601EEEE4 601F1B68 601F1E4C 6013F140 6013F12C
Mar 19 08:41:50: %X25-4-VCLOSTSYNC: Interface Serial3, VC 82 TCP connection corrupted
Mar 19 08:41:52:TCP0: extra packet reference for pak 0x60A031D8 found:
Mar 19 08:41:52: %TCP-2-BADQUEUE: Multiple entry for packet 60A031D8-Process= "TCP
Driver", ipl= 0, pid= 26-Traceback= 601F3384 601F5408 6023CCB4 6023D214 6013F140
6013F12C
Mar 19 08:41:52: pak: 135.135.100.1:1998, 135.135.1.4:11137, seq 1668710213length 47
Mar 19 08:41:52: TCB: 135.135.100.1:1998, 135.135.1.13:11137, sendnext 1668710220,
state 4[CSCdj06781]
```

- Memory allocated for a new TCP connection will not be freed after receiving an ICMP unreachable message if the new connection has its own listeners for processing of incoming connections. [CSCdj07761]
- Cisco boxes running small numbers of outgoing telnet sessions (that is, being used as terminal servers) will show unexpectedly high CPU utilizations. The high CPU utilization is a result of the way CPU usage is measured, and should not cause much concern. This is a regression introduced in 11.1(10.3) and 11.2(5.1). [CSCdj11528]

Wide-Area Networking

- When using Frame Relay IETF encapsulation, bridging fails for Token Ring-to-serial-to-Token Ring connections. [CSCdi70653]
- When the **x25 suppress-calling** command is configured on a router running ISIS over X.25, ISIS does not find the called address or the SNPA. [CSCdj00315]
- An asynchronous controller may hang and cause four connected modems to go into a hung state. [CSCdj01441]
- An AS5200 may experience hung calls, ISDN data structure memory leaks and may not be able to call out or accept incoming calls. [CSCdj05355]
- Deleting a subinterface causes the main interface and associated subinterfaces to vanish from the configuration. This problem occurs when the main interface uses Frame Relay encapsulation and is a member of a channel group. A workaround is to re-create the main interface by issuing the **interface serial** command. [CSCdj05415]
- For TS014 (Australia, PRI) switch types: When a clear collision occurs between the CE and the network simultaneously transferring a DISCONNECT message specifying the same call, the call is not properly cleared. Neither side sends the RELEASE message to release the call, and hence the call reference and the associated call control block (CCB). [CSCdj06157]

- A router reacts incorrectly to REJ frames. Probably, an REJ frame with the P-bit set is required to send the requested frames. Furthermore, frames seem to be queued and sent twice. [CSCdj08607]
- A router may reload without producing a stack trace or otherwise behave unpredictably on routing an X.25 call that contains 16 bytes of Call User Data. There is no known workaround. [CSCdj10216]
- The number of available B channels is incorrectly incremented by the total number of B channels per interface whenever the controller or the interface is reset. The incorrect number results in a dialer attempting to place calls on resources that are actually in use. [CSCdj11181]
- When the router receives an incorrectly formed LCP NAK frame, a software-forced crash may occur. [CSCdj15209]

Caveats for Release 11.1(1) through 11.1(10)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(10). These caveats also apply to Releases 11.1(1) through 11.1(9) (unless otherwise noted).

For more caveats of Release 11.1(10) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(11).

Basic System Services

- When using RSP code with HIP, TRIP, or FIP interfaces, and when the MTU is larger than 4096 bytes on TRIP or FIP interfaces, or larger than 8192 on HIP interfaces, there is a rare chance that a system error might occur. When this happens, the error message “CYBus error 8” or “CYBus error 10” is displayed. [CSCdi75522]
- After an incoming packet has been encapsulated for a tunnel, an access list check might prevent the packet from being switched. This is caused by the access list checking the new source of the tunnel packet, resulting from the encapsulation, against the interface the packet arrived on. The result is that packets are not switched over a GRE Tunnel. This could occur when access-lists are applied to the input interfaces. A workaround is to disable access-lists on the input interfaces or add the tunnel source address to the access-list. [CSCdi87500]
- A memory leak might be introduced whenever TACACS+ is enabled. The memory is released to the EXEC process as seen on the **show memory** command. This memory leak does not occur in Cisco IOS Release 11.0(9) or earlier releases. [CSCdi89479]
- The **hold-queue <n out** command is not accepted if the output interface is configured for fair queueing. Fair queueing is the default queuing mode for low-speed (less than 2 Mbps) serial interfaces.

The **hold-queue** command is intended to configure the number of output hold queue buffers for FIFO (or FCFS) queueing. It has no meaning in the context of fair queueing. So the (intentional) design was that this command would be ignored when fair queueing was enabled.

When fair queueing has been configured, you may use the **fair-queue** command to control the number of output buffers which may be used by fair queueing. [CSCdj01870]

- Sometimes the router may restart due to a Bus Error. [CSCdj02493]
- Telnet sessions can pause for up to 20 seconds. To interrupt the pause, press any key. [CSCdj06450]

EXEC and Configuration Parser

- The output of the **show tech-support** command displays some potentially sensitive SNMP data, such as the SNMP community strings, SNMP MD5 keys, and SNMP user IDs and passwords. If these data refer to read-write communities or views, they can be used to reconfigure the Cisco IOS software, providing the same level of access to the Cisco IOS software as is available with the enable password. Use caution when sending **show tech-support** command output across insecure channels. For example, remove the community strings, keys, user IDs, and passwords before sending. [CSCdj06881]

IBM Connectivity

- A crash is caused by the SP microcode on Cisco 7000 series routers when a buffer copy by the SP makes the Route Processor (RP) wait too long and take a bus error. [CSCdi77785]
- When source-route bridging is enabled on a Cisco 7500 series router in a Token Ring environment, if the router receives a packet that is to be routed but that contains a RIF, the router misclassifies the packet, treating it as a source-route bridge packet, which causes it to be discarded. This may cause intermittent failures of routed protocol sessions. There is no known workaround. [CSCdi87321]
- A DLUR router may start failing to establish new LU-LU sessions after hitting a race condition during session activation and deactivation. Messages similar to the following may be displayed on the router console when attempting to start new sessions. APPN must be stopped and restarted to clear the problem.

```
IPS ID: 1400 QUEUE: 2 ORIGIN: xxxpcs00 MUTYPE: C5
%APPN-0-APPNEMERG: Assertion failed in ../scm/xxximndr.c at line 158
-Process= "xxxims00", ipl= 0, pid= 58
-Traceback= 606C3488 606879EC 606818C8 606810E4 6067AF90 6019AB08 6019AAF4
```

[CSCdi90117]

- When running DLSw+/LLC2 over FDDI, when an REJ frame is received from an FDDI end station, the router sends a corrupted retransmitted I-frame. The last byte of the SMAC gets replaced by the DMAC value. [CSCdi91063]
- When an end station caches RIFs that it learns from broadcasts or when there are duplicate MAC addresses on each side of the DLSw cloud, DLSw will local switch circuits between two local SRB capable interfaces. This degrades SRB performance. [CSCdi91204]
- When a VTAM switched major node PU is deactivated while running NSP (with VDLC port) via DLSW, the router NSP connection does not come up again. To get the connection to come up, you must de-configure and re-configure the NSP on the router. [CSCdi91310]
- A router configured for DSPU may crash with the error “Software forced crash, PC 0x31598BC” if end stations are continually activating and deactivating. [CSCdi91368]
- The LanSuppManager process may leak memory if receiving UI-frames destined to SAP 0xF4 and sourced by another SAP. [CSCdi91571]
- The router might crash if you enter the **debug source error**, **debug llc2**, or **debug local** command. [CSCdi92503]

- When running DLSw+ local switching from SDLC/QLLC to Token Ring/Ethernet, if the XID negotiation is delayed or ends abnormally, a memory leak may occur. [CSCdi92511]
- The SDLC output queue can get stuck if the **sdlc line-speed** command is not set or if it is set to an incorrect value. A symptom is that the router stops sending SDLC frames out of the serial interface, resulting in SNA session drops. The interface needs to be recycled or reset to clear the condition. A workaround is to set the **sdlc line-speed** command parameter to equal the actual line speed being used. [CSCdj01434]
- Cisco 2520, 2521, 2522, and 2523 routers might report SDLC abort frames on the low-speed ports, but these abort frames do not get reported on the high-speed ports or on other platforms. This is because the low-speed ports count all aborts and the high-speed ports and other platforms only count aborts that are longer than 2 bytes. This is a cosmetic error and does not result in retransmitted frames. There is no performance impact at all. It is merely an indication that the transmitting device is sending erroneous bits after the trailing flag. These bits are simply ignored. No workaround is necessary. [CSCdj01488]
- A race condition may occur during session cleanup, which causes the DLUR router to crash or display a “Mfreeing bad storage” message for the “psp00” process. [CSCdj02249]
- DSPU/VDLC may not reconnect to the host if the switched major node is brought down and then back up. A workaround is to manually bounce the VDLC connection with the **no dspu start** and **dspu start** configuration commands. [CSCdj03475]
- When the user gives the **show fras** command, it might sometimes reload the router, if there are sessions trying to come up, or if there are sessions going down. [CSCdj03482]
- There is no handling for frame-reject SDLC frames. When the router is configured as SDLC primary, and the secondary device is configured as switched, then if the router receives a frame reject in response to XID, it fails to send an SDLC disconnect to reset the secondary devices SDLC state. [CSCdj03735]
- Exclusively configuring DLSw+ with the **icanreach netbios-name** command prevents some applications, including Microsoft Windows applications, from making NetBIOS connections. The workaround is to add an asterisk (*) to the end of the NetBIOS names configured with the **icanreach netbios-name** command. [CSCdj04936]

Interfaces and Bridging

- A Cisco 7500 series router in a transparent bridging environment suffers memory fragmentation causing the largest available memory block to be 120K. [CSCdi67513]
- A Cisco 4000 series Fast Ethernet Network Processor Module (NPM) does not respond to its virtual MAC addresses, which causes HSRP to fail. [CSCdi80641]
- When a router is configured as a RARP server and is also configured for transparent bridging on the same interface, the router does not respond to reverse ARP requests. The router should provide RARP service if configured as a RARP server, regardless of whether it is configured as later two bridge only. [CSCdi83480]
- Sometimes, HSRP running on VIP-Ethernet might fail to result in an active router. While Cisco is exploring the source of this problem, we recommend that if you have this problem, you should use the “use-bia” option and remove the use of the preempt feature. CSCdi85537 corrects the limitation where you should not use preempt with use-bia. [CSCdi83940]
- A Cisco 7200 series router configured for HSRP on an ethernet interface might send duplicate packets out the interface. [CSCdi85866]
- Sometimes FDDI interfaces may stop accepting multicast packets. [CSCdi92156]

- Packets destined to the HSRP virtual MAC address will not be routed if received on an 802.10 sub-interface. [CSCdj01435]
- When you are configuring IPX routing, a serial interface running BSTUN might be put into a down state and then come up again. Restarting the host session can bring the end-end connection back up. [CSCdj02488]
- Transparent bridging may cause high CPU utilization. The **show align** command can be used to confirm whether large “counts” of alignment errors are the source of the problem. The **show align** command will also yield TRACE information which can be decoded to determine the source of the problem. [CSCdj03267]
- A Cisco 7500 series router may report spurious errors such as the following:

```
*Dec 20 06:53:08: %RSP-3-ERROR: CyBus0 error 78
*Dec 20 06:53:08: %RSP-3-ERROR: invalid page map register
*Dec 20 06:53:08: %RSP-3-ERROR: command/address mismatch
*Dec 20 06:53:08: %RSP-3-ERROR: invalid command
*Dec 20 06:53:08: %RSP-3-ERROR: address parity error
*Dec 20 06:53:08: %RSP-3-ERROR: address parity error 23:16 1, 15:8 1, 7:0 1
*Dec 20 06:53:08: %RSP-3-ERROR: bus command invalid (0xF)
*Dec 20 06:53:08: %RSP-3-ERROR: address offset (bits 3:1) 14
*Dec 20 06:53:08: %RSP-3-ERROR: virtual address (bits 23:17) FE0000
*Dec 20 06:53:09: %RSP-3-RESTART: cbus complex
```

or

```
09:53:32.607 EST: %RSP-3-ERROR: MD error 0080008030003000
09:53:32.607 EST: %RSP-3-ERROR: SRAM parity error (bytes 0:7) 0F
09:53:33.363 EST: %RSP-3-RESTART: cbus complex
```

Such CyBus errors with code 78 and that point to a virtual address FE0000 or have MD errors similar to the above have two known causes. First, if there are HIPs in the router and on the bus reporting the CyBus error, if applicable, there is a race condition with the HIP microcode on an oversubscribed bus. The workaround on dual-CyBus platforms is to move all the HIPs onto a CyBus that is not oversubscribed. Second, these errors can be caused by the failure of a marginal CI arbiter board or an RSP board. As a result of this problem, all interfaces are reset, causing forwarding to be stopped for a few seconds. [CSCdj06566]

IP Routing Protocols

- The system might reload after a **show ip bgp inconsistent-as** command is entered. [CSCdi88669]
- The router does not forward BOOTP request broadcasts when the broadcast address is 0.0.0.0. [CSCdi88723]
- Cisco 4500 routers might reload and provide the following stack trace:

```
System was restarted by bus error at PC 0x601E4CD0, address 0xD0D0D0D
4500 Software (C4500-P-M), Version 10.3(16), RELEASE SOFTWARE (fc1)
Compiled Thu 24-Oct-96 18:32 by richardd (current version)
Image text-base: 0x600087E0, data-base: 0x60370000
```

Stack trace from system failure:

```
FP: 0x605D46B8, RA: 0x601E4CD0
FP: 0x605D46D8, RA: 0x601E4D88
FP: 0x605D46F8, RA: 0x601E50EC
FP: 0x605D4710, RA: 0x601C88E0
FP: 0x605D4740, RA: 0x601E4998
FP: 0x605D4760, RA: 0x601E5174
FP: 0x605D4778, RA: 0x60081D04
FP: 0x605D47B8, RA: 0x6006C8A4
```

This trace decodes as follows:

```
Symbols :
nhrp_cache_clear_nei
nhrp_cache_clear_nei
nhrp_cache_delete_subr
nhrp_cache_age_subr
rn_walktree_blocking_list
nhrp_cache_walk
nhrp_cache_age
registry_list
net_oneminute
```

[CSCdi90523]

- An extended access list that denies IP traffic and that does not require transport layer information might let fragments go through if the log option is configured. As a workaround, do not configure the log option. [CSCdj00711]
- After major topology changes, it is possible that OSPF neighbor lists can be corrupted. The **show ip ospf neighbor** command might indicate that OSPF has adjacency with itself. This prevents OSPF from establishing adjacency with other routers on the network. More seriously, this could lead to a router crash. [CSCdj01682]
- When set interface selects a multiaccess network, there should be a route in the routing table that matches the interface to determine the next hop. If the interface is point to point, there is no reason for the routing table entry. The workaround is to use set IP next-hop. [CSCdj01894]
- Potential memory corruption and memory leaks occur when sending out PIM packets. [CSCdj02092]
- A router may crash in NHRP while attempting to access a network which is not being served by NHS. [CSCdj03224]
- IGRP erroneously accepts a majornet route over an interface that is directly connected to a different majornet. [CSCdj03421]
- With certain topology in which host bit LSA could be generated, OSPF ABR will handle the host bit set LSA incorrectly and report the %OSPF-3-DBEXIST error message for type 3 LSAs. [CSCdj08699]

Novell IPX, XNS, and Apollo Domain

- When a device running LANE is configured as a LEC, it does not acknowledge any secondary IPX networks with frame types different from the primary. The **debug ipx packet** command displays these received packets as “bad pkt.” Only packets that arrive with the same IPX frame type as the primary IPX network on the ATM interface of the router are properly accepted. [CSCdi85215]
- XNS RIP requests for all networks cause normal periodic RIP updates to be delayed or skipped. [CSCdi90419]

- When IPX incremental SAP is running, the router's SAP table may not contain all the SAPs in the network if one of its interfaces goes down and comes back up later. [CSCdi90899]
- When running IPX incremental SAP, the router may not remove all the SAPs that are no longer reachable via this router. [CSCdi90907]
- When a router running NLSP receives an IPX aggregate route, SAPs whose source networks match that aggregate route will be installed into the SAP with a route hop count of 255, making those services unreachable. [CSCdi91209]
- On a Cisco C7200 series router running Cisco IOS Release 11.1 or 11.2, fast switching IPX traffic to a GRE tunnel can cause unexpected system reload. The workaround is to disable fast switching on the tunnel. [CSCdj01107]
- Connected routes are not redistributed to IPX Enhanced IGRP with the proper metrics. This may cause the remote routers to use a suboptimal route if multiple autonomous systems are configured and routes are mutually redistributed. [CSCdj04141]
- On a router that is configured for NLSP, when a more distant route is replaced by a better route, RIP might advertise two routes for the same network. [CSCdj04543]
- The IPX route table may be incomplete after an interface is shut down and more than one IPX Enhanced IGRP autonomous system is configured. [CSCdj07334]
- The router may reload if NLSP is disabled on an interface. [CSCdj08009]

TCP/IP Host-Mode Services

- The initiation of Telnet or other TCP connections may fail with an the error message “%Out of local ports.” A workaround is to attempt the connection a second time. [CSCdi60974]
- IP packets with valid TTLs (of varying values) that are received on a VIP2 serial PA or FSIP (both on RSP2 platform) with TCP header compression are intermittently dropped. The router sends an ICMP Time Exceeded message to the source:

```
show ip traffic will show ICMP Time Exceeded counter incrementing.
```

A workaround is to turn off TCP header compression. [CSCdj01681]

Wide-Area Networking

- Sometimes if a PPP is configured, the router may be restarted by a bus error. [CSCdi89566]
- If a **no shutdown** command is entered for a Group Async interface, the router may reload. [CSCdi91037]
- When using AAA accounting, a message similar to the following may be displayed:


```
%AAA-3-BADSTR: Bad accounting data: too many attributes
```

 [CSCdj00190]
- Sometimes, when a network management station frequently polls Frame Relay MIB data (of the *frCircuitTable*) from a router being reloaded and just trying to come up, a crash in Frame Relay MIB code area can occur. [CSCdj00447]

- When a Cisco router is configured for AAA accounting and it has agreed to authenticate with CHAP, each CHAP Challenge results in an accounting attribute being created. If the peer implements the optional mechanism to repeatedly authenticate the peer with multiple CHAP Challenges, this may eventually result in the “AAAA-3-BADSTR, Too many attributes” message. [CSCdj03234]
- The last X.25 fragment has the M-Bit set improperly when the packet is full, but no additional data is to be sent. [CSCdj03488]
- When you are modifying the LANE database, if you lose the Telnet session to the router, the database locks up. This is not a bug in the LANE code. A “dead” Telnet session takes approximately 5 to 8 minutes to be detected from the “alive” side. Once it is detected, the alive side cleans up and releases the lock. This is a Telnet feature and has nothing to do with the LANE database. The workaround is to reload the router. [CSCdj06660]
- When the CPU is very busy and running many processes, an attached ATM switch may tear down SSCOP and all SVCs because the SSCOP Poll PDUs sent by the switch are not serviced in time. The workaround is to keep other processes from using too much of the CPU. [CSCdj06928]

Caveats for Release 11.1(1) through 11.1(9)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(9). These caveats also apply to Releases 11.1(1) through 11.1(8) (unless otherwise noted).

For more caveats of Release 11.1(9) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(10).

Basic System Services

- On RSP systems, the router reloads with a SegV error when trying to free a misqueued buffer or a buffer that is an invalid size. The buffer might contain a bad packet passed to it from another router. [CSCdi74039]
- On Ethernets that experienced output errors, XBUFHDR and INVRTN errors could be seen. [CSCdi75404]
- The router may reload inadvertently if you respond improperly to extended ping dialogue prompts. [CSCdi88443]
- When using AAA accounting, a message similar to the following may be displayed:

```
%AAAA-3-BADSTR: Bad accounting data: too many attributes
```


[CSCdj00190]
- DHCP does not work across LANE. [CSCdj02153]
- After a Data-Direct VCC is created, the ATM-SIG input holding value is increased. Then, after the VCC times out, the ATM-SIG continues to hold some memory. This can cause a memory leak. This problem is common in VC environments. [CSCdj02779]

- When a Cisco router is configured for AAA accounting and it has agreed to authenticate using CHAP, each CHAP Challenge results in an accounting attribute being created. If the peer implements the optional mechanism to repeatedly authenticate the peer with multiple CHAP Challenges, this may eventually result in the “AAAA-3-BADSTR, Too many attributes” message. [CSCdj03234]

DECnet

- DECnet sends Phase IV prime hellos out Ethernet interfaces. [CSCdi83560]

EXEC and Configuration Parser

- Newer Telnet clients that support the NAWs option might cause **line** and **width** line configuration commands to appear on the vty. [CSCdi90442]

IBM Connectivity

- On CIP cards, it is possible to see the adapter type from the **show interface** command, but this information and version information is not available from the **show controller cbus** command. [CSCdi26192]
- This problem is most prevalent in STUN/local acknowledgment scenarios involving AS/400s: The remote router expects to see an OPCODE called LINK_ESTABLISHED from the host router, in order for it to transition the state from USBUSY to CONNECT. While in USBUSY state, the remote router continually sends RNR to the downstream devices. The host router will only send the OPCODE once it sees the first RR/P after a SNRM/UA exchange sequence. With other devices such as a FEP, an I-Frame can be sent out prior to the RR/P which would actually take the remote router state out of USBUSY, but the local acknowledgment states do not corresponding to the actual situation at hand. To work around this problem, you could use Cisco IOS releases that include the fix for CSCdi65599, which partially solves this problem. [CSCdi61514]
- If you have a serial tunnel (STUN) virtual multidrop configuration that is running local acknowledgment and STUN quick-response to accommodate AS/400 polling requirements, an AS/400 NPR time-out will occur if a remote physical unit (PU) T2.1 or T1 controller fails to activate when responding to the initial XID poll. To work around this problem, disable STUN quick-response, issue the **sdlc k 1** command on all Synchronous Data Link Control (SDLC) interfaces, and configure idle-character mark on the SDLC line(s) to the AS/400. [CSCdi66681]
- A router might reload when more than 125 sessions on the router are using QLLC/DLSw+ conversion. [CSCdi84896]
- When using the feature source-bridge local-route you may have a system failure if you issue the command **no ip routing**. Regular source-route bridging is not affected by this. [CSCdi86240]
- When using QLLC, a connection using a virtual MAC address from a pool of virtual MAC addresses may get connected to the wrong resource on the mainframe. [CSCdi86358]
- When a downstream PU2.0 stops by issuing a REQDISCONT to a DLUR router, the DLUR router may loop continuously restarting the link to a downstream PU2. In this case, the DLUR router sends a corrupted packet to the host, instead of a REQDACTPU. [CSCdi86769]
- An invalid packet might be received from the VTAM NN and the CP-CP session might be torn down. [CSCdi87217]
- When using NSP over DLUR, the router may leak small buffers. [CSCdi87320]

- For LU0-LU0 traffic the extended BIND may contain unformatted user data fields. The NN rejects the BIND; hence the session will never start. [CSCdi87365]
- Configuring the **output-lsap-list** command on local Token Ring interfaces does not block broadcast traffic from a DLSW peer. The workaround is to use a filter at the DLSW level on either router or to block the traffic with an **input-lsap-filter** command at the remote peer. [CSCdi88593]
- When running multiple large file transfers across DLSw using FST transport sequence, errors may occur, causing the job to abort. This is displayed by the command **show dlsw peer**. A sequence error occurs when a numbered FST (IP) packet is received by the DLSw peer and the sequence number does not match what the peer expects. [CSCdi89838]
- PEER INVALID trace messages are displayed on the console. Also, the session on the peer-on-demand does not come up for quite some time. [CSCdi90953]
- When running APPN/DLUR, heavy session activation can result in the router using all I/O (buffer) memory available in the router. Often the external symptom of this occurrence is the APPN subsystem shutting down. [CSCdi91380]
- On Cisco 7000 systems, packets that are fast switched from CIP to FDDI might be dropped by some Layer 2 switches because one additional byte is being added to the FDDI frame. The problem does not occur on RSP systems. A workaround is to use autonomous or process switching. [CSCdi91417]
- A DLUR router may crash with a “SegV exception” or an “Illegal access to a low address” message because of a DLUR memory corruption problem. This error results from a race condition that usually occurs when DLUR sessions are going up and down. The stack trace after the memory corruption usually indicates Mget_x. [CSCdi92947]

Interfaces and Bridging

- On Cisco 7200 systems, enabling automatic spanning tree on Token Ring interfaces causes the interface to transition. Disconnecting the cable might cause the router to reload with a PC bus error `ibm692_lap_read`, which results in a booting loop. To recover from this booting loop, reload the router. [CSCdi72257]
- On Cisco 7000 and Cisco 7500 series platforms that have FSIPs, transmitter delay does not seem to be working correctly. There is no workaround. The fix for this problem is available from 011.002(003.001) 011.001(008.003) 11.2(03.01)F 11.2(03.01)P. [CSCdi72431]
- On Cisco RP/SP 7000 series routers, if you reload the router after adding new interface processors or swapping interface processors, the configuration for serial interfaces may be lost. Also, the **encapsulation** command may be lost, causing the serial interface configuration to change to the default (HDLC). You can identify this problem if your interface is a serial interface, for example, an FSIP or a HIP, and the **show configuration** command correctly displays the original configuration for the serial interface. As a workaround, EOIR the new card, configure it, and issue the **write memory** command before reloading. [CSCdi79523]
- When pinging over sync DDR with HDLC stack compression, the router will unexpectedly reset. [CSCdi79832]
- The MultiChannel Interface Processor (MIP) **no channel-group** command causes the router to reload if OSPF is configured. [CSCdi79844]
- Issue occurs when performing a GetNext operation on the MIB object `dot1dTpFdbTable` in the Bridge MIB. A GetNext will not retrieve a request of index+1 and will instead return the lexicographically next index.

For example, if the table has the entries with indices of 0000.0000.0001 0000.0000.0002 0000.0000.0003 0000.0000.0005, a GetNext of 0000.0000.0002 would return the index 0000.0000.0005, because 0000.0000.0003 is the index requested + 1. A GetNext of 0000.0000.0003 would return the index 0000.0000.0005, because 0000.0000.0005 is greater than the requested index + 1. [CSCdi84559]

IP Routing Protocols

- When OSPF is configured with the **default-information originate** router command to generate default information, OSPF is prevented from installing the default information advertised by other OSPF routers. This causes a problem if OSPF does not really generate the default because a certain condition is not satisfied, for example, the gateway of last resort is not set. [CSCdi80474]
- IGMP and PIM should support multicast addresses (for example, c000.0004.0000) as configurable options on Token Ring interfaces instead of requiring broadcast address (for example, ffff.ffff.ffff). [CSCdi83845]
- RARP over ISL encapsulated Ethernet does not work. [CSCdi84700]
- A router might advertise a combination of unicast and DVMRP routes in excess of the configured route limit (but no more than two times the limit). The workaround is to configure a lower route limit. [CSCdi85263]
- The BGP **neighbor default-originate** command does not work if a 0.0.0.0 withdrawn message is sent to a neighbor. The workaround is to issue the **clear ip bgp *** command. [CSCdi87188]

ISO CLNS

- If minimum-sized (or sweeping sized) CLNS pings are done, and the CLNS source and destination addresses are very long, the system may fail. The workaround is to raise the minimum ping size to at least 63 bytes. [CSCdi91040]

Novell IPX, XNS, and Apollo Domain

- Routers might reload if configured for IPX Enhanced IGRP with parallel paths. The workaround is to run IPX RIP. [CSCdi84739]
- When a device running LANE is configured as a LEC, it does not acknowledge any secondary IPX networks with frame types different from the primary. The **debug ipx packet** command displays these received packets as “bad pkt.” Only packets that arrive with the same IPX frame type as the primary IPX network on the ATM interface of the router are properly accepted. [CSCdi85215]
- The **ipx down network-number** command might appear unexpectedly in the output of a **write terminal** command, and this command might be written to nonvolatile memory with the **write memory** command when the interface is down but you have not issued a **ipx down** command on that interface. There is no workaround. The unwanted command does not appear when the interface is up. If the unwanted command appears in nonvolatile memory, issue a **no ipx down** command followed by a **write memory** command when the interface is up to clear the undesired command from memory. [CSCdi85453]
- In a redundant IPX Enhanced IGRP network running IPX incremental SAP, the router’s SAP table SAP information may contain out of date information, such as the socket number if the socket number is changed from its initial advertisement. [CSCdi85953]

- SPX keepalive spoofing will cease to spoof after a router has been up for 24 or more days. The command **debug ipx spx-spoof** will show packets being skipped when they should be spoofed. The only workaround is to reload the router once every three weeks. [CSCdi86079]

TCP/IP Host-Mode Services

- A router will reload if TCP tries to repacketize a packet that has an invalid packet reference count. [CSCdi87175]
- Errors will be imposed on the TCP data structure if an RST is received while the application is half way through closing the connection. Local TCP will end up in an endless loop trying to send the last FIN to its peer. A typical symptom for the problem is that the CPU usage becomes very high, and the application that is doing the close will be stuck in TCP indefinitely. [CSCdi88063]
- TCP will get into endless acknowledgment war with its peer, if the application on both ends has stopped reading data. A typical symptom will be that CPU usage becomes very high on the router. A possible workaround for the problem is to clear the tty/vty line that owns the TCP connection in acknowledgment war. [CSCdi88065]
- A Telnet session with a nonzero number of unread input bytes cannot be cleared. [CSCdi88267]

VINES

- Routers that are connected via extremely slow links and that have a large routing table (for example, more than 300 entries) do not get the full routing update before the reassembly timer expires. The symptom is that routes repeatedly appear and then age out. To work around this problem, you can add access lists to eliminate some of the unneeded routes. [CSCdi79355]
- If you add a VINES static route of equal metric for an alternative path when **vines single-route** is configured, the system may reload. The workaround is to delete the static route or enter **no vines single-route** command. [CSCdi92190]

Wide-Area Networking

- The output hold queue holds all buffers that are being kept in the output queue because of traffic shaping. This slows down traffic for other VCs, causing the traffic to traverse the complete queue before it can leave the system. [CSCdi74940]
- Dial-on-demand (DDR) load balancing does not forward packets correctly when the system dials out via the **dialer load-threshold** command and more than one remote device is connected by either dial-out or dial-in. This typically occurs on a PRI with dialer load threshold configured, but may also occur on BRI or multiple DDR interfaces in a dialer rotary group when more than one remote device is connected. As a workaround, remove the **dialer load-threshold** command. [CSCdi76324]
- In certain environments, I/O and processor memory are being consumed by processes in the router, primarily the Critical Background process, and the router runs out of memory after 29 hours of operation. [CSCdi80450]
- When using a 4ESS PRI to place an international call (011), the call might be rejected with the error “cause i = 0x839C - invalid number format.” [CSCdi81069]

- When TEST/XID packets are received by a LANE client, the router may crash. There is no workaround for this problem. [CSCdi90868]
- ISDN signalling packets sometimes cannot be passed up through the serial driver. This makes BRI and PRI interfaces unable to talk to the phone switch. [CSCdi92159]

Caveats for Release 11.1(1) through 11.1(8)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(8). These caveats also apply to Releases 11.1(1) through 11.1(7) (unless otherwise noted).

For more caveats of Release 11.1(8) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(9).

AppleTalk

- A router might crash when an incomplete AppleTalk fast-switching cache entry is used. This happens when the cache entry is updated with another output interface within a small timing window. In most cases, this scenario is unlikely. [CSCdi77772]

Basic System Services

- AGS+ routers with first-generation FDDI cards (CSC-C2FCI) do not support translational bridging, and are no longer supported. They use encapsulated bridging. The second-generation AGS+ FDDI cards (CSC-C2FCIT) support both translational and encapsulated bridging.

Encapsulated bridging does not work on a Cisco 7500 series router. To bridge between an AGS+ and a Cisco 7500 series router, you must use CSC-C2FCIT cards in the AGS+ and translational bridging.

The big disadvantage of using encapsulated bridging is that it cannot use the hardware bridge filtering capabilities of the CSC-C2FCIT cards, which have a CAM built into them that is used to do bridge filtering on the card. When encapsulated bridging is used, the main processor must do all bridge filtering. This means that one busy encapsulated bridging FDDI network can consume the entire bandwidth of the router’s main processor, just for bridge filtering. Therefore, Cisco discourages the use of encapsulated bridging. [CSCdi46862]

- The router might reload after displaying the following message:

```
%SYS-3-TIMERNEG: Cannot start timer (0x1E4388) with negative offset (-495928).
-Process= "Per-minute Jobs", ipl= 0, pid= 37
-Traceback= 22157D7A 22154320 221A17EA 2215F45C 2213E074
```

High CPU utilization might occur prior to this message and the reload. [CSCdi76126]

- PCMCIA Flash card insertion or removal on a Cisco 7200 series router might cause a system reload with a PCI bus system/parity error. This caveat has been resolved in IOS releases 11.1(8.1) and 11.2(3.1). [CSCdi80691]

IBM Connectivity

- QLLC DLSw cannot reconnect after a failure. The following assert message is displayed:

```
%CLS-3-CLSFAIL: CLS: Assertion failed: file "../srt/qllc.c", line 4352
!"QsapAddCepFailed".
```

[CSCdi64840]

- Cisco 4700 series router Token Ring interfaces intermittently stop working and fail to reinitialize. This problem occurs only during heavy activity, when more than one Token Ring port is active. This problem only occurs on Cisco 4700 series routers, not 4000 or 4500 series routers. [CSCdi70398]
- The router crashes when you enter the **show lnm station** command. This might happen when there are many ring status changes, for example, when stations are added to or removed from the ring. This problem is platform independent. The workaround is to disable LNM. [CSCdi72954]
- APPN alerts are only sent over an LU6.2 session, even though it is a requirement to be able to configure these alerts to be sent over a SSCP-PU NSP session. [CSCdi73663]
- When two or more FEPs at a central site, each with the same TIC address, are connected to a different Token Ring and a different DLSw peer router, a remote SDLC attached PU2.0 device will not establish a session to the backup FEP if the first is taken offline. This problem does not affect PU2.1 devices. [CSCdi76575]
- The command **show dlsw reachability** crashes when the entry goes into VERIFY. [CSCdi77667]
- When running DLSw remote or local switching between QLLC/SDLC/VDLC and a TR, if the TR's largest frame (lf) is less than 4472, the circuit will not connect.

Using the **debug dlsw reachability** or **debug dlsw reachability error** commands will indicate an "lf" mismatch condition detected by DLSw. This condition should not be flagged as an error. The smallest "lf" across the entire path should be used for the circuit. [CSCdi77805]
- When using DLSw+ to communicate with non-Cisco devices, the Cisco platform might deal incorrectly with incoming transport keepalive packets. [CSCdi78202]
- When the command **stun remote-peer-keepalive** is enabled in a locally acknowledged STUN over Frame Relay configuration, STUN peers might constantly reset because of incorrect handling of STUN keepalives. [CSCdi78480]
- A router might reload when more than 125 sessions on the router are using QLLC/DLSw+ conversion. [CSCdi84896]

Interfaces and Bridging

- The MultiChannel Interface Processor (MIP) loopback remote command causes IPs to crash. [CSCdi69074]
- On Cisco 7000 and Cisco 7500 series platforms that have FSIPs, transmitter delay does not seem to be working correctly. [CSCdi72431]
- A Token Ring driver might misclassify IPX broadcast packets as SRB explorer packets, and flush them rather than switch them, if bridging. This problem occurs on low-end products only (igs xx c4500 platforms). No other protocol packets are affected. [CSCdi75134]
- Policy routing on a Cisco 7000 series router with silicon-switching enabled does not function correctly. To work around, manually disable silicon-switching on each of the interfaces with the **no ip route-cache sse** command. [CSCdi77492]

- In a Cisco 7206 router, when source-bridge is enabled the router may stop sending packets on the Token Ring interface. [CSCdi78494]
- The FDDI interface driver might interact poorly with OSPF during OIR, causing SPF recalculations. This occurs only when OSPF is running on a FDDI interface which is not being inserted or removed. [CSCdi81407]

IP Routing Protocols

- In very rare cases involving equal-cost backup routes to a failing route, it is possible for Enhanced IGRP to be caught in a “stuck in active” state (self-correcting after several minutes). There is no workaround to this problem. [CSCdi81791]
- OSPF can periodically lose neighbors over slow links when the OSPF database is refreshed. This problem causes excessive OSPF packets to be generated. There is no workaround. [CSCdi82237]
- An error might occur and cause these messages:

```
System restarted by error - Zero Divide, PC 0x38EF0C
(0x38EF0C:_igmp_report_delay(0x38eec6)+0x46)
```

[CSCdi83040]

- A router might advertise a combination of unicast and DVMRP routes in excess of the configured route limit (but no more than two times the limit). The workaround is to configure a lower route limit. [CSCdi85263]

ISO CLNS

- After removing a static CLNS route, ISO-IGRP prefix routes might count to infinity around a looped topology. The workaround is to use the **no clns router iso-igrp domain** command to break the loops in the CLNS topology until the routes age out. [CSCdi78048]

Novell IPX, XNS, and Apollo Domain

- NLSP links may reflect incorrect source network/node addresses in the routing tables. This does not hinder connectivity to other IPX networks when going between Cisco devices. However, certain non-Cisco routers may not like the incorrect address and NLSP routing may fail. NLSP routers should use the address Internal-Network.0000.0000.0001 when sending NLSP packets. Therefore, on WAN media that require MAPs for IPX, this should be the next hop address in the map statement. [CSCdi68981]

TCP/IP Host-Mode Services

- Non-TCP reverse connections to lines may corrupt memory, resulting in a software-forced crash. This problem was introduced starting in Releases 10.3(15.1), 11.0(11.1), and 11.1(6.1). [CSCdi79310]

Wide-Area Networking

- PRI ISDN calls may be dropped on heavily loaded Cisco 7513 routers with multiple PRIs. The following error is displayed when this occurs: “BRI Error: isdn_fromrouter() msg dequeue NULL.” [CSCdi66816]
- When two routers are connected to the same destination, outbound IP fast switching on dialer interfaces does not work on the more recently connected interface. The workaround is to turn off fast switching on the DDR interfaces using the **no ip route-cache** command. [CSCdi75490]
- When online insertion and removal (OIR) is applied to a VIP2 board, an ATP Interface Processor (AIP) might become stuck in an uninitialized state. The following messages may appear:

```
CBUS-3-CMD: Cmd failed: global ptrs, response 0x8010, AIP1 CBUS-3-AIPRSET: Interface  
ATM1/0, Error (8010) select - aip_reset() CBUS-3-AIPRSETU: Unit 32, Error (8010) enable  
- aip_reset()  
The workaround is to reload the router. [CSCdi75659]
```
- IPX fast switching with multiple route paths over multiple ATM/LANE interfaces/subinterfaces may cause random system reloads. The workaround is to use only one AMT/LANE IPX path, to set **ipx maximum-path 1**, or to use **ipx per-host-load-balance** to force only one interface to be used. [CSCdi77259]
- The negotiation of a PPP callback option, passing a dial string or E.164 number, will fail because of a defect that was introduced into 11.2(1.4), 11.1(7.1), 11.2(1.4)P, 11.2(1.4)F, and 11.0(12.1). The negotiation will appear to complete successfully, but the callback will not succeed. The failure can be seen if **debug ppp negotiation** is set. The callback option will be marked “acked,” but there will typically be garbage on the debug line between “allocated” and “acked,” for example, “PPP Callback string allocated ^” acked.” [CSCdi77739]

Caveats for Release 11.1(1) through 11.1(7)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(7). These caveats also apply to Releases 11.1(1) through 11.1(6) (unless otherwise noted).

For more caveats of Release 11.1(7) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(8).

Basic System Services

- The **boot config nvram**: configuration command, which was added for the RSP platform, interacts improperly when the **service compress-config** command is enabled. This causes the NVRAM to become locked, and the router must be rebooted to free the NVRAM. [CSCdi52587]
- On some devices, SNMP GetNext requests performed on the Cisco Discovery Protocol (CDP) MIB can cause the device to pause for an extended length of time. [CSCdi69892]
- In cases where an accountable task has a duration shorter than the time it takes to contact the TACACS+ accounting server, the stop record may be discarded without being transmitted to the server. [CSCdi70312]

- A problem has been found in the RSP code within Cisco IOS Releases 10.3, 11.0, 11.1, and 11.2. In extremely rare conditions, a failure condition can occur when Backing-Store or Fair Queuing are enabled. To avoid these problems, the rsp- Cisco IOS images in affected releases are no longer available. For IOS Release 11.1, this problem has been fixed in maintenance release 11.1(8) and later 11.1 releases.

To avoid this problem, you should upgrade all IOS Release 11.1 RSP-based systems to Cisco IOS Release 11.1(8), or a later 11.1 release.

For those systems that cannot be upgraded, you can avoid this problem by disabling Backing Store, Fair Queuing, and UDP turbo flooding.

Disable Backing Store and Fair Queuing on each interface with the commands **no transmit-buffers backing-store** and **no fair-queue**. Backing Store defaulted to OFF in images beginning with 11.1(4.1). However, it is important to look at the current configuration. An image configured before Backing Store defaulted to OFF may have it ON for router interfaces.

Disabling UDP turbo flooding is a workaround required for 11.0 and later major releases. UDP turbo flooding is OFF by default in all releases, however, you should ensure that it is turned OFF in the current configuration. The command to disable UDP turbo flooding is **no ip forward-protocol turbo-flood**.

[CSCdi71609]

- A device with RMON enabled may reload if free memory gets too low. [CSCdi74278]
- Timer-related functions, such as NTP and routing update intervals, do not work correctly in Revision D Cisco 4700 routers. Also, Revision E Cisco 4700 routers are recognized by SNMP as “4700” instead of “4700M.” [CSCdi75353]
- The router might display this message, then reload:

```
%SYS-3-TIMERNEG: Cannot start timer (0x1E4388) with negative offset (-495928).
-Process= "Per-minute Jobs", ipl= 0, pid= 37 -Traceback= 22157D7A 22154320 221A17EA
2215F45C 2213E074
```

High CPU utilization may be seen prior to message and reload. [CSCdi76126]

EXEC and Configuration Parser

- The router will crash if you issue a command line that is an alias and that is greater than 256 characters in length after the alias is expanded. [CSCdi63994]

IBM Connectivity

- QLLC devices that are connected through a router using QLLC/LLC2 conversion might occasionally experience poor response time. [CSCdi44923]
- Online Insertion and Removal (OIR) of an IP in a Cisco 7500 series router equipped with a CIP and another IP that has the same size MTU as the CIP can cause the router to crash with a ciscoBus error. [CSCdi59377]

- If you are running IOS Version 11.1(x) and you have a four port Token Ring port adapter in a VIP2 you may see the following crash:

```
ALIGN-1-FATAL: Illegal access to a low address addr=0x1, pc=0x60544FE0, ra=0x60544FE8,
sp=0x60AEE780
*** System received a SegV exception ***
signal= 0xb, code= 0x8000200c, context= 0x60a1a980 PC = 0x6010bfd4, Cause = 0x2020,
Status Reg = 0x34008002
DCL Masked Interrupt Register = 0x00000000
DCL Interrupt Value Register = 0x00000000
MEMD Int 6 Status Register = 0x00000000
System was restarted by error - a SegV exception, PC 0x60544FE0
```

The workaround is to not use the Token Ring interfaces on the VIP. [CSCdi69234]

- If you are running DSLW Fast Sequenced Transport (FST) on a Cisco RSP 7500 series router, the Token Ring input queue on the Token Ring might become wedged. [CSCdi71840]
- When segmentation or reassembly is involved in a DLUR-managed LU-LU session (that is, the MTU for the downstream link to the PU is smaller than the MTU for the upstream link toward the host) and the RU size is larger than can be transmitted in a single frame (most common with IND\$FILE transfers from a PU to the host), the router may reload with an “intermediate_reassembly” or a memory corruption stack trace. [CSCdi72260]
- On a Cisco 7000 series router running an RSP7000 with Release 11.1(6) or Release 11.1(7), CIP microcode cannot be read if it has been loaded into boot Flash. The workaround is to load the CIP microcode into Flash. [CSCdi72463]
- A defect introduced by the fix for defect CSCdi69231 may cause NSP to stop working. The following messages may be displayed when NSP stops working: “SNA: Connection to Focal Point SSCP lost.” and “SNA: MV_SendVector rc = 8001.” [CSCdi72696]
- Data-link switching (DLSw) sometimes cannot handle disconnects being issued by two stations that are in session, if the stations have a requirement to re-establish a session in less than 3 seconds. The first disconnect is answered with a UA message but the second is not responded to until the station resends the disconnect message (DISC). After the DISC is resent, a DM message is sent to answer. [CSCdi73204]
- Frames coming from a High-Speed Serial Interface (HSSI) are sometimes dropped. This problem occurs when a Cisco router has remote source-route bridging (RSRB) configured direct over a HSSI interface. The HSSI interface shows that the packets are forwarded on the interface itself, but the packets are not passed to the source-route bridging (SRB) process. The **show source** command on FHDC-1 shows “receive cnt:bytes 0,” and the **show interface h 5/0** command shows that nonzero packets are input. [CSCdi73357]
- An APPN/DLUR router cannot establish an LU-LU session with a downstream DSPU router. The bind sent by the host is rejected by the DLUR with an 0x0806002b sense code. [CSCdi73494]
- When more than 38 SDLC devices are configured upstream and downstream using DLSw local switching, the router crashes with the following message:

```
Exception: Line 1111 Emulator at 0x7E9500 (PC)
```


[CSCdi73675]
- When many sessions are created and then torn down over an ISR network, a memory leak might occur in the router. [CSCdi73676]
- DLSw+ backup peers continue to accept new connections after the primary link is restored. This continues until the backup link is torn down when the linger time expires. [CSCdi73864]

- A Cisco 7206 fails to source-route-bridge IP packets (“no ip routing”). The workaround is to route instead of bridge IP. [CSCdi75477]
- If SNA/DSPU receives a RECFMS frame that contains control vectors *and* the RECFMS cannot be forwarded to the focal point host for any reason (for instance, the focal point is inactive), the negative response sent by DSPU causes the router to display the BADSHARE error and deactivate the connection. [CSCdi76030]
- If a BIND request is received before the Notify response has arrived, DSPU will reject the BIND request with sense code 0x80050000. [CSCdi76085]

Interfaces and Bridging

- A Cisco 2500 router Token Ring interface will not try to reinsert itself into the Token Ring hub after one failed attempt. [CSCdi41499]
- When an ARP packet is received from the ATM interface, the router sends out a total of two ARP packets to the Ethernet interface. [CSCdi70533]
- If transparent bridging and an IP address is configured on a VIP Fast Ethernet or Ethernet interface, duplicate packets may occur on directly connected LANs to the VIP interface. In particular, Unicast DODIP packets between two workstations on a segment on which the VIP2 interface is attached can be incorrectly duplicated by the router. This can also occur when running bridging and any other protocol in this type of configuration.

In addition, if VIP Ethernet is used with multiple unicast protocols such as HSRP, packet duplication can occur on the LAN segment. These problems can significantly degrade RSP performance. [CSCdi71856]

- Under certain conditions Spanning Tree Protocol can cause a memory leak. This occurs when small buffers are created but not released. (“Created” increases but “Trims” doesn’t in the show buffer.) Also, the **show memory** command will show the available memory going down.

Spanning Tree BPDUs are handled by small buffers. If a BPDU that was handled in a small buffer is used at the same time the interface is going down, this small buffer will erroneously not be released. [CSCdi72783]

- Weighted fair queuing, custom queuing, and priority queuing should not be enabled on a MIP interface. In addition, the MIP tq1 should be no smaller than 32. Note that the T1 controller does not need to be reset when outhung is cycling. [CSCdi73106]
- In Cisco 7500 series routers, the following error message might be displayed while booting the system image from TFTP or Flash memory, or when changing the serial encapsulation (for example, from HDLC to SMDS) or when doing OIR of another card in the chassis:

```
%CBUS-3-CMDTIMEOUT: Cmd timed out, CCB 0x5800FF50, slot x, cmd code 0
```

The **show diag x** command reports that the board is disabled (wedged). The **show version** command does not show the card in the specified slot. The **write terminal** command does not show the configuration for the card in the slot. A possible workaround is to issue a **microcode reload** command or to load a new system image that has the fix for this bug. [CSCdi73130]

IP Routing Protocols

- A Management Information Base (MIB) query of the ospfLsdbTable fails because no MIB objects are found under the ospfLsdbTable subtree. However, some subtrees under OSPF can be successfully queried, such as ospfGeneralGroup, ospfAreaTable, and ospfIfTable. [CSCdi69097]

- When clearing an IP host route (for example, 10.1.1.1/32) learned by OSPF out of the IP routing table, it can take a long time for the network route (for example, 10.1.1.0/24) to reappear in the table when done on a stable network, and when only the net route, not the host route, exists in the table. To avoid this problem, clear the network route exactly as it appears in the IP route table; do not clear the host route. [CSCdi70175]
- When a primary active router that has gone down comes back up, it is possible that both routers might forward packets instead of just the primary. [CSCdi70693]
- ATM blocking occurs with input queue full 151/150. No signalling occurs, just RFC defined for packets blocked and returned by **show buffers old dump**. [CSCdi72840]
- The system suffers a gradual loss of free memory whenever **ip sd listen** or **ip sdr listen** are enabled. [CSCdi72863]
- Use of the DNS Name Service for alias lookups causes the router to reload. Lookups of canonical names do not exhibit this problem. [CSCdi73022]
- When the cache is populated, the system will not perform correctly policy routing on subinterfaces. This has been produced on Cisco 4500 series routers with ATM LANE subinterfaces. The problem does not occur when the IP route cache is cleared. [CSCdi74375]

ISO CLNS

- If an interface is down when it is configured as passive for IS-IS, it will not be advertised in IS-IS link state packets when the interface comes up. The workaround is to unconfigure the interface and then reconfigure it as passive after it is up. [CSCdi76431]

Novell IPX, XNS, and Apollo Domain

- Some Service Advertisement Protocols (SAPs) might not be seen if an interface is flapping while running IPX Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) and the **ipx sap-incremental** command is configured. As a work around, clear the IPX Enhanced IGRP neighbors. [CSCdi72438]
- A Cisco 7200 series router running IPX fast switching with various encapsulations of IPX—including IPX over ISL—may produce packets that are ignored by the receiving host. A workaround is to disable IPX fast switching using the **no ipx route-cache** command; however, this workaround causes increased router overhead. [CSCdi73231]

TCP/IP Host-Mode Services

- A crash sometimes occurs at PC 0x12CFA8, address 0xD0D0D11 [CSCdi70432]

Wide-Area Networking

- The AIP cannot be configured to issue idle cells instead of unassigned cells. [CSCdi48069]
- In certain circumstances, the router might reload if a dialer interface (ISDN/Serial/Async) is used for load-backup or failure-backup along with an IPX routing protocol like RIP or Enhanced IGRP and the primary and backup interfaces are active. This is usually seen immediately after the dialer interface connects. [CSCdi61504]

- Some ISDN PRI NET5 switches may send a Restart message with either an invalid or an unused B-channel. The router should answer the Restart message with a Restart Acknowledge message for the valid B-channels. If the router does not answer the Restart message, the switch may place the ISDN PRI interface “out-of-service.” [CSCdi70399]
- Using TACACS+ with dialback over a rotary group causes the authorization to fail for the user when the callback script aborts or finishes incorrectly, so failover to another line of the rotary occurs. The call is made, but an internal error occurs when debugging TACACS+. [CSCdi70549]
- After a number of days PRI calls may be dropped and high ISDN CPU utilization may be seen. There may be some discrepancy between the output of the **show dialer** command, which indicates that free B channels are available, and the **show isdn service** command, which shows that all channels are busy. A software forced crash also will eventually occur. [CSCdi75167]
- The negotiation of the PPP Callback option will fail due to a defect that was introduced into 11.2(1.4), 11.1(7.1), 11.2(1.4)P, 11.2(1.4)F, and 11.0(12.1). The failure can be seen if **debug ppp negotiation** is set when the following trace message is output: “PPP Callback string allocated ^” acked.” Note the gibberish after the word “allocated.” There is no workaround for this defect. [CSCdi77739]

Caveats for Release 11.1(1) through 11.1(6)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(6). These caveats also apply to Releases 11.1(1) through 11.1(5) (unless otherwise noted).

For more caveats of Release 11.1(6) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(7).

AppleTalk

- When ARAP is configured, the message “%SYS-2-INPUTQ: INPUTQ set, but no idb, ptr=xxxxx %SYS-2-LINKED: Bad enqueue of xxxxx in queue yyyy” might appear and the router might reload. [CSCdi63635]
- There has been a request for additional debugging messages for the **arap logging** command. The requested command is **arap logging debug-extensions**, which enables seven advanced debugging messages in addition to the traditional ARAP logging messages. [CSCdi68276]
- AppleTalk domains do not operate correctly when configured on subinterfaces. The domain properties will be applied to the main interface rather than its subinterface(s). The workaround is to disable AppleTalk fast switching. [CSCdi69886]

Basic System Services

- If a **microcode reload** command is issued over a Telnet connection, the router may enter an infinite loop or display the message “%SYS-3-INTPRINT: Illegal printing attempt from interrupt level.” whenever microcode is downloaded. [CSCdi47580]

- Multiple simultaneous **copy** operations to the Flash devices on a Cisco 7500 router (bootflash:, slot0:, and slot1:) will cause the router to crash. This only happens when more than one user is logged in to the router (for example, one at the console, and one via Telnet) and both are trying to perform a **copy tftp flash** at the same time. This is true even if the two users are trying to write to different devices. [CSCdi50888]
- When **service compress-config** is configured, accessing the configuration stored in NVRAM from simultaneous Exec sessions might leave the NVRAM locked and inaccessible. The only recourse is to reload the software. [CSCdi68092]
- A Cisco 2511 may reset with the error message “System restarted by bus error at PC 0x30B65F4, address 0xD0D0D29.” [CSCdi69068]
- The **debug chat line x** command and parser do not display the chat script components correctly if the octal 7 or 8 bit \xxx format is used to specify a byte greater than 0x7f. [CSCdi69149]
- If a new MIP channel group is added after a microcode reload has been performed, the system must be rebooted to ensure correct operation. [CSCdi70909]

DECnet

- DECnet may fail to work properly when using an area number of 63 for L2 routers. The symptoms are being unable to ping (DECnet) between two area routers, one of which is using area 63.x, and having the **show dec** command report that the “attached” flag is false even though the **show dec route** command shows routes to it. The workaround is to use the **decnet attach override** command to force the router into an attached state. This command is available in Releases 10.2(7.3), 10.3(4.4), 11.0(0.13), and all versions of Release 11.1 and higher. [CSCdi69247]

EXEC and Configuration Parser

- Under some circumstances, a Cisco AS5200 may run low on memory or may run out of memory after processing more than 11,000 calls. A small amount of memory may be lost under two conditions, only when **aaa new-model** is configured: when a user hangs up at the “Username:” prompt, or when a user successfully autoselects with the **autoselect during-login** command configured. [CSCdi67371]

IBM Connectivity

- Some IBM LLC2 implementation devices send an RNR when they run out of buffers and drop the frame. This causes data traffic flow to halt for 30 seconds. Non-IBM LLC2 devices using IEEE LLC2 send REJ rather than RNR, thus no delay occurs. [CSCdi49447]
- With Release 11.0 and a direct Escon-attached CIP, the host may “box” the CIP if the router is reloaded without the CIP being varied offline. This problem has not been seen with CIPs connected through a director or if the CIP is taken offline before the router is reloaded. The workaround is to vary the device offline before reloading the router. [CSCdi59440]
- When the PS/2 Link Station Role is configured as Negotiable, the XID(3) Negotiation may not complete. The workaround is to configure the PS/2 Link Station Role as Secondary. [CSCdi60999]
- When running CIP SNA over DLSw, the LLC2 control blocks may not get freed even when the LLC2 session is lost and the DLSw circuit is gone. The workaround is to reload the router. [CSCdi62627]

- When **source-bridge sdllc-local-ack** is enabled, the router stays in disconnect after the SDLC PUs are inactivated in VTAM. The workaround is to remove the **sdllc-local-ack**. [CSCdi64640]
- LSAP filters and NetBIOS host filters that are applied to the DLSw remote-peer statements do not work on DLSw border routers. [CSCdi66251]

- If the Channel Interface Processor (CIP) card on a Cisco 7000 router is in a hung state, the Cisco IOS software may enter a loop trying to reset it. The following messages will be repeated:

```
%CBUS-3-CIPRSET: Interface Channelslot/port, Error (8010) disable - cip_reset()
%CBUS-3-INITERR: Interface decimal, Error (8004), idb hex decimal cmd_select -
cbus_init() %CBUS-3-INITERR: Interface decimal, Error (8004), idb hex decimal
cmd_select -cbus_init() %CBUS-3-CTRLRCMDFAIL1: Controller decimal, cmd (128 hex) failed
(0x8010)count (16) %CBUS-3-FCICMDFAIL1: Controller decimal, cmd (32 0x00000001) failed
(0x8010) count (1)
```

Looping may be severe enough to require a router reboot.

The looping messages may overrun the logging buffer and thus obviate the reason for the initial attempt to reset the CIP. [CSCdi66420]

- The router may crash with the message “Illegal access to low address” if it is running low on memory and RSRB is configured. [CSCdi67879]
- The router crashes when NSP is configured and is trying to connect back to the owning host. [CSCdi69231]
- A router interface operating in an SDLC secondary role will not respond to TEST P. [CSCdi70562]
- When using DLSw FST, end-user sessions may not switch over to an alternate LAN or peer path after a connectivity failure. [CSCdi70709]

Interfaces and Bridging

- When you perform buffer changes on a serial interface with SMDS encapsulation, the changes are not recognized after a reload. [CSCdi62516]
- The **source-bridge ring-number** command allows you to configure a ring-number mismatch. The workaround is to make sure that all bridge devices on a ring use the same ring number. [CSCdi63700]
- In Cisco 7500 series routers, the following error message might be displayed while booting the system image from TFTP or Flash memory, or when changing the serial encapsulation (for example, from HDLC to SMDS):

```
%CBUS-3-CMDTIMEOUT: Cmd timed out, CCB 0x5800FF50, slot x, cmd code 0
```

The **show diagnostics x** command reports that the board is disabled, the **show version** command does not show the card in the specified slot, the **write terminal** command does not show the configuration for the card in the slot. A possible workaround is to issue a **microcode reload** command or load a new system image that has the fix for this bug. [CSCdi66450]

- Using 802.10 encapsulation on an FDDI trunk port, a Cisco 4700 router cannot form OSPF neighbor adjacencies with other routers on the other side of a Catalyst switch connected via 10BaseT. The workaround is to configure bridge-group under the FDDI subinterface.
- Small and middle buffers leak when transparent bridging on ATM is enabled. [CSCdi69237]
- When using the custom-queuing feature in conjunction with payload compression on HDLC or Frame Relay encapsulations, traffic regarded as “low-priority” by custom-queuing might be passed uncompressed. This results in lower than expected compression ratios. [CSCdi71367]

IP Routing Protocols

- If the router is reloaded when the OSPF dead-interval setting is the same as the original default (40 for broadcast networks and 120 for nonbroadcast networks) and the hello-interval is not the default, the router does not retain the OSPF dead-interval setting, even though the configuration in NVRAM shows the dead-interval set properly. The router sets a default value to the dead-interval instead of what is set in the NVRAM config.

The workaround is to not set the dead-interval the same as the original default.

When the fixed image is first loaded, the problem still happens. To resolve the problem, reconfigure the dead-interval again and perform a **write memory** operation. [CSCdi62640]

- The **match** keyword is not working with the **redistribute** command. The workaround is to use the **route-map** keyword. [CSCdi64310]
- IPX Enhanced IGRP updates do not propagate if the MTU size is less than the IPX Enhanced IGRP packet size. [CSCdi65486]
- Processing of input offset lists in Enhanced IGRP was disabled erroneously, so offset list processing is not available. There is no workaround. [CSCdi65889]
- If you have neighbor statements pointing to a subnet broadcast address, it may fail to send updates to that broadcast address. [CSCdi67411]

Novell IPX, XNS, and Apollo Domain

- After upgrading Cisco IOS software, a **show processor memory** command might indicate that the IPX SAP table memory usage has grown by almost 300%. [CSCdi65740]
- Using IPX-Enhanced IGRP can cause a memory leak when a link with an Enhanced IGRP neighbor is flapping. The SAP updates are queued and backed up, thus taking increasing amounts of memory. [CSCdi66169]
- If SPX spoofing fails to send a keepalive, a traceback message will be display on the system console. [CSCdi69062]

TCP/IP Host-Mode Services

- RSH commands entered without a controlling shell return only the first 1608 bytes of data. [CSCdi69424]
- The fix of defect CSCdi66910 introduced this defect, and CSCdi71158: the system may reload when doing DNS name validation. There is no workaround. [CSCdi70707]

Wide-Area Networking

- Dialing into an asynchronous line and starting a SLIP/PPP session may fail even though the same IP address was previously allocated successfully for the particular user. [CSCdi63143]
- Setting a group range on a pre-11.2 group-async interface while calls are active causes all asynchronous modem calls to be disconnected. [CSCdi66297]
- The command **no interface atm#/0.#** does not remove PVCs configured on the subinterface. The workaround is to use the **no atm pvc** command to remove the PVCs, and then remove the subinterface using the **no interface atm#/0.#** command. [CSCdi66774]
- A Cisco 2511 may reload at `_bridge_enq` when no bridging is configured. [CSCdi67157]

- The error message “%UTIL-3-TREE: Data structure error--received” might occur when using NHRP in Release 11.1(4). [CSCdi67350]
- The VIP/VIP2 IPC overlaps some TX accumulators and makes those accumulators spurious. Those accumulators are not used until the number of interfaces is more than 20. [CSCdi67842]
- When parallel, nonmultilink connections exist in a dialer group, the loss of one connection will remove the route to the peer address even though one or more connections exist to forward packets to the destination. This defect occurred as a result of fixing CSCdi59425. [CSCdi67844]
- Using ATM PVC and bridging, the number of ARP requests sent out depends on the number of subinterfaces created under the ATM interface. [CSCdi67980]
- Memory corruption (and subsequent reload of the router) may occur if AAA authorization is enabled and there is no DNS server configured on the router. Enabling **no ip domain-lookup** will decrease the chances of memory corruption. If you are running an Enterprise image, you may enable to command **kerberos local-realm kerberos-realm** as a workaround for this problem. [CSCdi68041]
- When dialing into a Cisco AS5200 from an I-Courier modem over synchronous ISDN and then starting a PPP session, the router might crash. This occurs only when login is performed on a non-asynchronous interface and when extended TACACS is enabled. A workaround for non-asynchronous interfaces is to use AAA/TACACS+. [CSCdi68257]
- If multiple, parallel connections to the same peer are made and one connection drops, the remaining connections may be unusable as packets will not be forwarded over them. [CSCdi68456]
- On certain platforms, entering an **ip address** configuration command while the interface is connected to a SLIP or PPP peer may cause a software-forced reload. [CSCdi69809]
- A neighbor route is not installed for PPP connections over an asynchronous or a vty-asynchronous connection. This defect was introduced by the fix for CSCdi50490, and only affects Releases 11.1(6.0.2) through 11.1(6) and 11.2(0.25) through 11.2(1). [CSCdi69919]
- Some IPX clients, including Windows 95, change their IPX node number on every connection. This means in a DDR environment it is impossible to create a static dialer map for a dial-in Windows 95 IPX client. The workaround is to create a dynamic dialer map for IPX when a client authenticates and provides their IPX node number. [CSCdi70873]
- ISDN BRI routers may have problems bringing up multiple B-channels to the same destination. The router and PBX may also get into a Layer 3 state mismatch and continuously exchange Layer 3 messages. [CSCdi71333]

Caveats for Release 11.1(1) through 11.1(5)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(5). These caveats also apply to Releases 11.1(1) through 11.1(4) (unless otherwise noted). For more caveats of Release 11.1(5) and earlier 11.1 releases, see all the preceding caveat sections. Only serious caveats are described in these release notes. For the complete list of caveats against this release,

access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document. All the caveats listed in this section are resolved in Release 11.1(6).

Additionally, one caveat was resolved in a special release prior to Release 11.1(6), as well as in Release 11.1(6). This special release was named 11.1(5a) and is described in the following paragraphs.

Cisco IOS Release 11.1(5a)

The Cisco IOS Release 11.1(5) rsp- images were rebuilt to include a single defect fix, and were renumbered to 11.1(5a). The defect is bug CSCdi66673 and is described as follows:

When Ethernet runt packets are received by Cisco 7500 series router processors (RSP1, RSP2, or RSP7000), a Reserved Exception crash or a QAERROR error will occur. When either of these problems happens, a switching complex restart is forced. The Reserved Exception crash has the following output:

```
Queued messages:
Aug 14 10:44:16: %RSP-3-ERROR: memd write exception, addr 08000000
Aug 14 10:44:16: %RSP-3-ERROR: RSP alignment error on write to QA, addr 080000
00
*** System received a reserved exception ***
signal= 0x9, code= 0x0, context= 0x60c72fd0
PC = 0x60107514, Cause = 0x2020, Status Reg = 0x34008702
DCL Masked Interrupt Register = 0x000000ff
DCL Interrupt Value Register = 0x00000000
MEMD Int 6 Status Register = 0x00000000
```

The QAERROR error has the following output:

```
Jun 17 10:50:23.329: %RSP-2-QAERROR: reused or zero link error, write at addr 03
08 (QA)
log 260308C0, data A816FFFF 00000000
```

Access Server

- If an unprovisioned or incorrectly provisioned T1 is attached to a Cisco AS5200, the router becomes unresponsive. [CSCdi64205]

AppleTalk

- A router configured with AppleTalk Enhanced IGRP takes too long to age-out routes even when the link is down, causing a long convergence time for features such as backup interface. [CSCdi62796]
- In Release 11.1(4), the Cisco IOS software displays the **appletalk domain** global configuration command after all the interfaces. This causes the **appletalk domain-group** interface configuration command to be invalid. If the router reloads, the network remapping does not work automatically and causes major network conflicts in AppleTalk. [CSCdi63707]
- IPTalk does not function correctly. IPTalk-speaking CAP servers cannot communicate and are not recognized on the network. [CSCdi64165]

Basic System Services

- On RSP-based systems, the following message may appear:

```
%DBUS-3-DBUSINTERR: Slot 0, Internal Error
```

The message may also be accompanied by the following:

```
%CBUS-3-CMDTIMEOUT: Cmd time out, CCB 0XXXXXXXX slot n, cmd code n
```

```
%DBUS-3-WCSLDERR: Slot n, error loading WCS, status 0xXX cmd/data 0xXX pos n
```

If the WCSLDERR error occurs, the board is effectively disabled and is not displayed when you issue a **write terminal** command. Issue a **microcode reload** command to take the card out of the disabled state. [CSCdi49854]

- Cisco 7500 series routers cannot fast switch packets whose size is greater than 8192. These packets are switched at process level which is a slower performance path. [CSCdi60295]
- HSA and VIPs now can coexist in Cisco 7500 series routers. [CSCdi60891]
- RADIUS passwords are limited to 16 bytes and are truncated if longer. [CSCdi62518]
- When installing HSA, both RSPs must have an equal amount of DRAM, and the slave and master RSPs must both have a minimum of 24 MB of DRAM. [CSCdi62683]
- Control characters are not interpreted properly in chat scripts. [CSCdi62960]
- In some cases the **snmp-server party** and **snmp-server context** configuration commands may cause a system reload. Neither of these commands verifies that the configured OID is not already in use, so it permits multiple records to be configured with the same OID, violating the rule that each record must have a unique OID. A common occurrence is to attempt to configure an `initialPartyIdentity` or `initialContextIdentity` that conflicts with the OIDs that are automatically preconfigured per RFC 1447. A workaround is to not configure OIDs that conflict with the initial party and context OIDs specified in RFC 1447. [CSCdi63694]
- Cisco routers with Motorola 68000 microprocessors (such as the Cisco 7000 and Cisco 2500 series) cannot fast switch packets larger than 8192 bytes. These packets are switched at process level, a slower performance path. [CSCdi63695]
- Using RADIUS for PPP authentication causes a slow memory leak. A periodic reload of the router will prevent this from becoming a problem. [CSCdi63788]
- The remote file system (RFS) (a Cisco IOS facility that allows interface processors the ability to access the RSP Flash file system) can fail on RSPs with RAM configurations less than or equal to 16 MB. Since the Channel Interface Processor relies upon the RFS to download run-time code dynamically, it is unusable. Either the CIP must be removed from the configuration, or the RSP RAM must be increased. [CSCdi64706]

- When Ethernet runt packets are received by Cisco 7500 series router processors (RSP1, RSP2, or RSP7000), a Reserved Exception crash or a QAERROR error will occur. When either of these problems happens, a switching complex restart is forced. The Reserved Exception crash has the following output:

```
Queued messages:
Aug 14 10:44:16: %RSP-3-ERROR: memd write exception, addr 08000000
Aug 14 10:44:16: %RSP-3-ERROR: RSP alignment error on write to QA, addr 080000
00
*** System received a reserved exception ***
signal= 0x9, code= 0x0, context= 0x60c72fd0
PC = 0x60107514, Cause = 0x2020, Status Reg = 0x34008702
DCL Masked Interrupt Register = 0x000000ff
DCL Interrupt Value Register = 0x00000000
MEMD Int 6 Status Register = 0x00000000
```

The QAERROR error has the following output:

```
Jun 17 10:50:23.329: %RSP-2-QAERROR: reused or zero link error, write at addr 03
08 (QA)
log 260308C0, data A816FFFF 00000000
```

[CSCdi66673]

- -fin- images do not support RIP, but should. [CSCdi67269]

IBM Connectivity

- A Cisco 4500 or Cisco 4700 series router running RSRB might restart with the error message “%ALIGN-1-FATAL: Illegal access to a low address.” [CSCdi35905]
- An SDLLC secondary router fails to respond to SNRM input frames. This problem was introduced by CSCdi51341. [CSCdi56398]
- Valid multicast explorers that should be handed to the protocol stack are instead being diverted to the SRB module and are being flushed by the SRB explorer control mechanism.

This problem was introduced by some changes to the Token Ring interrupt handler in Release 11.0 and later.

There is no workaround for the diversion, though the flushing can be avoided by raising the explorer maxrate value to some high number. However, this may cause instability in the network. [CSCdi59090]

- A FRAS BNN-to-SDLC link does not restart when Frame Relay is power-cycled. After the CSU is powered off, the “fras backup rsrb” kicks to put the SDLLC traffic across the RSRB peers. When the CSU is powered back on and the Frame Relay DLCI comes back up, the FRAS BNN connection to the SDLC nodes does not reactivate, although connections to Token Ring nodes do restart. [CSCdi61156]
- If the **vmac** parameter is not specified in the **qllc dlsw** command, a Cisco 4500, Cisco 4700, or Cisco 7500 router may crash in the function **QLLCtestStnReq()**. [CSCdi61562]
- QLLC may try to initiate a connection in the middle of activating a connection. [CSCdi62155]
- Using DLSw+ local switching and QLLC, the LF field in the RIF of Test Responses sent on Token Ring are not consistent. A workaround is to configure an MTU size of 4500 on the X.25 interface. [CSCdi62416]
- DLSW NetBIOS cannot connect to Windows NT. [CSCdi62784]

- A race condition when one DLSw peer has come up while another is in the process of coming up results in the error message “IBM: Unknown L3 PID, fr_doencap failed.” This is a warning message that does not prevent the DLSw peers from coming up. [CSCdi63658]
- A memory leak in QLLC can result in buffer starvation on the serial interface, and may cause LAPB on the serial interface to become stuck in the RNRSENT state. [CSCdi64333]
- Configuring the **dlsw remote-peer cost** command has no effect on peer selection. All peers displayed in the **show dlsw capabilities** command show equal costs. [CSCdi64537]
- A router running remote source-route bridging where the input explorer queue overflows may crash with the message “%ALIGN-1-FATAL: Illegal access to low address from srb_enq.” [CSCdi65489]
- DLSw FST on the RSP was broken by CSCdi58658, which was integrated into 11.001(004.005). This problem results in a buffer leak in the RSP’s Token Ring interface buffer pool. The Token Ring interface eventually hangs when it runs out of buffers. The output of a **show controller cbus** command shows the number of buffers the interfaces thinks are still available.

The following error messages occur:

```
*Aug 7 11:48:33 mst: %SYS-2-LINKED: Bad enqueue of 60AE6FC0 in queue 60B0EB60 -Process=
"<interrupt level>", ipl= 5 -Traceback= 60110530 6016901C 60169070 60211C8C 600F2E70
600F2B70 600F06D4 601B78E0 60188EB0
boxer% rsym rsp-j-mz.111-5.0.1.symbols Reading rsp-j-mz.111-5.0.1.symbols
rsp-j-mz.111-5.0.1.symbols read in Enter hex value: 60110530
0x60110530:p_enqueue(0x601104d0)+0x60 Enter hex value: 6016901C
0x6016901C:process_enqueue_common(0x60168fb4)+0x68 Enter hex value: 60169070
0x60169070:process_enqueue_pak(0x6016905c)+0x14 Enter hex value: 60211C8C
0x60211C8C:ip_simple_enqueue(0x60211c74)+0x18 Enter hex value: 600F2E70
0x600F2E70:dlsw_lan2fst(0x600f2c1c)+0x254 Enter hex value: 600F2B70
0x600F2B70:dlsw_srb_input(0x600f2ab0)+0xc0 Enter hex value: 600F06D4
0x600F06D4:fs_srb_to_vring(0x600f054c)+0x188 Enter hex value: 601B78E0
0x601B78E0:rsp_process_rawq(0x601b673c)+0x11a4 Enter hex value: 60188EB0
0x60188EB0:rsp_qa_intr(0x60188dec)+0xc4
```

Also, DLSw FST needs to be allowed over a Channel Interface Processor (CIP) LAN interface. [CSCdi65603]

- DLSw may crash when using FST or Direct peer encapsulations on an RSP system and using a CIP interface as a LAN port. The crash will occur due to an access to address 0x00. [CSCdi66239]
- SNA sessions using QLLC over X.25 PVCs do not become active. The following tracebacks are a symptom of this problem:


```
%SYS-2-LINKED: Bad enqueue of 9600E8 in queue 88380. SNA: Alert xxxxx not sent, Focal
point buffer overflowed.
```

[CSCdi66340]
- The router may reload when the second device tries to connect for reverse QLLC with DLSw+ local-switching. [CSCdi67189]

Interfaces and Bridging

- Incoming packets to the Hot Standby Router Protocol (HSRP) MAC address are process-switched, regardless of the route cache status on the interface. [CSCdi44437]
- Serial interfaces may occasionally show the following symptom when the interface cable is changed or the remote end dies and comes back:

```
PC2PR2#sh int s 4/1
Serial4/1 is down, line protocol is down
Hardware is cyBus Serial.
  0 output buffer failures, 0 output buffers swapped out 0 carrier transitions
RTS up, CTS up, DTR up, DCD up, DSR up
```

Note that router reload is not necessary; two workarounds are known. If the first workaround is not successful at bringing up the interface, try the second.

- This workaround was discovered while attempting to observe this problem. It can permit the problem interface to be brought on line without resetting every interface in the cBus complex.

Enter the cBus test mode and select the interface having the problem. Read a portion of the interface processor memory.

This example is for an FSIP interface at 2/0:

```
Router#test cb
RSP diagnostic console program
Enter slot number: [0x0]: 2
Enter interface number: [0x0]:
Command queue for slot 2 is 0x12. CCB is 0xFF50
RSP (? for help) [?]: ri
Enter FSIP Mem starting address [0x0]:
Enter FSIP Mem ending address [0x20000]: 0x20
FSIP Mem 0000: 0001 FFFC
FSIP Mem 0004: 0000 01C6
FSIP Mem 0008: 0000 049A
FSIP Mem 000C: 0000 049A
FSIP Mem 0010: 0000 049A
FSIP Mem 0014: 0000 049A
FSIP Mem 0018: 0000 049A
FSIP Mem 001C: 0000 049A
FSIP Mem 0020: 0000 049A
```

This example is for the HIP at 1/0:

```
Router#test cb
RSP diagnostic console program
Enter slot number: [0x2]: 1
Enter interface number: [0x0]:
Command queue for slot 1 is 0x11. CCB is 0xFF40
RSP (? for help) [?]: ri
Enter IP Mema starting address [0x0]:
Enter IP Mema ending address [0x10000]: 0x20
IP Mema 0000: 7FA2 7FA0 7FA4 0044 0005 0000 0000 0000
IP Mema 0008: 0000 0098 00D0 0080 0032 0000 0000 0000
IP Mema 0010: FFFF 0001 0000 0003 0000 7EA0 7E98 7E90
IP Mema 0018: 0000 0000 0000 0000 0000 0003 0000 00DD
```

- This workaround will reset all the interfaces in the cBus complex.

```
Router(config)#mic rel
```

[CSCdi57573]

- A router running Frame Relay crashes at bridge_enq even when bridging is not configured. [CSCdi63140]
- When passing compressed bridged traffic on HDLC WAN links, many errors of the type “Decompression size error” occur. The router sometimes crashes when processing these packets. This fix causes compressed bridged traffic not to be compressed. The fix is considered temporary until process-level bridging can be made compatible with payload compression. [CSCdi63245]
- In DCE mode, FSIP looks for DCD and DSR up before declaring the Line UP. FSIP should only look for DCD. [CSCdi64735]
- The MIP interface will not come up automatically after a reload. A workaround is to issue a **clear controller t1/e1** command to manually reset the T1/E1 controller. [CSCdi67143]

IP Routing Protocols

- A problem introduced in Releases 10.3(11.1), 11.0(7.3), 11.1(2.3), and 11.2(0.5) causes OSPF to crash when an OSPF external LSA with a nonzero forwarding address exists and the router has a non-OSPF route for the forwarding address. If the non-OSPF route is removed, OSPF crashes when it reprocesses the external LSA. There is no workaround for the problem. However, in general, no more than one routing protocol should be run over the same topology. If you follow this guideline, no non-OSPF route for forwarding address will exist and the router will not crash. [CSCdi61864]
- Shutdown interfaces with IP addresses or static routes that point to down next-hops or other interfaces may cause the IP cache to be partially invalidated more frequently than necessary. This is particularly evident when there are multiple paths. The workaround is to remove IP addresses from down interfaces or remove static routes through down interfaces, or both. [CSCdi62877]
- A problem introduced in Releases 11.0(9.3), 11.1(4.2), and 11.2(0.14) might cause OSPF to fail to install an external route that has no forwarding address. This occurs if the next hop of the path to the ASBR changes and its cost increases. The workaround is to create an external LSA with forwarding address set. [CSCdi64208]
- A directly connected route may disappear from the IPX Enhanced IGRP topology table if the interface that is configured for IPX Enhanced IGRP goes down and comes back up in brief period of time, on the order of 2 seconds. The workaround is to issue the **shut** and **no shut** commands on the interface. [CSCdi65345]

Novell IPX, XNS, and Apollo Domain

- In rare circumstances, NLSP may not report information learned from RIP and SAP. There is no workaround to this problem. [CSCdi45425]
- CSCdi63412 introduced an alignment error, in particular for IPX frames routed from Token Ring networks with multiring enabled. Alignment errors occur in process-switched and certain fast-switched paths. [CSCdi63741]
- CSCdi58363 introduced a problem where NLSP-learned services and SAP-learned services overwrite one another, causing unstable service table information. This is particularly a problem in networks with redundant paths. There is no workaround. [CSCdi63771]
- The SPX spoofing code does not automatically age out old entries from the SPX spoofing table. Over time, this table can grow very large. Some customer sites have reported that when the table is very large, the routers cease to send SPX keepalive acknowledgment spoof packets. At that

time, reloading the router is the only way for SPX spoofing to function again. The workaround is to issue the command **clear ipx spx spoof** on a regular basis to clear the SPX spoofing table. [CSCdi64010]

Protocol Translation

- On PAD-TCP and TCP-PAD translations, changes in PAD parameter settings can incorrectly cause Telnet option messages to be sent on the corresponding TCP connection even if the stream option is set. [CSCdi62987]

VINES

- VINES time server service may get out of synch when the system runs more than 49 days. This is because only the low 32 bits of the internal clock counter are used when VINES computes network time. When network time is out of synch, it is recommended that you either disable VINES time server service for devices running Cisco IOS Releases 10.2 or 10.3, or upgrade to Cisco IOS Release 11.0(11) or 11.1(6). [CSCdi58105]
- VINES clients running an Oracle application program cannot make connection to a server due to packet reordering when **vines route cache** is enabled. A suggested workaround is to use process switching for those applications that cannot process out-of-sequence packets. [CSCdi59059]

Wide-Area Networking

- Bridging IP between two routers through an SMDS network may not work correctly if the IP session originates or terminates in the router, such as in the case of remote source-route bridging or data-link switching. If IP routing is turned on, this is not a problem. [CSCdi61364]
- An RSP-based system running Cisco IOS software that contains the defect documented as CSCdi55969 may start dropping all packets incoming to the input queue of a AIP interface.

The error message “%SYS-2-INPUTQ: INPUTQ set, but no idb, ...” will appear.

A temporary workaround is configuring the interface level command: **hold-queue 750 in** until you are able to reload the router. Remove this configuration after upgrading the software. [CSCdi61629]

- RFC 1577 and LANE applications get blocked due to a difference between VCD known by different parts of the software. This problem has been reported with both applications (LANE, RFC 1577) in Releases 11.0(8) and 11.1(4). [CSCdi61979]
- Error messages similar to the following may appear in devices that contain ATM interfaces:

```
%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
```

```
%SYS-2-MALLOCFAIL: Memory allocation of 52 bytes failed from 0x60298EF4, pool  
Processor, alignment 0
```

These messages most often show up in Cisco 4000 series routers when the routers are being reloaded. The workaround is to put the ATM interfaces in the shutdown state before reloading. [CSCdi62194]

- An error in the AIP microcode introduced in `aip177-2/rsp_aip205-2` causes a race condition in the microcode and commands from the RP/RSP are rejected. When this happens, the following console messages are logged:

```
%ATM-3-FAILCREATEVC: ATM failed to create VC(VCD=1011, VPI=0, VCI=262) on Interface
ATM5/0, (Cause of the failure: Failed to have the driver to accept the VC)
%AIP-3-AIPREJCMD: Interface ATM5/0, AIP driver rejected Teardown VC command (error code
0x8000)
```

[CSCdi62445]

- The **printer** *printer-name* **line number** global command uses the **newline-convert** option as the default. There is no way to get the router to work without either the **newline-convert** or **formfeed** option. [CSCdi63342]
- If a Cisco 7000 router is forwarding a NetBIOS or NetBEUI packet from the ATM (LANE) cloud, the packet might be dropped. This occurs only with protocols that cannot be routed. [CSCdi63540]
- Part of the fix for CSCdi63245 broke bridging on HDLC links. This fix returns the broken code to its original state. [CSCdi64710]
- On the Cisco AS5200, the performance does not scale well when additional asynchronous interfaces are deployed. The symptoms include the Ethernet interface showing input drops and frequent throttles. [CSCdi65706]
- PAP authentication fails when using TACACS+ as an authentication method for PPP. [CSCdi66077]
- LANE does not set up the data direct again after it has been established the first time. This problem was introduced as a result of the fix for CSCdi61979.

Any release containing this bug should *not* be used in sites using LANE. The following releases are affected: 11.0(10.3), 11.1(5.3), 11.1(5.4), 11.2(0.23), and 11.2(0.24).

Note that for Release 11.0, only the Cisco 7000 images (gs7-) will be affected, as the Cisco 4500 and RSP-based systems do not run LANE using Release 11.0. [CSCdi68089]

Caveats for Release 11.1(1) through 11.1(4)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(4). These caveats also apply to Releases 11.1(1) through 11.1(3) (unless otherwise noted).

For more caveats of Release 11.1(4) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(5).

AppleTalk

- MacIP server will not give an IP address to a MacIP client if the next address to give out is currently being use by a genuine IP device. The problem is that the MacIP server does not skip over that IP address and assign the next available address. This causes the process to get stuck. [CSCdi61526]

- According to *Inside AppleTalk*, 2nd Edition, page 8-18, the router should convert NBP BrRq to NBP FwdReq packets. Instead, the router sends NBP LkUp packets for nonextended networks.

Note: For routers that are directly connected to a Phase 1 (non-Phase 2) router in compatibility mode, the **appletalk proxy-nbp network zone** command must be used. This will allow the router to convert the NBP FwdReq to NBP LkUp to the Phase 1 router. [CSCdi61668]

Basic System Services

- Under some conditions, the SEEQ will incorrectly pass up runt Ethernet packets. Previously, these were not checked for, resulting in incorrectly received Ethernet runt packets. [CSCdi55978]
- The error message “RSP-3-RESTART: interface Serialx/y, output stuck” might affect output interfaces on an RSP-based platform. This is seen when bursty traffic is optimum-switched to an output interface with either **fair queue** or **transmit-buffers backing-store** being enabled. A workaround is to disable optimum switching. [CSCdi56782]
- In rare instances, a system might reload during online insertion or removal of slave RSP. [CSCdi57076]
- User should turn backing store ON for slow interface processors. Routers without slow interface processors suffer performance degradation during peak activity. [CSCdi57740]
- An RSP router (Cisco 7500 series or Cisco 7000 with RSP7000) can crash with a “reserved exception” error due to a software error, or else due to an error in the microcode for an interface processor.

More than one problem can generate a similar error message and stack trace, which can make this problem hard to trace. See also CSCdi58999, CSCdi60952, and CSCdi60921. [CSCdi58658]

- AutoInstall does not work in RSP. This is reported only in serial media but the problem exists in LAN media as well. There is no workaround. [CSCdi59063]
- A Cisco 7507 router might reload and indicate SegV exception after receiving a serial interface RSRB explorer. [CSCdi59082]
- HSA (dual RSP in the Cisco 7507 or Cisco 7513) can now coexist with CIP interface processors. [CSCdi60833]
- Use of the **show rmon filter** command in Release 11.1 can cause a router core dump. A workaround is to only use SNMP gets to retrieve the information in the RMON filterTable and channelTable. [CSCdi61957]

DECnet

- A router running DECnet might present “ALIGN-3-SPURIOUS” error messages. This condition occurs only if the adjacency between neighbors expires. [CSCdi60716]

IBM Connectivity

- In extremely rare circumstances the router may crash while removing RSRB peers. This might occur only when running an AGS+ and the CSC1r/CSC2r Token Ring boards. [CSCdi39270]
- When automatic spanning tree (AST) is configured on multiple routers in a high-redundancy topology, a bridge protocol data unit (BPDU) broadcast storm might be triggered. [CSCdi41851]
- A Cisco 4700 router running DLSw+ and SDLC might crash in the SDLC process. [CSCdi48414]

- ACTPU RSP never received by the host in a parallel SDLLC network [CSCdi55142]
- The APPN DLUR router may unbind LU sessions with the DLUS and the downstream node if fixed pacing was enabled on the session bind request from the DLUS. If this is the case, when the user attempts to logon from the downstream device, the USS message 7 with a sense code of 0835 0009 may be displayed. [CSCdi57729]
- On rare occasions, CSNA Virtual Port X/2 may hang in down/down state following a **shut / no shut** command sequence or microcode reload of the channel interface. The workaround is to reload the router. [CSCdi58517]
- A router might crash and display the message “System restarted by bus error at PC 0xD0D0D0D, address 0x0.” The crash happens when using promiscuous TCP peers. The crash occurs when peer structures are deleted (for example, due to transmission line problems or peer routers reloads) while still being used by TCP.

The work around is to define static peers.

Note: CSCdi61278 is a follow-on fix to this problem. [CSCdi58842]

- LNM Resync does not work with Release 10.3(10.2) on a Cisco 7000 if the router is configured for IBM automatic spanning tree support. [CSCdi59890]
- The QLLC features, npsi-poll, and proxy XID do not operate correctly for DLSw+. [CSCdi60002]
- DLSw LLC Ethernet 80d5 bad frames are observed after an LLC retransmission. [CSCdi60102]
- The command **stun schema cnt offset 0 length 1 format hexadecimal** must be entered as **stun schema cnt offset 0 length 1 format hexadecimal** but is saved as **stun schema cnt offset 0 length 1 format hexadecimal**. When the router is reloaded the following error is printed:

```
d7c#conf mem
stun schema cnt offset 0 length 1 format hexadecimal
                                     ^
% Invalid input detected at '^' marker.
```

[CSCdi60992]

- The router crashes and displays the message “System restarted by bus error at PC 0xD0D0D0D, address 0x0.” The crash happens when using promiscuous TCP peers. The crash occurs when peer structures are deleted (for example, due to transmission line problems or peer routers reloads) while still being used by TCP. The work around is to define static peers. If there is a stack trace, action_b() will be one of the entries.

This bug fix is a follow-on fix to CSCdi58842. [CSCdi61278]

- This software fix enables DSPU/FDDI support for end-stations attached directly to FDDI media [CSCdi61351]
- Connections cannot be established when using IBM process-switched features (for example, RSRB/TCP or DLSw+/TCP) because of dropped packets.

The symptom is that “dropped Routed protocol” messages are output when **debug source-bridge error** is enabled. [CSCdi62738]

Interfaces and Bridging

- Turning on **ipx route-cache sse** with microcode version SSP10-12 or SSP10-13 produces a mismatch between the frame length on odd-byte 802.3 IPX packets and the 802.3 length. Novell devices might not recognize these packets, resulting in communication timeouts.

The following three workarounds can be used:

- Turn off padding on process-switched packets using the following command:

no ipx pad-process-switched-packets

- Configure the router for autonomous switching instead of SSE switching using the following commands:

no ipx route-cache sse

ipx route-cache cbus

- Turn off SSE switching using the following command:

no ipx route-cache sse

[CSCdi42802]

- If a Cisco 7000 series router or Route Switch Processor (RSP) has a serial interface on an FSIP that receives several “giant” packets, you might get the error “%DBUS-3-CXBUSERR: Slot x, CBus Error.” Issuing the **show interface** command for the affected slot will show giants occurring. To work around this problem, load an image that contains new microcode: fsip 1-15 or later microcode for the Cisco 7000 series router, and rsp_fsip202-5 or later microcode for the RSP. [CSCdi58194]
- Cisco 7500 (RSP systems) performance is degraded with ISL, fast switching, and access lists applied. The work around is to disable fast-switching on the main interface. [CSCdi59825]
- This defect was introduced in 11.1 (4.0.2) by CSCdi44333. It prevents a channel group on the MIP being created on a Cisco 700 series router in which approximately 32 ports are loaded (plugholes). The router becomes nonresponsive after a channel group is created. [CSCdi64153]

IP Routing Protocols

- If there is a very large set of IP cache entries created because of the same IP route, for example, the default route, a CPUHOG message occurs for the routing protocol when the original route changes and the router clears the related cache entries. Although the cause of the CPUHOG is the IP cache invalidation, the CPUHOG indicates the routing protocol as the guilty one. [CSCdi55725]
- During **show ip ospf**, if OSPF is unconfigured (for example through a different session), the router will crash. [CSCdi58092]
- A router running Enhanced IGRP with Appletalk, IPX, or IP that has input route filters configured may improperly filter routes that it should install. Additionally, if a router running IPX-Enhanced IGRP receives an update containing an external route that was originated by the router itself, the rest of the update will be ignored. There is no workaround to this problem. [CSCdi61491]
- Input queues may become full running IP multicasts. The only way to clear them is to reload the router. [CSCdi61826]
- OSPF corrupts memory and might cause the system to reload. [CSCdi61956]
- A problem introduced in Releases 10.3(12.4), 11.0(9.3), 11.1(4.2) and 11.2(0.14) causes OSPF to crash if there are parallel intra-area paths. [CSCdi62870]

ISO CLNS

- A router running IS-IS will not clean up its adjacency database properly when switched from being a level-1/level-2 router to being level-1 only. A workaround is to manually clear the adjacency database using the **clear clns neighbors** command on the reconfigured router and on all of its neighboring routers. [CSCdi58953]

Novell IPX, XNS, and Apollo Domain

- IPX SPX spoofing might fail when using RPRINTER across a spoofing interface. [CSCdi42806]
- Configuring **no ipx router eigrp autonomous-system-number** may cause the router to reload if there are many SAPs in the router and the SAP table is changing. [CSCdi60174]
- A Cisco 7500 fast-switching IPX traffic might demonstrate excessive CPU utilization in the 90-100% range though forwarding a moderate amount of traffic (less than 5000 pps). Alignment errors in the fast switching path occurring on some specific IPX frames cause this incorrect behavior. [CSCdi61334]
- Defining a static IPX route using the peer address of an IPXWAN neighbor may fail with a message about multicast addresses. The workaround is to avoid using 8-digit IPX internal network numbers which have an odd numbered first byte. A 7-digit or fewer length IPX internal address also will not give this error message. [CSCdi61993]
- Under certain conditions, an IPX packet may be received that has an incorrect IPX length in the IPX header, the CRC is good, and the router processes this packet. However, the system incorrectly pads the packet to the length specified in the IPX header instead of throwing the malformed packet away. [CSCdi63412]
- CSCdi63412 introduced an alignment error for IPX frames routed from Token Rings with multiring enabled. This alignment error is in both process-switched and certain fast-switched paths. [CSCdi63741]
- CSCdi58363 introduced a problem where NLSP learned service and SAP learned services overwrite one another, causing unstable Service Table Information. This is particularly a problem in networks with redundant paths. There is no workaround. [CSCdi63771]

VINES

- VINES clients running Oracle application program can not make connection to a server due to packet reordering when **vines route cache** is enabled. A suggested workaround is to use process switching for those applications that cannot handle out-of-sequence packets. [CSCdi59059]

Wide-Area Networking

- When authentication is not configured and different phone numbers are dialed to add bandwidth for dialer load balancing or multilink PPP, additional links may not be added to the correct group or bundle. This can result in lower than expected performance for dialer load balancing. The result for multilink PPP is no data transfer at all. The workaround is to configure authentication and put the name of the remote system in the dialer map name field. [CSCdi46872]

- Multilink bundles do not disconnect during a low or idle period if more than one link is in the bundle. The load must drop below the threshold for links to disconnect. When the bundle contains only one link, the link may disconnect when the load is low or the link is idle. However, if you configure **dialer load-threshold 1**, links will never disconnect because of idle or low load.
To cause links to disconnect earlier during a low-load or idle period, increase the load threshold. [CSCdi48263]
- IP route configuration commands accept Group-Async interfaces as an interface parameter. This causes crashes in the asynchronous dialer. [CSCdi58223]
- When configuring on a LANE interface a bridge group, the system will not be able to discover Enhanced IGRP neighbors on these emulated LANs. To work around, remove the bridge group. This will allow the router to find neighbors. [CSCdi60268]
- Serial lines with SMDS encapsulation may take SegV catastrophic failures when enabled after reboot. There is no workaround. [CSCdi60761]
- Asynchronous lines on a Cisco AS5200 may become hung and cannot be cleared using the **clear line** command. Only a reload can restore the lines to service. [CSCdi62565]
- RFC 1483 transit bridging is broken. [CSCdi62961]
- The amount of free system memory may decrease when using the command **dialer hold-queue** over an ISDN interface. [CSCdi63716]

Caveats for Release 11.1(1) through 11.1(3)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(3). These caveats also apply to Releases 11.1(1) and 11.1(2) (unless otherwise noted).

For more caveats of Release 11.1(3) and earlier 11.1 releases, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(4).

Access Server

- Asynchronous lines may become stuck in “Carrier Dropped” state when running TACACS+ against a slow TACACS+ server. Only a reload can make the lines usable again. [CSCdi54618]

AppleTalk

- SMRP packets coming in to FDDI interface are dropped. To work around this problem, disable SMRP fast switching on FDDI interface using **no smrp mroute-cache**. [CSCdi57119]

Basic System Services

- Reloading the microcode from ROM on an Interface processor board in a Cisco 7500 series router can cause the system to enter a rebooting loop that requires a system reload for recovery. The ROM-based microcode on the interface processors is only compatible with Cisco 7000 series routers. [CSCdi44138]

- A Cisco 7500 series router can crash if Frame Relay interfaces are active at the same time as MIP channel groups. [CSCdi49868]
- On late model 11.0 and 11.1 RSP system images, Optimum Switching will be disabled upon router reboot. [CSCdi54567]
- A memory leak can occur in some circumstances while running Release 10.3 on a Cisco 7000 series router. The symptoms include small buffers that are created but are not trimmed. This is linked to RSRB and explorers being received with a wrong SNAP type value. [CSCdi54739]
- When using Kerberos authentication for dial-in, the router will crash any time the second dial-in connection is initiated if the user ID contains a slash. It should be noted that it appears that Microsoft prepends the domain information to the user ID and separates the domain and user ID with two slashes. [CSCdi55541]
- Configuring custom/priority queuing on an MBRI interface causes performance degradation. [CSCdi56473]

DECnet

- When DECnet conversion is enabled, discard routes are inserted into the Connectionless Network Service (CLNS) routing table. [CSCdi40503]

EXEC and Configuration Parser

- The **terminal download** privileged EXEC command is omitted from the configuration after it is configured. [CSCdi52164]
- The **write memory** and **copy running-config startup-config** commands now work at privilege level 15. The remaining **write** and **copy running-config** commands still operate at the current privilege level for security considerations. [CSCdi55809]

IBM Connectivity

- When a Synchronous Data Link Control (SDLC) device is reloaded, the connection is not automatically reestablished. To reestablish the connection, issue the configuration commands **shut** and **no shut**. [CSCdi42369]
- A Cisco 4700 router may report intermittent “SYS-2-LINKED” error messages, even though there is no memory shortage. [CSCdi52327]
- Automatic Spanning Tree (AST) is affected in some mixed vendor bridge environments. A hidden option has been added to the **source-bridge spanning** command: **message-age-increment**. This option assists message age count manipulation. This hidden command may be needed in environments where the existing max_age is insufficient for network diameter and max_age is not configurable by vendor bridges. [CSCdi53651]
- Some NetBIOS applications that require a UI frame in response to Add Name Query will not be able to connect using a DLSw peer on demand if the NetBIOS circuit is the initial circuit that triggers the peer-on-demand to connect.

The software fix for this problem passes UI frames through the border peer relay network. [CSCdi54796]

- If two Token Ring interfaces are attached to the same physical Token Ring and either an all routers explorer is generated on that ring or a packet is received with a RIF that indicates that the packet should go back onto the Token Ring it originated on, a bridge loop will be created causing router CPU to rise and ring utilization to increase. The workaround is to issue a **clear rif** command. [CSCdi55032]
- A bug prevents multiple **qllc dlsw** commands from being configured. [CSCdi55749]
- Issuing a **no source-bridge remote-peer** command may cause the router to reload. [CSCdi55919]
- If frames between Token Rings or to or from Ethernet are handled by SRB/SRTLb and one of the local ports is configured for local switching, frames between the local switch port and other LAN ports are handled by DLSw. But when a test frame from a nonlocal switch port is retried, the frame is sent incorrectly to all ports (including nonlocal switch ports) instead of being sent only to local switch ports. Note that when a frame is received from a local switch port, the correct behavior for retries is to send to all ports. [CSCdi56281]
- Connection to DLU (DSPU or APPN) across RSRB may fail when the remote SAP address is not enabled at the destination router. The workaround is to enable the remote SAP address. [CSCdi56660]
- A problem has been discovered with the Cisco 2520, 2521, 2522, and 2523 routers where the router can experience poor Synchronous Data Link Control (SDLC) performance on the low speed asynchronous/synchronous serial ports (interfaces serial 2 through serial 9). The low speed asynchronous/synchronous serial interface has trouble maintaining clock synchronization when configured for all of the following parameters at the same time:
 - **encapsulation sdlc-primary** or **encapsulation sdlc-secondary**
 - **nrzi-encoding**
 - The interface is configured as a DCEThe low speed asynchronous/synchronous serial interface may drop SDLC frames with this configuration. The symptoms of this problem are poor performance and excessive Cyclic Redundancy Check (CRC) errors on the interface (as seen via the **show interface** command).
The fix for this problem requires: hardware version 00000002 *and* a software fix for this defect, which is incorporated into Cisco IOS Release 11.0(9) and 11.1(4), and later.
All Cisco 2520, 2521, 2522, and 2523 routers manufactured before May 24, 1996 are subject to this problem.
To identify whether your router is affected, issue a **show version** command. The hardware revisions that are subject to the problem are “00000000” and “00000001.” Hardware revision “00000002” contains the hardware fix that resolves this problem [CSCdi57040]:

```
cisco 2520 (68030) processor (revision E) with 4096K/2048K bytes of memory.  
Processor board ID 02351913, with hardware revision 00000002
```
- DLSw FST encapsulation does not work over a WAN Token Ring or FDDI. [CSCdi57207]
- An APPN router may unbind an LU6.2 session after receiving an unsolicited IPM with a nonzero next-window size. [CSCdi57730]
- Directed source-route bridge frames with control field of 010 instead of the more usual 000 are dropped. [CSCdi59100]

Interfaces and Bridging

- The MIP T1 and E1 interfaces do not support enhanced online insertion and removal (EOIR/OIR). There is no workaround. This bug is fixed in Releases 11.0(8) and 11.1(4) and later, and requires a minimum of MIP hardware version 1.1 (73-0903-08 Rev A0).

In addition to the hardware requirement, the fix for this bug that is in Release 11.0(8) and 11.1(4) and later releases requires that you allow a minimum of 15 seconds to elapse between OIR events. Removal of one interface counts as one event, and insertion of one interface counts as one event.

If your MIP hardware isn't at least hardware version 1.1, it will *not* EOIR or OIR correctly!

Failure to provide this time for the router to stabilize between OIR events can result in the reset performed for one event corrupting the reset performed for another event, which could require interfaces to be reconfigured or reinitialized manually. This reset requires even more time if additional channel-groups are defined within the router. The time between OIR events should be increased to as much as 30 seconds if three or more MIP cards are fully channelized in the router. While the corruption of this reset activity might occur only occasionally if OIR events are too closely timed, it is *mandatory* to allow the correct interval to guarantee the benefits of EOIR/OIR. [CSCdi46137]

- If you run a MIP EIOR-capable software release with a non-EOIR capable 1.0 hardware version MIP, you will notice that a controller reset is necessary on the MIP for it to work again after adding or removing another card. This controller reset should not be necessary. [CSCdi49807]
- On a Cisco 7000 router with a Silicon Switch Processor, access lists used for packet filtering that contain an entry matching all IP packets followed by two or more entries can cause the router to reload. As a workaround, remove all access list entries following the entry that matches all packets. Doing so will not change the behavior of the access list. [CSCdi50886]

For example, change:

```
access-list 116 permit ip any any
access-list 116 permit tcp any any gt 1023
access-list 116 permit tcp any any eq smtp
```

to:

```
access-list 116 permit ip any any
```

[CSCdi50886]

- While booting a Cisco 7500 router, the FIP FDDI interface might momentarily beacon the ring, causing ring instability. [CSCdi54444]
- If a Token Ring Interface Processor (TRIP) is present in a Cisco 7000 series router, Token Rings that beacon frequently may cause router performance to be degraded. This is not a problem on Cisco 7500 series routers. [CSCdi55758]

IP Routing Protocols

- There is a small delay between the time OSPF marks an LSA as deleted and the time the LSA is actually removed. Within this small window, if OSPF receives an old copy of the LSA which has a higher sequence number, probably from some new neighbors through database exchange, OSPF will be confused and not able to remove the LSA. Customer will observe self-originated LSA stuck in the database. The stuck LSA would be removed automatically when the router regenerate a new instance of the LSA. [CSCdi48102]

- OSPF put incorrect information in the source field for stub route. It prevents BGP to advertise this stub route to peer as the route will not be synchronized. This fix put the advertising router in the source field for stub route and avoid the problem. [CSCdi49377]
- The system may fail when a **no router eigrp as-number** command is issued and there are summary routes present. A workaround is to turn off auto-summary and deconfigure all manual summaries before deconfiguring Enhanced IGRP. [CSCdi57814]
- Attempting to copy an empty startup configuration to the network will cause the router to reload. [CSCdi58040]
- Disabling Optimum Switching on an RSP system has no effect. [CSCdi59203]
- If an Enhanced IGRP candidate default route is overwritten by another protocol, the Enhanced IGRP topology table may be left in a state where the candidate default route will not return to the routing table. A workaround to this problem is to clear all Enhanced IGRP neighbors. [CSCdi59276]

ISO CLNS

- There is no method for altering the transmission rate of IS-IS link state packets in cases where the rate would add undue load to the receiving system. There is no workaround for this problem. [CSCdi54576]
- If IS-IS is running, and a CLNS static route is configured that points to a point-to-point interface on which IS-IS is not configured, and the static route is removed, the system may crash.
A workaround is to either disable IS-IS before removing the static route or enable IS-IS on the interface before removing the static route. [CSCdi56815]
- A router reload may occur when CLNS traffic is fast-switched. This defect affects Releases 10.3(12) and 11.0(9). [CSCdi57629]
- Under situations of extreme load, IS-IS and NLSP may cause packets to be dropped unnecessarily. There is no workaround to this problem. [CSCdi58433]
- If a non-Cisco router running IS-IS on a level-1-only circuit is also sending ES-IS End System Hello (ESH) messages, it is possible for the Cisco router to not recognize the other router for IS-IS.
A workaround is to filter out the ESH packets using the **clns adjacency-filter es** configuration command in conjunction with an appropriate filter set (which should specify a wildcard [**], in the last byte of the address). [CSCdi58621]

Novell IPX, XNS, and Apollo Domain

- If there are more than 42 neighbors on a single LAN interface, IS-IS and NLSP will be unable to establish neighbor adjacencies. The workaround is to limit the number of neighbors to 42 or less. [CSCdi56547]
- IPX SAP table may not accurately reflect SAP entries learned locally if IPX Enhanced IGRP and IPX RIP/SAP is configured at the same time. Some of the SAP entries may show up on the SAP table as Enhanced IGRP derived rather than RIP/SAP derived even when the local LAN where the problem SAP sourced, is not running Enhanced IGRP. [CSCdi56588]
- IPX SNMP request sent to the router accumulate in the input queue and are not processed. This can result in full input queues. [CSCdi57589]

- The router may reload if an interface running IPX is turned off and on immediately thereafter. [CSCdi57683]
- The router may reload when running IPX Enhanced IGRP due to illegal access to memory. [CSCdi57728]
- Under obscure circumstances, some IS-IS and NLSP link-state packets (LSPs) may not be transmitted on some point-to-point interfaces. There is no workaround to this problem. [CSCdi58613]

Protocol Translation

- When doing large file transfers on VTY-asynchronous interfaces that must cross an X.25 network with large RTT, an aggressive TCP implementation can cause return traffic on the VTY-asynchronous interface to be delayed. [CSCdi54905]

Wide-Area Networking

- If the cell burst size is a multiple of 64, the AIP may reset with the error CBUS-3-OUTHUNG: ATM3/0: tx0 output hung (800E = queue full). This incurs a short temporary interruption of the ATM traffic. [CSCdi45984]
- Groups of four ports on Cisco 2511 may have DSR behaving in unison on a single stimulus. Reloading the router is the only workaround. [CSCdi49127]
- When authenticating to a peer using Password Authentication Protocol (PAP), the username password might be sent to a peer that is not authenticated. Currently there is no mechanism to disable outbound PAP. This problem may represent a security risk. [CSCdi49278]
- Frame Relay switching across an IP tunnel does not work if one of the Frame Relay serial interfaces is configured to be **frame-relay intf-type dte**.

In addition, when the serial line is configured to be **frame-relay intf-type dce** or **frame-relay intf-type nmi**, if a **frame-relay intf-type** command is entered after the desired PVCs have been configured, then the router will fail to send the correct LMI Full Status message. [CSCdi52339]

- The number of packet descriptors is hard-coded to 256. Rx count is 192 and Tx count is 64, which can lead to problems with configurations of up to 20 Emulated LANs or many virtual circuit (VC) connections. The router shows normal CPU usage. To view the Pktdescriptor-miss, issue a **show cont atm 0** command. [CSCdi54770]
- With ILMI-resolution of the switch portion of ATM NSAP addresses, an attempt to place a multipoint call to a destination can occur (and with PIM, always will occur) before the switch part of the address is discovered. This leaves the router in a state where it will never place calls to that static map again. To work around this problem, do not use ILMI negotiation. [CSCdi55904]
- In a Cisco 7500 series router running LANE, with approximately 50 emulated LANs configured with bridging, some packets in the incoming queue can be blocked. After some time, the ATM interface will not accept new data. [CSCdi56897]

- If the router receives an incoming ATM SVC call with an SDU size incompatible with the configured MTU on the ATM interface, the router may crash. This problem is present in Releases 11.0(8.3), 11.0(8.4), 11.1(3.1), and 11.1(3.2). If the router is generating the following warning messages in earlier releases, it is likely that the defect will affect them if the images from the releases listed earlier are installed:

```
%ATM-4-MTUCALLMISMATCH: Incoming call has mismatched maximum transmission unit
```

To workaround, reconfigure the remote device with the correct SDU size. [CSCdi57676]

Caveats for Release 11.1(1) through 11.1(2)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(2). These caveats also apply to Release 11.1(1) (unless otherwise noted).

For more caveats of Releases 11.1(2) and 11.1(1), see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(3).

Access Server

- A busy access server sometimes pauses indefinitely, which indicates an invalid address error. This is usually seen in environments where a number of short-duration modem calls are answered. A workaround is to configure **modem ansvertimeout 10**. [CSCdi48100]

AppleTalk

- Adding the command **appletalk virtual-net network-number zone-name** to the configuration of a Cisco 4000 router running Release 11.0(5) can cause the router to reload. [CSCdi51787]

Basic System Services

- When trying to set the MTU on an interface in an RSP chassis (Cisco 7500 series or RSP7000) larger than 8192, the MTU change will fail and report the error message “can’t carve anything.” [CSCdi50133]
- When using the RMON events feature—either through the command line interface, or through SNMP sets—to create rows in the RMON MIB eventTable, the effectiveness of the alarmTable is limited. As long as there are no eventTable entries in the MIB, the rest of the RMON MIB can be used from those feature sets where it is available. [CSCdi50963]
- A router using TACACS+ accounting will experience a slow reduction in the amount of available system memory. A **show memory** command will show many small pieces of memory allocated to AAA AV Last. Eventually (usually over several weeks), the system will become unusable. A workaround is to periodically reboot the router. [CSCdi51197]
- A router containing a CIP card does not become fully operational when Cisco IOS software is loaded. [CSCdi51441]
- Transparent bridging with Cisco 7500 series routers may fail if a frame crosses the HDLC link. [CSCdi52360]

- An attempt to use the RADIUS Access-Challenge feature (used for authentication with some smart-card access systems) will cause a Cisco router running RADIUS to spontaneously reload, indicating a memory allocation failure. [CSCdi55467]
- Under some conditions SNMP queries of the CISCO-ENVMON-MIB can cause the system to reload. This occurs when an SNMP get-request is received that tries to retrieve instance 0 of an object in the ciscoEnvMonSupplyStatusTable. Since the instances of this table start with 1, the correct processing is to return a *noSuchName* error (or *noSuchInstance* if SNMPv2 is used). A workaround is to not use SNMP get-requests that specify instance 0 for objects in the CISCO-ENVMON-MIB. Instead, applications should either use SNMP get-requests starting with instance 1, or else use SNMP get-next-requests or get-bulk-requests. [CSCdi55599]

IBM Connectivity

- A router running RFC 1490 support over Frame Relay does not properly swap the direction bit in the RIF frame. [CSCdi36042]
- When stopping and starting APPN or deactivating links when sessions exist on those links, a bus error may occur. [CSCdi45190]
- When the **dls w icanreach mac-exclusive** and **dls w icanreach mac-address mac-addr** commands are issued to specify a single MAC address to be filtered, all traffic is filtered instead. [CSCdi45773]
- An incorrect timer reference causes explorer frames to be flushed on interfaces, even though the maximum data rate for explorers on any interface does not exceed the maximum data rate for explorers. [CSCdi47456]
- Low-end platforms will cache invalid RIF entries when using any form of the **multiring** command. This can also be seen in the DLSw reachability cache and possible loops with LNM. [CSCdi50344]
- RSRB will not declare that a peer is dead until keepalive times out. Therefore, for RSRB to detect the dead peer so that the ring list can be cleaned up properly, the keepalive value should be set as small as possible. [CSCdi50513]
- Removing DLSw configuration by configuring **no dls w local-peer** and adding the DLSw configuration back can cause a memory leak in the middle buffer. [CSCdi51479]
- Applying a **source-bridge output-lsap-list** to a Token Ring interface when **source-bridge explorer-fastswitch** is enabled may cause packets permitted by the output-lsap-list to be dropped. The workaround is **no source-bridge explorer-fastswitch**. [CSCdi51754]
- When a very large number of I-frames is sent by an end station to a DLSw router at the same instant, the following message may appear on the console:


```
DLSW:CPUHOG in CLS background, PC=0x60549f3c
```

Because the CPU is being occupied by the CLS background process for a period of time, protocols that involve polling may lose their connections because of poll starvation. [CSCdi52382]
- Ethernet sessions do not come up or drop. The LLC frames are bad after a retransmission. [CSCdi52934]

- The LAN Network Manager (LNM) fails to link to the router's source bridge after the Token Ring interface is shut down on the remote router. The **show lnm bridge** command continues to display active link to the LNM. This problem does not occur when bridges are linked locally to the LNM.

The workaround is to remove the **source-bridge** command from the Token Ring interface and configure it back in. [CSCdi53954]

- When configured to use the DSPU feature, the router may crash during deactivation of multiple downstream physical units. [CSCdi54114]
- A router may crash when DSPU debugging is enabled on a Cisco 4500 or Cisco 7500 router. [CSCdi54277]
- Very small SRB bridged frames on a large FDDI ring are not properly stripped from the ring and continue to loop indefinitely. [CSCdi54594]

Interfaces and Bridging

- The concurrent routing and bridging (CRB) feature does not bridge IP traffic if the destination IP address is internal to the router. Also, IP packets with a destination IP address internal to the router are not responded to. [CSCdi48117]
- Transparent bridge ports in the blocking state do not respond to ARP broadcasts. This problem is acute only when there is no other IP route to the blocking port. A workaround is available in the form of a static ARP entry in the host. [CSCdi51444]
- A problem in the MEMD carve code on the Cisco 7000 can cause bandwidth considerations to be ignored. This might result in nonoptimal MEMD carving. [CSCdi52227]
- A router may pause indefinitely when the configuration command **encapsulation ppp** is entered for Async-Group Interfaces. The configuration command **async mode dedicated** has the same effect. [CSCdi53185]
- Asynchronous TTY lines on Cisco 2509 through Cisco 2512 devices sometimes stop answering new modem calls. The **show line x** command output shows the line with modem state in Idle and Hanging-up. A workaround is to configure **sessiontimeout 0** for asynchronous lines. [CSCdi54196]

IP Routing Protocols

- Running multiple Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) autonomous systems might consume all available memory in the router. [CSCdi36031]
- Multicast fast-switching is not functional for ATM subinterfaces. A workaround is to configure **no ip mroute-cache** on the incoming subinterface. [CSCdi51178]
- Unconfiguring OSPF can cause the router to reload. [CSCdi51283]
- If two IP-Enhanced IGRP autonomous systems are configured, and an interface address is changed so that the interface moves from one autonomous system to the other, Enhanced IGRP will fail to operate on that interface. The workaround is to delete the IP address (using the **no ip address** command) before configuring the new address. [CSCdi52078]
- Under certain conditions, Enhanced IGRP may stop transmitting packets. This may manifest itself as large numbers of routes repeatedly Stuck-In-Active. The workaround is to unconfigure and restart Enhanced IGRP, or reload the system. [CSCdi53466]

- Regular expressions longer than 59 characters in the **ip as-path access-list** configuration command will cause the router to reload. [CSCdi53503]
- Enhanced IGRP will stop working on an interface if the interface goes down for some reason and then comes back up. There is no workaround to this problem. [CSCdi53903]
- Because of an uninitialized variable, multipoint GRE tunnels in Releases 10.3 and 11.0 may allow non-IP network protocols to be forwarded to all endpoints of the tunnel. This can lead to the perception that non-IP protocols are capable of being routed over the multipoint tunnel in these versions. Only IP multipoint tunnels are supported in these versions. In Release 11.1, routing IPX over GRE multipoint tunnels does not function. [CSCdi54192]
- When booting a Cisco 7000 series router with a Release 11.1(2.2) or 11.1(2.3) software image, the router will crash. To work around, deconfigure **ip sd listen** on the interfaces. [CSCdi55369]

ISO CLNS

- If two routers running Intermediate System-to-Intermediate System protocol (IS-IS) are connected via multiple point-to-point links and one of the links fails in only one direction, it is possible for traffic to be sent down the failing link and subsequently lost. This is because of a deficiency in the IS-IS protocol specification. There is no workaround to this problem. [CSCdi48351]
- ISO-IGRP fails to install parallel routes into the CLNS prefix table under certain conditions. [CSCdi50714]

Novell IPX, XNS, and Apollo Domain

- A Cisco 4000 router running Enhanced IGRP for IPX may generate CPU-HOG messages for the IPX SAP process. [CSCdi39057]
- Clearing the SPX spoofing table with either the **clear ipx spx-spoof** command or by removing the **ipx spx-spoof** command from the last interface left spoofing may cause a system reload. [CSCdi53070]
- The system may reload if NLSP is enabled and SNMP queries are done of the NLSP neighbor table. [CSCdi54546]
- The default for **ipx eigrp-sap-split-horizon** needs to be changed to off. [CSCdi55576]

Wide-Area Networking

- Under certain conditions, the router can reload with the message “System was restarted by error - Illegal Instruction, PC 0x300D646.” This problem is related to ISDN. There currently is no workaround. [CSCdi45085]
- With synchronous dial-on-demand routing (DDR) the dialer does not respect the enable-timeout before trying a second dialer map. The dial command is lost when the modem is initializing. [CSCdi46421]
- Systems using the ATM Interface Processor (AIP) card may restart with the error message “System was restarted by error - Illegal Instruction, PC 0x0.” [CSCdi47523]

- A Cisco 7000 with two ATM interfaces running RFC 1577 ARP server will not register its own IP address. There are two workarounds:
 - Specify the full NSAP address of the ARP Server interface, using the **atm nsap-address nsap-address** command, instead of just the ESI portion.
 - After boot-up, issue a **no atm arp-server** command and then reissue the **atm arp-server** command. [CSCdi50592]
- The dialer fails to bring up an additional BRI interface when both BRI B-channels are active and the **dialer load-threshold load** is exceeded. [CSCdi50619]
- Under some unknown circumstances, a Cisco 4000 series router with MBRI will stop transmitting on an ISDN interface. Only a reload of the router can correct this. [CSCdi50628]
- When bridging between a Cisco 7500 and an ISDN router running Cisco IOS software, data is not successfully passed if multilink PPP is used. [CSCdi51813]
- If the LAN Extender (LEX) interface in a router running Cisco IOS Release 11.1(1) or 11.1(2) is shut down, and a **no shutdown** command is issued on the interface, the LEX interface will not come up. To recover, reboot the router or run Release 11.0. [CSCdi52515]
- Using multidrop lines on a 5ESS ISDN switch is not recommended. If used, they will have SPIDs. SPIDs are sent out BRI0 only, so on a router equipped with an MBRI, lines other than BRI0 will not be able to place calls. The workaround is to get point-to-point lines from the telco. [CSCdi53168]
- The DEC Spanning Tree protocol does not function properly in a LANE environment. To work around, use IEEE Spanning Tree protocol. [CSCdi53442]
- A heavily loaded X.25 link that is experiencing congestion can, under rare conditions, enter a state where it oscillates between sending a RNR and a REJ. [CSCdi55677]

Caveats for Release 11.1(1)

This section describes caveats (possibly unexpected behavior) of Cisco IOS Release 11.1(1). For more Release 11.1(1) caveats, see all the preceding caveat sections.

Only serious caveats are described in these release notes. For the complete list of caveats against this release, access CCO or use the Documentation CD-ROM as described in the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of this document.

All the caveats listed in this section are resolved in Release 11.1(2).

Access Server

- The **service hide-telnet-address** command does not hide the Telnet address in a connection closing message. The **busy-message** command does not suppress a connection closing message. [CSCdi47740]

Basic System Services

- Available memory will slowly decrease on a router that is bridging IP and that has more than one interface with the same IP address. [CSCdi44023]
- A Cisco 7500 that is fast switching source-route bridging (SRB) explorers, fast switching IP multicasts, or bridge-flooding packets might crash with a SegV exception error message and a stack trace that ends in the `rsp_fastsend()`.

A workaround is to disable fast switching of IP multicasting, or fast switching of SRB fast explorers by using the **no source explorer-fastswitch** command. Another possible workaround is to remove or add an IP card, particularly of a different media type. [CSCdi45887]

- Under heavy load conditions, a Cisco 2509 through Cisco 2512 access server might pause indefinitely and report a bus error. [CSCdi47190]
- The *alarmValue* RMON MIB object always returns the sampled value at the end of the sampling period. This is incorrect behavior when the *alarmSampleType* is *deltaValue(2)*. [CSCdi48677]
- After some time running with RADIUS configured, the router will no longer successfully receive Ethernet packets, and communication will stop. A **show interface** command indicates that the interface on which RADIUS responses are received has a full input queue. [CSCdi49072]
- RADIUS only works 255 times, after which it fails to recognize responses to the requests that the router sends. [CSCdi49412]

DECnet

- DECnet Phase IV-to-Phase V conversion might introduce incorrect area routes into the ISO Interior Gateway Routing Protocol (IGRP), if DECnet L2 routes exist on the DECnet side. These area routes appear as “AA00” and are propagated to other routers. [CSCdi47315]

IBM Connectivity

- When source-route transparent (SRT) bridging is configured on the router, calls to management functions related to source-route bridging (SRB) may not work correctly. [CSCdi42298]
- When a front-end processor (FEP) initiates a Qualified Logical Link Control (QLLC) connection, a virtual circuit is established, but the exchange identification (XID) negotiation never proceeds to completion. The router sends XID responses as commands, rather than as responses. [CSCdi44435]
- When two or more routers are connected to the same Token Rings, and each uses source-route bridging (SRB), a station on one of the rings might choose a non-optimal route with a path through both routers. In typical (large) networks, this behavior might result in explorer storms as well as suboptimal routes. [CSCdi45116]
- A router might crash if running QLLC and using remote source-route bridging (RSRB) over a serial line to provide the Logical Link Control, type 2 (LLC2) connection from QLLC to an end station or host. The crash only occurs if multiple changes are made to the encapsulation type on the RSRB serial line. [CSCdi45231]
- A router might report inaccurate traffic statistics. In particular, nonbroadcast frame counts might be incorrect if the router is acting as a source bridge on a Token Ring. [CSCdi46631]
- Explorers are not forwarded to the CIP CSNA feature from DLSw+. [CSCdi47239]
- When an IP peering protocol is in use in the router (for example, RSRB, STUN, or BSTUN), CLS DLUS (such as APPN and DSPU) may have difficulty establishing LLC2 sessions over RSRB virtual interfaces when the LLC2 path is bridged SRB only and does not traverse an IP cloud local to this router. [CSCdi47301]
- Using a CIP with CSNA configured in a Cisco 7500 series router causes cBus complex restarts and output stuck messages for the CIP virtual interface. [CSCdi47536]
- If a router receives a source-route bridging (SRB) packet with bit 2 of the routing control field set, the router might send back a bridge path trace report frame to a group address, instead of to the source of the original frame. This behavior may cause congestion. [CSCdi47561]

- When using APPN/dependent LU requestor (DLUR) on a Cisco 4500, Cisco 4700, or Cisco 7500 router, a DLUR may accept only one downstream PU for dependent session activation at a time. [CSCdi47584]
- A downstream physical unit (DSPU) sometimes retries connecting to the host too rapidly, with as many as sixty tries per second, flooding the host with exchange identification (XID) packets. This problem causes the NetView log to get congested and run out of storage, which might bring down the host. [CSCdi47803]
- If DLSw with FST is configured, an LLC2 session should not be set up. [CSCdi47888]
- The DLSw SDLC ABM bit is not turned off in the first exchange identification (XID) packet sent to an SDLC station. [CSCdi47942]
- When proxy explorer and proxy NetBIOS are configured, looped RIFs might be created. The only workaround is to disable the feature. [CSCdi48577]
- During cross-domain file transfers via Data Link Switching Plus (DLSw+) on a Logical Link Control (LLC) connection, frames might be sent out of sequence. This problem can cause a receiving Physical Unit 4 (PU 4) or Physical Unit 5 (PU 5) to disconnect. [CSCdi48915]
- When a router running DSPU over Frame Relay in communication with a frame device breaks the session, it does not try to reconnect after a disconnect mode response is received. [CSCdi49044]
- When attempting to run APPN over Frame Relay, the router may generate the following error and traceback messages: “APPN-6-APPNSENDMSG,” “APPN-7-APPNETERROR,” and “SYS-2-BADSHARE.” [CSCdi49162]
- On Cisco 7000 series routers installed with a CIP, the commands **csna**, **llc2**, **offload**, and **show extended channel tcp-stack** fail after a router reload or reboot. To recover, reboot the microcode. [CSCdi49312]
- The router crashes when a get many command is issued for the *ciscoDlswTConn* MIB object from a management station. [CSCdi49393]
- Accessing the object *ciscoDlswVirtualSegmentLFSize* returns a value of 17800 instead of the valid value of 17749 defined in the MIB. [CSCdi49435]
- Zero is returned for SNMP get commands on *ciscoDlswActiveCircuits* and *ciscoDlswCircuitCreates*, even though circuits are open through DLSw. [CSCdi49441]
- The number of downstream PUs that the Cisco IOS software supports should be increased from 256 to 1024. [CSCdi49448]
- Sessions using an APPN Connection Network over FDDI that also use the router as a member of the FDDI connection network will fail to activate. [CSCdi49560]
- Connections to a host cannot be established from a DSPU using virtual telecommunications access method (VTAM) through an IBM 3172 Channel Interface Processor (CIP). [CSCdi49872]
- If peer A and peer B are DLSw priority peers (the keyword **priority** is on the remote peer definition), and peer A is reloaded, peer B may crash. [CSCdi50155]
- Peer-on-Demand peers (peers that learn of each other through Border Peers) do not connect. The Cisco IOS software should be enhanced to add the options **inactivity timeout** and **If lfsize** to the **dlsw peer-on-demand-defaults** command. [CSCdi50574]

Interfaces and Bridging

- On a Cisco 4500 router, if you issue the **no shutdown** command on a Fiber Distributed Data Interface (FDDI) interface, the router will reboot. [CSCdi42429]
- The Versatile Interface Processor (VIP) does not support enhanced online insertion and removal (EOIR) in Release 11.1(1). Do not online insert or remove any card on a Cisco 7000 or Cisco 7500 router if it has VIP installed and is running Cisco IOS Release 11.1(1). VIP EOIR is supported in Release 11.1(2). [CSCdi45136]
- When a Cisco 7000 router Ethernet interface is the root of a spanning tree and UDP flooding is configured with turbo flooding, packet loops occur. The workaround is to disable turbo flooding. [CSCdi45659]
- Transparent bridging and the Hot Standby Router Protocol (HSRP) cannot be simultaneously enabled on Fast Ethernet interfaces. Random crashes occur, which can result in image or memory corruption. [CSCdi48646]
- Bridging from a Token Ring through an ATM cloud via RFC 1483 AAL5-SNAP encapsulation back to a Token Ring does not function because of an incorrect CTL/OUI. There is no workaround. [CSCdi49151]

IP Routing Protocols

- If a router is incorrectly configured with an autonomous system (AS) placed in a confederation it is not part of, the confederation information within the AS path will be incorrectly propagated. The workaround is to configure the router correctly. [CSCdi46449]
- Next Hop Resolution Protocol (NHRP) may cause memory corruption when attempting to send an NHRP purge packet. Specifically, if the network layer route to the destination no longer would cause the purge packet to be transmitted out the nonbroadcast multiaccess (NBMA) interface, NHRP attempts to modify low memory. On some systems, this behavior can cause the system to reload. [CSCdi47623]
- Packet corruption can occur when IP packets are fast-switched from ATM interfaces to Token Ring interfaces configured with the **multiring** command. [CSCdi49734]
- Multicast fast switching is not functional for ATM subinterfaces. A workaround is to configure **no ip mroute-cache** on the incoming subinterface. [CSCdi51178]

ISO CLNS

- ISO Interior Gateway Routing Protocol (IGRP) will not work when interoperating between Motorola processor-based Cisco routers (older routers such as MGS, AGS+, or Cisco 7000) and millions of instructions per second (mips) processor-based Cisco routers (later routers such as the Cisco 4500, Cisco 4700, or Cisco 7500). [CSCdi44688]
- Issuing a CLNS ping to one of the router's own address will cause the router to reload if **debug clns packet** is on. The workaround is to not have this particular debug on if you need to ping to one of the router's own addresses. [CSCdi50789]

Novell IPX, XNS, and Apollo Domain

- Cisco 1003, Cisco 1004, and Cisco 1005 routers advertise all IPX services with a SAP hop count of zero. Both dynamically learned and static SAPs are sent out every interface with a zero hop count, which makes remote services invisible to Novell servers connected directly to the router (for example, on the LAN interface).

Clients on LANs with no server can connect correctly, because the router answers the GetNearestServer request. However, whenever a Novell server resides on the same LAN as the client, the client will not be able to connect to any remote services.

Use the **show ipx servers** command to determine whether any SAPs are being seen with zero hop count from the neighboring router. [CSCdi46488]

- When an Enhanced IGRP route is advertised back into RIP, the delay within the Enhanced IGRP cloud is not taken into account properly in the ticks value of the route when it is redistributed into RIP. The RIP-advertised route appear to be closer than it really is. [CSCdi49360]
- When an interface goes down, services that are not learned over that interface are marked as down. This behavior might cause excessive SAP packet generation because packets are flooded first as down, are then learned, and are finally flooded again as new. [CSCdi49369]
- If IPX Enhanced IGRP is running, the command sequence **interface serial / no ipx network / no ipx routing** may cause the router to reload. [CSCdi49577]

TCP/IP Host-Mode Services

- Under unknown circumstances, random lines on an ASM will pause indefinitely in Carrier Dropped state. The only way to clear the line is to reload the ASM. [CSCdi44663]
- Opening hundreds of simultaneous Telnet connections from a TTY or VTY can cause the software to reload with a watchdog timeout error. [CSCdi47841]

VINES

- VINES servers located downstream might unexpectedly lose routes that were learned via Sequenced Routing Update Protocol (SRTP). This behavior results from improper handling of network sequences numbers by the system. Issuing a **clear vines neighbor *** command or disabling SRTP are suggested workarounds. [CSCdi45774]
- The system reloads when it receives badly formatted Interprocess Communications Protocol (IPC) packets from the VINES application software Streetprint. Streetprint uses reliable messages that can span up to four VINES IP packets. The VINES IPC length field should contain the number of bytes that follow the long IPC header in a data packet, but Streetprint sets the IPC length in each IPC message to the total number of bytes of all IPC messages. The Streetprint vendor is working to resolve this problem. A workaround that validates the IPC length and drops IPC packets if they are longer than the maximum allowed IPC length (5800 bytes) should be available in an early 11.1 maintenance release. [CSCdi47766]

Wide-Area Networking

- An X.25 interface might hang if the Link Access Procedure, Balanced (LAPB) layer gets stuck in the RNRsent state. This might occur if virtual circuits (VCs) receive encapsulated datagram fragments that are held for reassembly, and the number of these fragments approaches the

interface input queue count. The LAPB protocol will not exit the RNRsent state until the number of held buffers decreases. This condition can be cleared if a **shut /no shut** is performed on the interface, or if the other end of the LAPB connection resets the protocol. [CSCdi41923]

- If a new permanent virtual circuit (PVC) is defined on an ATM Interface Processor (AIP) when existing switched virtual circuits (SVCs) and PVCs are already defined, an interface reset might occur with a subsequent restart of all SVCs. [CSCdi43779]
- When IP traffic is fast-switched from an AIP onto an FDDI interface, an extra byte added to the end of the packets. [CSCdi44580]
- When ATM is running on a Cisco 7000, memory corruption may occur. [CSCdi45540]
- Running X.25 Defense Data Network (DDN) encapsulation on a Cisco 2500 serial port might cause the router to reload. This problem appears to be the result of mixing X.25 switching and X.25 DDN. A workaround is to shut down the serial interface. [CSCdi45673]
- Under certain conditions XOT data might be delayed by the router. [CSCdi45992]
- Routers with ISDN BRI interfaces that use the **isdn switch-type basic-net3** command may experience BRI port failures due to all network layer control blocks (NLCBs) being used and never released. Once all NLCBs and call control blocks (CCBs) are used and hung, a reload of the router is required to use the BRI interface. The problem does not apply to ISDN Primary Rate interfaces (PRIs).

A possible workaround is to set the **dialer idle-timeout** value on the BRI routers connected to NET3 switches higher than the timeout value of the other router or routers connecting via ISDN. This workaround assumes the other router or routers do not have BRIs connected to NET3 switches, because they would have the same problem. This workaround also requires knowledge of the **dialer idle-timeout** value configured on the other router or routers.

The problem does not occur if the call hangup is initiated by the ISDN network rather than the BRI router connected to a NET3 switch.

Releases 11.0(2.1), 10.3(6.1) and 10.2(8.5) were the first software versions to exhibit the problem. [CSCdi46668]

- A Cisco 4000 series router with ISDN BRI interfaces can run out of timer blocks and crash. Use the **show isdn memory** command to see if memory is not being freed. [CSCdi47302]
- In some failed CHAT script operations over asynchronous interfaces, data can be left in an inconsistent state, sometimes causing a reload to occur during later operations. [CSCdi47460]
- Under some unknown conditions, an ISDN B Channel may fail to disconnect. The PPP keepalive feature detects the partially disconnected link and repeatedly reports “exceeded max retries taking LCP down” every few minutes. This defect was introduced in software version 11.0(3.2). [CSCdi48111]
- When packets are lost because of hold queue overflow or line errors, multilink PPP may incorrectly discard packets that were properly received.

To prevent this behavior, remove the cause of the line errors or increase the hold-queue size. [CSCdi48424]

- If parallel connections are made to a dialer group or ISDN interface that use the same IP address and a neighbor route is necessary, then the neighbor route is added for the first connection only. Subsequent connections will detect that a route already exists and do not add another route. This situation works until the first connection closes and its neighbor route is removed. The other connections remain but no neighbor route is installed for them. This problem applies to parallel connections not to multilink bundles. [CSCdi49007]

- When booting a router on which all ATM interfaces are in a **no shut** state, you need to issue a **shutdown** and **no shutdown** command sequence on one of the ATM interfaces to make Service-Specific Connection-Oriented Protocol (SSCOP) fully initialized and to allow ATM signaling to function properly. [CSCdi49275]
- If Cisco's enhanced Terminal Access Controller Access Control System (TACACS+) is enabled, you cannot specify inbound authentication on the Point-to-Point Protocol (PPP) authentication configuration line. [CSCdi49280]
- Nondefault IPX encapsulation on an ATM subinterface using the **ipx encaps xxx** command does not work. To configure the nondefault encapsulation, use the **ipx network network encapsulation encapsulation-type** command. [CSCdi49729]
- Cisco IOS Release 11.0(6), Release 11.1(2), and Catalyst 5000 ATM software Release 2.1 and later contain a fix for an Emulated LAN defect. If you deploy Release 11.0(6), Release 11.1(2), or Catalyst 5000 ATM software Release 2.1 or later releases in your network, and you use Emulated LAN bridging features, you must upgrade the Cisco IOS software in all routers and Catalyst 5000 switches in your network to use a version of Cisco IOS software that contains the fix. Failure to upgrade all devices in a particular Emulated LAN will result in interoperability problems between Cisco devices.

If you choose to continue to use Cisco IOS Release 11.0(5), Release 11.1(1) or earlier releases, the Catalyst 5000 requires ATM software Release 1.1. [CSCdi49790]

- IPX packets fast switched by a Cisco 4500, Cisco 4700, or Cisco 7500 series router to an Emulated LAN (LANE) subinterface using SAP, SNAP, or Novell-Ethernet encapsulation may be dropped by the receiving IPX server or client because of a mismatch between the length indicated in the Ethernet packet header and the actual packet length. To work around, disable IPX fast switching on the ATM interface with the **no ipx route-cache** command. [CSCdi50312]
- If a backup interface is brought up, a floating static route points through the backup interface to the remote node and network. When the original interface comes back up, the floating static route is removed. The backup interface will not see any traffic, and an idle timeout will bring down the backup connection.

If, however, the original interface comes back up before the backup connection is complete, the floating static route will have been removed and a neighbor route will be added to the peer address. This route will carry routing updates to the peer over the backup connection and thus reset the idle timeout with each packet. As a result, the backup interface will never disconnect. This behavior was added with Release 11.0(3). [CSCdi50489]

- Fast switching IP traffic may fail from an ATM Interface Processor (AIP) onto an FDDI with RIF presence. [CSCdi50609]
- International calls placed using the Australian Primary Rate switch type of primary-ts014 do not tag the format of the called address field correctly. As a result, calls to locations outside of Australia are rejected as unassigned. [CSCdi50927]
- Cisco LANE clients do not interoperate with non-Cisco broadcast-and-unknown servers (BUSs) that deliver data to the client on Multicast Send virtual channel connections (VCCs). Packets sent to the client on the Multicast Send VCC are discarded. In addition, the error message "%LINK-2-NOSOURCE: Source idb not set" may appear when these packets arrive. There is no workaround. [CSCdi50945]

Microcode Software

For Cisco 7000 and 7500 series platforms, microcode software images are bundled with the Release 11.1 system software images (features sets). The only exceptions are the Channel Interface Processor (CIP) microcode and the Versatile Interface Processor (VIP) microcode. CIP microcode is unbundled in all system software images. VIP and VIP2 microcode is contained only in feature sets that have “VIP” in the feature set name.

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 onto all the interface processor boards.

Table 16 lists the microcode versions bundled into Release 11.1(17) software images for the Cisco 7000 series platforms.

Table 17 lists the microcode versions bundled into Release 11.1(17) software images for the Cisco 7500 series platforms.

Note For the Cisco 7000 series, all boards must use the Level 10 (or greater) microcode that is bundled (except CIP) with the system image.

Table 16 Current Microcode Versions for the Cisco 7000 Series

Processor or Module	Current Bundled Microcode Version	Minimum Version Required
AIP (ATM Interface Processor)	10.25	10.12
EIP (Ethernet Interface Processor)	10.2	10.1
FEIP (Fast Ethernet Interface Processor)	10.7	10.2
FIP (FDDI Interface Processor)	10.2	10.2
FSIP (Fast Serial Interface Processor)	10.19	10.12
HIP (HSSI Interface Processor)	10.3	10.2
MIP (MultiChannel Interface Processor)	12.2	11.4
SP (Switch Processor)	11.15	11.14
SSP (Silicon Switch Processor)	11.15	11.14
TRIP (Token Ring Interface Processor)	10.4	10.3
VIP (Versatile Interface Processor) ¹	21.40	21.9

¹ VIP microcode resides within the Cisco IOS software; it is not “bundled” in.

Table 17 Current Microcode Versions for the Cisco 7500 Series

Processor or Module	Current Bundled RSP Microcode Version	Minimum Version Required
AIP (ATM Interface Processor)	20.18	20.5
EIP (Ethernet Interface Processor)	20.6	20.1
FEIP (Fast Ethernet Interface Processor)	20.6	20.1
FIP (FDDI Interface Processor)	20.1	20.1
FSIP (Fast Serial Interface Processor)	20.8	20.1
HIP (HSSI Interface Processor)	20.2	20.0
MIP (MultiChannel Interface Processor)	22.2	20.3
POSIP (Packet over SONET OC-3 Interface Processor)	20.0	20.0
RSP2 (Route Switch Processor) ¹	N/A	200.0
TRIP (Token Ring Interface Processor)	20.1	20.0
VIP (Versatile Interface Processor) ¹	21.40	21.9
VIP2 (second-generation Versatile Interface Processor) ¹	21.40	21.40

¹ RSP2, VIP, and VIP2 microcode reside within the Cisco IOS software; they are not “bundled” in.

Note RSP2 microcode was introduced in Release 11.1(2).

Note POSIP and VIP2 microcode were introduced in Release 11.1(5).

Channel Interface Processor (CIP) Microcode

Beginning with Cisco IOS Release 11.1, the CIP microcode is no longer bundled with the Cisco IOS software image.

Also note that to use the IBM channel attach features in Cisco IOS Release 11.1, you must have Flash memory installed on the Route Processor (RP) card and 8 MB RAM installed on your CIP card.

See the “Important Notes” section for more information about CIP microcode.

Microcode Revision History (for Cisco 7000 Series Platforms)

This section describes each revision of microcode for Cisco 7000 series routers using a route processor/silicon switch processor (RP/SSP) or route processor/switch processor (RP/SP) combination. The descriptions list the caveats that were fixed in each microcode revision. This

section does not describe RSP microcode. For descriptions of each revision of RSP microcode, which is used with Cisco 7500 series routers and Cisco 7000 series routers using an RSP7000, see the next section, "Route Switch Processor (RSP) Microcode Revision History."

ATM Interface Processor (AIP) Microcode Revision Summary

AIP Microcode Version 10.13

Modification

AIP Microcode Version 10.13 fixes the following:

- Ping between two routers fails intermittently with SMDS configuration. [CSCdi45807]

AIP Microcode Version 10.14

Modifications

AIP Microcode Version 10.14 fixes the following:

- The AIP cannot be configured to issue idle cells instead of unassigned cells. [CSCdi48069]
- The ATM Interface Processor (AIP) used with a RSP processor may stop receiving data if OAM cells are inserted in the incoming cell flow. [CSCdi55512]
- New AIP microcode in 11.1(4.0.1) (aip177-1 and rsp_aip205-1) breaks ATM on RSP. [CSCdi60561]

AIP Microcode Version 10.15

Modification

AIP Microcode Version 10.15 fixes the following:

- Sometimes a race condition occurs, and commands from a Route Processor (RP) or Route Switch Processor (RSP) are rejected. When this condition occurs, the following console messages are logged [CSCdi62445]:

```
%ATM-3-FAILCREATEVC: ATM failed to create VC(VCD=1011, VPI=0, VCI=262) on Interface ATM5/0, (Cause of the failure: Failed to have the driver to accept the VC)
%AIP-3-AIPREJCMD: Interface ATM5/0, AIP driver rejected Teardown VC command (error code 0x8000)
```

AIP Microcode Version 10.16

Modifications

AIP Microcode Version 10.16 fixes the following:

- AIP microcode version 20.8 may cause the AIP to lock into a state where it transmits corrupted packets, causing debug atm error showing "ATM(ATM9/0.1): VC(1) Bad SAP ..." at the receive side of the ATM VC. The transmission of data is usually affected in one direction only. The

problem may occur when the input traffic exceeds the average rate configured on the ATM VC, when the bandwidth of the incoming interfaces exceeds the average rate on the outgoing VC or SVC.

A workaround is either to downgrade the AIP microcode to aip20-6 or to upgrade the AIP microcode to rsp_aip205-5, or aip20-9 when available. A short term workaround is **clear int atm 5/0** on the transmit side. [CSCdi67812]

The same problem applies for aip10-15 on RP based platforms.

- ATM traffic is lost during an online insertion or removal (OIR) event of an RSP4 card. [CSCdi66076]

AIP Microcode Version 10.17

Modifications

AIP Microcode Version 10.17 fixes the following:

- Online insertion and removal (OIR) of a VIP2 brings down ATM in a Cisco 7507 router. [CSCdi75659]
- Sometimes the AIP hangs. [CSCdi60941]
- The AIP microcode does not support configurable LBO settings. [CSCdi72800]
- The AIP sometimes fails to set up a DS3 scramble. [CSCdi57924]

AIP Microcode Version 10.18

Modification

AIP Microcode Version 10.18 fixes the following:

- The VPI/VCI hash lookup in AIP is not optimal. [CSCdi69673]

AIP Microcode Version 10.19

Modification

AIP Microcode Version 10.19 fixes the following:

- LANE does not support 9K MTU for Ethernet ELAN packets. [CSCdj06005]

AIP Microcode Version 10.20

Modification

AIP Microcode Version 10.20 fixes the following:

- AIP does not show ATM packets dropped because of traffic shaping. [CSCdi72246]

AIP Microcode Version 10.21

Modification

AIP Microcode Version 10.21 fixes the following:

- The following error messages are seen:
%AIP-3-AIPREJCMD with error code 0x8000
%SYS-3-CPUHOG
[CSCdj20667]

AIP Microcode Version 10.22

Modification

AIP Microcode Version 10.22 fixes the following:

- Online insertion and removal (OIR) of any card in a router that has AIP microcode causes problems. [CSCdj37259]

AIP Microcode Version 10.23

Modification

AIP Microcode Version 10.23 fixes the following:

- AIP forwards giants to RSP causing RSP crash at rsp_free_memd_pak. [CSCdj59745]

AIP Microcode Version 10.24

Modification

AIP Microcode Version 10.24 fixes the following:

- AIP has mroute-cache corruption. [CSCdj82421]

AIP Microcode Version 10.25

Modification

AIP Microcode Version 10.25 fixes the following:

- AIP applies incorrect physical format on BookTree 8222 framer. [CSCdj90325]

Fast Ethernet Interface Processor (FEIP) Microcode Revision Summary

FEIP Microcode Version 10.3

Modification

FEIP Microcode Version 10.3 fixes the following:

- Serial interfaces that are down but not administratively disabled (downed) may periodically reset with error “8010 - disable fsip_reset.” [CSCdi49431]

FEIP Microcode Version 10.4

Modifications

FEIP Microcode Version 10.4 fixes the following:

- The FX port adapter is not supported.
- FEIPs keepalive will not detect line protocol down (disconnected cable) when configured for full duplex, so reliance on this feature to detect cable faults is inaccurate. The only known workaround is to periodically track successful transmissions and reception on the suspect interface. [CSCdi48337]

FEIP Microcode Version 10.5

Modifications

FEIP Microcode Version 10.5 fixes the following:

- The FEIP MII interface fails to reset if there is OIR of another card in the router. [CSCdi82350]
- There is a failure of both ping and telnet to HSRP virtual addresses on FastEthernet. [CSCdi92485]

FEIP Microcode Version 10.6

Modifications

FEIP Microcode Version 10.6 fixes the following:

- An internal error may occur on Cisco 7513 routers using FEIP: “%DBUS-3-DBUS.” [CSCdi92811]
- An active router resigns after receiving its own packet. [CSCdi93012]

FEIP Microcode Version 10.7

Modification

FEIP Microcode Version 10.7 fixes the following:

- Enabling FEIP in RP/SP 7000 causes the error message “CBUS-3-INITERR with Error (8021).” [CSCdj14743]

Fast Serial Interface Processor (FSIP) Microcode Revision Summary

FSIP Microcode Version 10.13

Modification

FSIP Microcode Version 10.13 fixes the following:

- Serial interfaces that are down but not administratively disabled (downed) may periodically reset with error “8010 - disable fsip_reset.” [CSCdi49431]

FSIP Microcode Version 10.14

FSIP Microcode Version 10.14 was never released.

FSIP Microcode Version 10.15

FSIP Microcode Version 10.15 was never released.

FSIP Microcode Version 10.16

Modifications

FSIP Microcode Version 10.16 fixes the following:

- Using FSIP might cause a CiscoBus restart. [CSCdi58194]
- Transmitter-delay does not work on FSIP DCE interfaces. [CSCdi58196]

FSIP Microcode Version 10.17

Modification

FSIP Microcode Version 10.17 fixes the following:

- FSIP does not recognize CDE leads during a cutover from a Cisco 2501 serial port. [CSCdi64735]

FSIP Microcode Version 10.18

Modification

FSIP Microcode Version 10.18 fixes the following:

- In DCE mode, FSIP looks for DCD and DSR up before declaring the line UP. FSIP should only look for DCD. [CSCdi64735]

FSIP Microcode Version 10.19

Modification

FSIP Microcode Version 10.19 fixes the following:

- Transmitter-Delay does not work in DTE/DCE mode. [CSCdi72431]

HSSI Interface Processor (HIP) Microcode Revision Summary

HIP Microcode Version 20.1

Modification

HIP Microcode Version 20.1 fixes the following:

- HIP microcode could reset the HIP while it is in the middle of a CyBus transaction, resulting in “CyBus error 78” or “SRAM parity error” messages. The reset only occurs if the CyBus is being utilized at near capacity. A possible workaround is to balance the load across each CyBus (7513/7508). [CSCdi85371]

HIP Microcode Version 20.2

Modification

HIP Microcode Version 20.2 fixes the following:

- Fixed [CSCdj21227]

MultiChannel Interface Processor (MIP) Microcode Revision Summary

MIP Microcode Version 12.0

Modification

MIP Microcode Version 12.0 fixes the following:

- Non-FIFO queuing is not supported on MIP. [CSCdi44333]

MIP Microcode Version 12.1

Modification

MIP Microcode Version 12.1 fixes the following:

- A channelized T1 remote interface loop might report failure. [CSCdi76327]

MIP Microcode Version 12.2

Modifications

MIP Microcode Version 12.2 fixes the following:

- The MIP loopback remote command causes IPs to crash. [CSCdi69074]
- MIP framing changes from Super Frame (SF) to Extended Superframe Format (ESF) after a microcode reload. [CSCdi71556]
- MIP channel creation may cause output stuck on others. [CSCdi74075]

Switch Processor (SP) Microcode Revision Summary

SP Microcode Version 11.15

Modification

SP Microcode Version 11.15 fixes the following:

- Turning on **ipx route-cache sse** with microcode version SSP10-12 or SSP10-13 produces a mismatch between the frame length on odd-byte 802.3 IPX packets and the 802.3 length. Novell devices might not recognize these packets, resulting in communication timeouts.

The following three workarounds can be used:

- Turn off padding on process-switched packets using the following command:

no ipx pad-process-switched-packets

- Configure the router for autonomous switching instead of SSE switching using the following commands:

no ipx route-cache sse

ipx route-cache cbus

- Turn off SSE switching using the following command:

no ipx route-cache sse

[CSCdi42802], [CSCdi45139], [CSCdi46156]

Silicon Switch Processor (SSP) Microcode Revision Summary

SSP Microcode Version 11.15

Modification

SSP Microcode Version 11.15 fixes the following:

- Turning on **ipx route-cache sse** with microcode version SSP10-12 or SSP10-13 produces a mismatch between the frame length on odd-byte 802.3 IPX packets and the 802.3 length. Novell devices might not recognize these packets, resulting in communication timeouts.

The following three workarounds can be used:

- Turn off padding on process-switched packets using the following command:
 - **no ipx pad-process-switched-packets**
- Configure the router for autonomous switching instead of SSE switching using the following commands:
 - **no ipx route-cache sse**
 - **ipx route-cache cbus**
- Turn off SSE switching using the following command:
 - **no ipx route-cache sse**

[CSCdi42802], [CSCdi45139], [CSCdi46156]

Token Ring Interface Processor (TRIP) Microcode Revision Summary

TRIP Microcode Version 10.4

Modification

TRIP Microcode Version 10.4 fixes the following:

- A SpyGlass problem causes the command queue to the SpyGlass to overflow. The symptom of this problem is a “trucheck” at location 0x925 in trip10-3.

Versatile Interface Processor (VIP) Microcode Revision Summary

VIP Microcode Version 20.18

Modifications

VIP Microcode Version 20.18 fixes the following:

- If you are connected to the VIP by the unsupported RVIP console interface, the Cisco 7000 router will crash if you remove the VIP. This problem does not exist on Cisco 7500 series routers.
[CSCdi45132]

- The 4R ports on the VIP card do not support fast switching. Use process switching as a workaround. [CSCdi51744]

VIP Microcode Version 20.23

The next major release of VIP microcode after Version 20.18 is Version 20.23.

For modifications related to VIP, refer to the section “Caveats for Release 11.1(1) through 11.1(2)” earlier in this document.

VIP Microcode Version 20.31

The next major release of VIP microcode after Version 20.23 is Version 20.31.

For modifications related to VIP, refer to the section “Caveats for Release 11.1(1) through 11.1(3)” earlier in this document.

VIP Microcode Version 20.40

The next major release of VIP microcode after Version 20.31 is Version 20.40.

For modifications related to VIP, refer to the section “Caveats for Release 11.1(1) through 11.1(4)” earlier in this document.

Route Switch Processor (RSP) Microcode Revision History

This section describes each revision of RSP microcode, which is used with Cisco 7500 series routers and Cisco 7000 series routers using an RSP7000. The descriptions list the caveats that were fixed in each microcode revision.

For descriptions of each revision of microcode for Cisco 7000 series routers using a route processor/silicon switch processor (RP/SSP) or route processor/switch processor (RP/SP) combination, see the previous section, “Microcode Revision History (for Cisco 7000 Series Platforms).”

ATM Interface Processor (AIP) Microcode Revision Summary

AIP Microcode Version 20.6

Modification

AIP Microcode Version 20.6 fixes the following:

- Ping between the two routers fails intermittently with SMDS configuration. [CSCdi45807]

AIP Microcode Version 20.7

Modifications

AIP Microcode Version 20.7 fixes the following:

- AIP sends out incorrect idle cells. [CSCdi48069]

- VINES encapsulation errors cause an AIP outhung condition. [CSCdi50568]
- Configuring the AIP microcode might cause a race condition to occur. [CSCdi54829]
- ATM fails when used on a Route Switch Processor (RSP). [CSCdi60561]

AIP Microcode Version 20.8

Modification

AIP Microcode Version 20.8 fixes the following:

- Sometimes a race condition occurs, and commands from a Route Processor (RP) or Route Switch Processor (RSP) are rejected. When this condition occurs, the following console messages are logged [CSCdi62445]:

```
%ATM-3-FAILCREATEVC: ATM failed to create VC(VCD=1011, VPI=0, VCI=262) on Interface
ATM5/0, (Cause of the failure: Failed to have the driver to accept the VC)
%AIP-3-AIPREJCMD: Interface ATM5/0, AIP driver rejected Teardown VC command (error code
0x8000)
```

AIP Microcode Version 20.9

Modifications

AIP Microcode Version 20.9 fixes the following:

- AIP microcode version 20.8 may cause the AIP card to lock into a state where it transmits corrupted packets, causing debug atm error showing “ATM(ATM9/0.1): VC(1) Bad SAP ...” at the receive side of the ATM VC. The transmission of data is usually affected in one direction only. The problem may occur when the input traffic exceeds the average rate configured on the ATM VC, when the bandwidth of the incoming interfaces exceeds the average rate on the outgoing VC or SVC.

A workaround is either to downgrade the AIP microcode to aip20-6 or to upgrade the AIP microcode to rsp_aip205-5, or aip20-9 when available. A short term workaround is **clear int atm 5/0** on the transmit side. [CSCdi67812]

The same problem applies for aip10-15 on RP-based platforms.

- ATM traffic is lost during an online insertion or removal (OIR) event of an RSP4. [CSCdi66076]

AIP Microcode Version 20.10

Modifications

AIP Microcode Version 20.10 fixes the following:

- Online insertion and removal (OIR) of a VIP2 brings down ATM in a Cisco 7507 router. [CSCdi75659]
- Sometimes the AIP hangs. [CSCdi60941]
- The AIP microcode does not support configurable LBO settings. [CSCdi72800]
- The AIP sometimes fails to set up a DS3 scramble. [CSCdi57924]

AIP Microcode Version 20.11

Modification

AIP Microcode Version 20.11 fixes the following:

- The VPI/VCI hash lookup in AIP is not optimal. [CSCdi69673]

AIP Microcode Version 20.12

Modification

AIP Microcode Version 20.12 fixes the following:

- LANE should support 9k MTU for Ethernet ELAN. [CSCdj06005]

AIP Microcode Version 20.13

Modification

AIP Microcode Version 20.13 fixes the following:

- AIP does not show ATM packets dropped because of traffic shaping. [CSCdi72246]

AIP Microcode Version 20.14

Modification

AIP Microcode Version 20.14 fixes the following:

- The following error messages are seen:

`%AIP-3-AIPREJCMD with error code 0x8000`

`%SYS-3-CPUHOG`

[CSCdj20667]

AIP Microcode Version 20.15

Modification

AIP Microcode Version 20.15 fixes the following:

- Online insertion and removal (OIR) of any card in a router that has AIP microcode causes problems. [CSCdj37259]

Route Switch Processor (RSP) Microcode Revision History

AIP Microcode Version 20.16

Modification

AIP Microcode Version 20.16 fixes the following:

- AIP forwards giants to RSP causing RSP crash at `rsp_free_memd_pak`. [CSCdj59745]

AIP Microcode Version 20.17

Modification

AIP Microcode Version 20.17 fixes the following:

- AIP has `mroute-cache` corruption. [CSCdj82421]

AIP Microcode Version 20.18

Modification

AIP Microcode Version 20.18 fixes the following:

- AIP applies incorrect physical format on BookTree 8222 framer [CSCdj90325]

Ethernet Interface Processor (EIP) Microcode Revision Summary

EIP Microcode Version 20.2

Modification

EIP Microcode Version 20.2 fixes the following:

- Version 1.6 Rev C0 EIPs may cause cache parity errors on all Cisco 7500 series routers and RSP7000 systems. The cache parity errors may cause system reloads. Hardware revision and version levels can be determined by using the **show diag** command. The problem is resolved in EIP microcode `rsp_eip20-2` or above. [CSCdi52082]

EIP Microcode Version 20.3

Modification

EIP Microcode Version 20.3 fixes the following:

- A bad R4600 processor causes router crashes with errors such as XBUFHDR errors, INVRTN errors, and GETBUF errors. [CSCdi75404]

EIP Microcode Version 20.4

Modification

EIP Microcode Version 20.4 fixes the following:

- Renumbered EIP microcode with code change to fix problem with interfaces changing between up and down state. Fix committed into 11.1CA release only. [CSCdk36767]

EIP Microcode Version 20.5

Modification

EIP Microcode Version 20.5 fixes the following:

- Renumbered rsp_eip20-5 after commenting some debug code. Fixes problem with interfaces changing between up and down state in all releases (11.1/11.2/12.0). [CSCdk36767]

EIP Microcode Version 20.6

Modification

EIP Microcode Version 20.6 fixes the following:

- fixed problem with corrupted frame being seen on RSP Ethernet under heavy load. [CSCdk34545]

Fast Ethernet Interface Processor (FEIP) Microcode Revision Summary

FEIP Microcode Version 20.2

Modification

FEIP Microcode Version 20.2 fixes the following:

- Serial interfaces that are down but not administratively disabled (downed) may periodically reset with error "8010 - disable fsip_reset." [CSCdi49431]

FEIP Microcode Version 20.3

Modifications

FEIP Microcode Version 20.3 fixes the following:

- The FX port adapter is not supported.
- FEIP's keepalive will not detect line protocol down (disconnected cable) when configured for full duplex, so reliance on this feature to detect cable faults is inaccurate. The only known workaround is to periodically track successful transmissions and reception on the suspect interface. [CSCdi48337]

FEIP Microcode Version 20.4

Modifications

FEIP Microcode Version 20.4 fixes the following:

- The FEIP MII interface fails to reset if there is OIR of another card in the router. [CSCdi82350]
- There is a failure of both ping and Telnet to HSRP virtual addresses on Fast Ethernet. [CSCdi92485]

FEIP Microcode Version 20.5

Modifications

FEIP Microcode Version 20.5 fixes the following:

- An internal error may occur on Cisco 7513 routers using FEIP: “%DBUS-3-DBUS.” [CSCdi92811]
- An active router resigns after receiving its own packet. [CSCdi93012]

FEIP Microcode Version 20.6

Modification

FEIP Microcode Version 20.6 fixes the following:

- Enabling FEIP in RP/SP 7000 causes the error message “CBUS-3-INITERR with Error (8021).” [CSCdj14743]

Fast Serial Interface Processor (FSIP) Microcode Revision Summary

FSIP Microcode Version 20.2

Modifications

FSIP Microcode Version 20.2 fixes the following:

- When using the X.21 protocol, DTE devices erroneously send data when Control is OFF. [CSCdi45512]
- Using FSIP might cause a CiscoBus restart. [CSCdi58194]
- Transmitter-delay does not work on FSIP DCE interfaces. [CSCdi58196]

FSIP Microcode Version 20.3

Modifications

FSIP Microcode Version 20.3 fixes the following:

- Serial interfaces and their line protocols might occasionally go down if the interface cable is changed or the remote end dies and comes back. Issuing a **show interface serial** command produces the following:

```
Serialx/y is down, line protocol is down
Hardware is cyBus Serial
.
.
.
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
RTS up, CTS up, DTR up, DCD up, DSR up
```

The serial interface will stay down if the remote side toggles. [CSCdi57573]

- FSIP does not recognize CDE leads during a cutover from a Cisco 2501 serial port. [CSCdi64735]

FSIP Microcode Version 20.4

Modification

FSIP Microcode Version 20.4 fixes the following:

- In DCE mode, FSIP looks for DCD and DSR up before declaring the line UP. FSIP should only look for DCD. [CSCdi64735]

FSIP Microcode Version 20.5

Modifications

FSIP Microcode Version 20.5 fixes the following:

- FSIP gets lost from the chassis during online insertion and removal (OIR) of a VIP2. [CSCdi73130]
- A serial interface stays line down when the remote side toggles. [CSCdi57573]

FSIP Microcode Version 20.6

Modification

FSIP Microcode Version 20.6 fixes the following:

- Transmitter-Delay does not work. [CSCdi72431]

FSIP Microcode Version 20.7

Modification

FSIP Microcode Version 20.7 fixes the following:

- The “CBUS-3-CMDTIMEOUT” error message causes FSIP to vanish. [CSCdj00013]

FSIP Microcode Version 20.8

Modification

FSIP Microcode Version 20.8 fixes the following:

- The “RSP-3-IP_PANIC” error message causes interface resets and buffer misses. [CSCdi78086]

HSSI Interface Processor (HIP) Microcode Revision Summary

HIP Microcode Version 20.1

Modification

HIP Microcode Version 20.1 fixes the following:

- HIP microcode could reset the HIP while it is in the middle of a CyBus transaction, resulting in “CyBus error 78” or “SRAM parity error” messages. The reset only occurs if the CyBus is being utilized at near capacity. A possible workaround is to balance the load across each CyBus (7513/7508). [CSCdi85371]

HIP Microcode Version 20.2

Modification

HIP Microcode Version 20.2 fixes the following:

- Online insertion and removal (OIR) of any card in a router that has HIP microcode causes problems. [CSCdj21227]

MultiChannel Interface Processor (MIP) Microcode Revision Summary

MIP Microcode Version 22.0

Modification

MIP Microcode Version 22.0 fixes the following:

- Non-FIFO queuing is not supported on MIP. [CSCdi44333]

MIP Microcode Version 22.1

Modification

MIP Microcode Version 22.1 fixes the following:

- A channelized T1 remote interface loop could report failure. [CSCdi76327]

MIP Microcode Version 22.2

Modifications

MIP Microcode Version 22.2 fixes the following:

- The MIP loopback remote command causes IPs to crash. [CSCdi69074]
- MIP framing changes from Super Frame (SF) to Extended Superframe Format (ESF) after a microcode reload. [CSCdi71556]
- MIP channel creation may cause output stuck on others. [CSCdi74075]

Route Switch Processor 2 (RSP2) Microcode Revision Summary

The next major release of RSP2 microcode after Version 200.0 is Version 20.0.

For modifications related to RSP2, refer to the section “Caveats for Release 11.1(1) through 11.1(4)” earlier in this document.

Note The initial release of RSP2 microcode was Version 200.0, in Cisco IOS Release 11.1(2).

Token Ring Interface Processor (TRIP) Microcode Revision Summary

TRIP Microcode Version 20.1

Modification

TRIP Microcode Version 20.1 fixes the following:

- A SpyGlass problem causes the command queue to the SpyGlass to overflow. The symptom of this problem is a “ctruccheck” at location 0x925 in trip10-3.
- The DMA engine appears to “clock in” the memd address an extra time or increment the memd address an extra time. The obvious symptom is an “800E” (output stuck).
- With transmit frames, the prototype Access Control byte is invalid (bit 0x10 is set).

TRIP Microcode Version 20.2

Modification

TRIP Microcode Version 20.2 fixes the following:

- Online insertion and removal (OIR) of any card in a router that has TRIP microcode causes problems. [CSCdi75287]

Versatile Interface Processor (VIP) Microcode Revision Summary

The VIP microcode for the RSP is the same as the Cisco 7000 VIP microcode.

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 access 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 might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Open Source License Acknowledgements

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”
The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CDDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0102R)

Copyright © 1996–2001, Cisco Systems, Inc.
All rights reserved. Printed in USA.

