Doc. No. 78-1784-20

Router Products Release Notes for Cisco IOS Release 10.3

September 10, 1997

These release notes describe the features, modifications, and caveats for Cisco IOS Release 10.3, up to and including Release 10.3(19a). They include all routing and protocol translation features.

Cisco IOS releases 10.3(14) through 10.3(19a) are deemed “Generally Deployable.” Cisco believes that Release 10.3 is suitable for deployment anywhere in the network where the features and functionality of this release are required.

Cisco IOS Release 10.3(19a) is the last regularly scheduled 10.3 maintenance release. The End of Engineering milestone occurs at Release 10.3(19a).

Introduction

These release notes discuss the following topics:

Documentation

For printed documentation of Cisco IOS Release 10.3 router software features, refer to the Cisco IOS Release 10.3 *Router Products Configuration Guide Addendum* and *Router Products Command Reference Addendum*. These addenda include new features introduced since Release 10.0 and supplement the information in the following manuals:

- Release 10 *Router Products Configuration Guide*
- Release 10 *Router Products Command Reference*

The configuration guide and command reference addenda are divided into seven main parts. Six parts match the parts in the Release 10 *Router Products Configuration Guide* and *Router Products Command Reference*. The seventh part contains chapters covering new technology areas.

Electronic documentation of Release 10.3 router software features is available on the Documentation CD-ROM. Refer to the Release 10.3 *Router Products Configuration Guide* and *Router Products Command Reference* publications, which are located in the Cisco IOS Release 10.3 database. (Note that the two addenda are not separate documents on CD because the information in them has been incorporated into the electronic documents.)

For printed protocol translation documentation, refer to the Release 10.3 *Protocol Translation Configuration Guide and Command Reference* publication. On CD, refer to the Release 10.3 *Protocol Translation Configuration Guide and Command Reference* publication in the Cisco IOS Release 10.3 database.

You can also access Cisco technical documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Platform Support

Cisco IOS Release 10.3 supports the following router platforms:

- Cisco 7000 series and 7500 series
- Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, and 4700-M)
- Cisco 3000 series (except the Cisco 3202)
- Cisco 2500 series (except Cisco 2520 through Cisco 2525)
- Cisco 1000 series routers (Cisco 1003, Cisco 1004, Cisco 1005)
- Cisco 1000 LAN Extender
- AccessPro PC Card
- AGS+ (with a CSC/4 processor board)
- MGS (with a CSC/4 processor board)
- CGS (with a CSC/4 processor board)

Table 1 summarizes the LAN interfaces supported on each platform. Table 2 summarizes the WAN data rates and interfaces supported on each platform.

Table 1 LAN Interfaces Supported by Router Platforms

Interface	Cisco 7000, 7500 Series	Cisco 4000 Series	Cisco 3000 Series[1]	Cisco 2500 Series[2]	Cisco 1000 Series Routers	Cisco 1000 LAN Extender	Access-Pro PC Card	AGS+	MGS	CGS
Ethernet (AUI)	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Ethernet (10BaseT)	No	Yes	No	Yes (2505 and 2507 only)	Yes	Yes	Yes	Yes	No	No
Fast Ethernet (100BaseTX)	Yes	No	No	No	No	No	No	No	No	No
4-Mbps Token Ring	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes
16-Mbps Token Ring	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes
FDDI DAS	Yes	Yes	No	No	No	No	No	Yes	No	No
FDDI SAS	Yes	Yes	No	No	No	No	No	Yes	No	No
FDDI multimode	Yes	Yes (DAS/ SAS)	No	No	No	No	No	Yes	No	No
FDDI single-mode	Yes	Yes	No	No	No	No	No	Yes	No	No

Interface	Cisco 7000, 7500 Series	Cisco 4000 Series	Cisco 3000 Series[1]	Cisco 2500 Series[2]	Cisco 1000 Series Routers	Cisco 1000 LAN Extender	Access-Pro PC Card	AGS+	MGS	CGS
ATM Interface Processor (AIP)	Yes	No	No	No	No	No	No	No	No	No
Channel Interface Processor (CIP)	Yes	No	No	No	No	No	No	No	No	No
Second-generation Channel Interface Processor (CIP2)[3]	Yes	No	No	No	No	No	No	No	No	No
MultiChannel Interface Processor (MIP)	Yes	No	No	No	No	No	No	No	No	No

1. Except the Cisco 3202.
2. Except the Cisco 2520 through Cisco 2525.
3. In the Cisco 7000 series routers (Cisco 7000 and Cisco 7010), these interfaces require the 7000 series Route Switch Processor (RSP7000) and the 7000 series chassis interface (RSP7000CI).

Table 2 WAN Data Rates and Interfaces Supported by Router Platforms

	Cisco 7000, 7500 Series	Cisco 4000 Series	Cisco 3000 Series[1]	Cisco 2500 Series[2]	Cisco 1000 Series Routers[3]	Cisco 1000 LAN Extender	Access-Pro PC Card	AGS+	MGS	CGS
Data Rate										
48/56/64 kbps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
1.544/2.048 Mbps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
34/45/52 Mbps	Yes	No	No	No	No	No	No	Yes	No	No
Interface										
EIA/TIA-232	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
X.21	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
V.35	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EIA/TIA-449	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No
EIA-530	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No	No
EIA/TIA -613 (HSSI)	Yes	No	No	No	No	No	No	Yes	No	No
ISDN BRI	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No
ISDN PRI	Yes	No	No	No	No	No	No	No	No	No
G.703/G.704	Yes	Yes	No	No	No	No	No	Yes	No	No

1. Except the Cisco 3202.
2. Except the Cisco 2520 through Cisco 2525.
3. Except the Cisco 1005.

Cisco IOS Software Packaging

The Cisco IOS software is available in different packages depending upon the platform.

- Table 3 lists the software for the Cisco 7000 series, Cisco 7500 series, AGS+, MGS, and CGS.
- Table 4 lists the feature sets for the Cisco 1003 and Cisco 1004 ISDN routers.
- Table 5 lists the features sets for the Cisco 1005 router.
- Table 6 lists the feature sets for the Cisco 2500 series and the AccessPro PC card.
- Table 7 lists the feature sets for the Cisco 4000 series, which includes the Cisco 4000, Cisco 4000-M, Cisco 4500, Cisco 4500-M, Cisco 4700, and Cisco 4700-M.
- Table 8 lists the software for the Cisco 3000 series.

Table 3 Cisco 7000 Series, Cisco 7500 Series, AGS+, MGS, and CGS Software Feature Sets

	Feature Set		
Feature	**Enterprise**	**Enterprise/CIP2**	**Source Route Switch[1]**
SNMP	Yes	Yes	Yes
Asynchronous support (SLIP)	Yes	Yes	—
Frame Relay	Yes	Yes	—
SMDS	Yes	Yes	—
X.25	Yes	Yes	—
ISDN	Yes	Yes	—
PPP	Yes	Yes	—
HDLC	Yes	Yes	—
IP	Yes	Yes	Yes (host only)
RIP	Yes	Yes	—
IGRP	Yes	Yes	—
Enhanced IGRP	Yes	Yes	—
OSPF	Yes	Yes	—
BGP	Yes	Yes	—
EGP	Yes	Yes	—
PIM	Yes	Yes	—
NHRP	Yes	Yes	—
ES-IS	Yes	Yes	—
IS-IS	Yes	Yes	—
Snapshot routing	Yes	Yes	—
NTP	Yes	Yes	—
Transparent bridging	Yes	Yes	Yes
Translational bridging	Yes	Yes	—
Multiring	Yes	Yes	—
LAN extension host	Yes	Yes	—
IPX	Yes	Yes	—

	Feature Set		
Feature	**Enterprise**	**Enterprise/CIP2**	**Source Route Switch[1]**
NLSP	Yes	Yes	—
IPXWAN 2.0	Yes	Yes	—
AppleTalk Versions 1 and 2	Yes	Yes	—
AURP	Yes	Yes	—
DECnet IV, V	Yes	Yes	—
Apollo Domain	Yes	Yes	—
Banyan VINES	Yes	Yes	—
ISO CLNS	Yes	Yes	—
XNS	Yes	Yes	—
Source-route bridging	Yes	Yes	Yes
Remote source-route bridging	Yes	Yes	—
DLSw+	Yes	Yes	—
SDLC	Yes	Yes	—
SDLLC	Yes	Yes	—
STUN	Yes	Yes	—
TG/COS	Yes	Yes	—
QLLC	Yes	Yes	—
DSPU	Yes	Yes	—
Telnet	Yes	Yes	—
AutoInstall	Yes	Yes	—
DHCP	Yes	Yes	—

1. The Source Route Switch applies to the Cisco 7000 and Cisco 7010 only, not to the AGS+, MGS, or CGS.

Table 4 Cisco 1003 and Cisco 1004 ISDN Router Software Feature Sets

	Feature Set	
Feature	**IP**	**IP/IPX/AT**
SNMP	Yes	Yes
Asynchronous support (SLIP)	—	—
ARA	—	—
Frame Relay (RFC 1490)	—	—
SMDS	—	—
X.25	—	—
ISDN	Yes	Yes
PPP	Yes	Yes
HDLC	Yes	Yes
IP	Yes	Yes
RIP	Yes	Yes

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

	Feature Set	
Feature	**IP**	**IP/IPX/AT**
XRemote	—	—
Telnet	Yes	Yes
AutoInstall	—	—
DHCP	—	—

Table 5 Cisco 1005 Router Software Feature Sets

	Feature Set		
Feature	**IP**	**IP/IPX/AT**	**IP/IPX/AT/X.25**
SNMP	Yes	Yes	Yes
Asynchronous support (SLIP)	—	—	—
ARA	—	—	—
Frame Relay (RFC 1490)	Yes	Yes	—
SMDS	Yes	Yes	—
X.25	Yes	—	Yes
ISDN	—	—	—
PPP	Yes	Yes	—
HDLC	Yes	Yes	Yes
IP	Yes	Yes	Yes
RIP	Yes	Yes	Yes
IGRP	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes
OSPF	—	—	—
BGP	—	—	—
EGP	—	—	—
PIM	—	—	—
NHRP	—	—	—
ES-IS	—	—	—
IS-IS	—	—	—
Snapshot routing	Yes	Yes	—
NTP	—	—	—
Transparent bridging	Yes	Yes	Yes
Multiring	—	—	—
LAN extension host	—	—	—
IPX	—	Yes	Yes
NLSP	—	—	—
IPXWAN 2.0	—	Yes	Yes
AppleTalk Versions 1 and 2	—	Yes	Yes

	Feature Set		
Feature	**IP**	**IP/IPX/AT**	**IP/IPX/AT/X.25**
AURP	—	—	—
DECnet IV	—	—	—
DECnet V	—	—	—
Apollo Domain	—	—	—
Banyan VINES	—	—	—
ISO CLNS	—	—	—
XNS	—	—	—
Source-route bridging/ remote source-route bridging	—	—	—
DLSw+	—	—	—
SDLC	—	—	—
SDLLC	—	—	—
STUN	—	—	—
TG/COS	—	—	—
QLLC	—	—	—
DSPU	—	—	—
Protocol translation	—	—	—
TN3270	—	—	—
LAT	—	—	—
XRemote	—	—	—
Telnet	Yes	Yes	Yes
AutoInstall	Yes	Yes	Yes
DHCP	—	—	—

Table 6 Cisco 2500 Series and AccessPro PC Card Software Feature Sets

	Feature Set								
Feature	**IP**	**IP/IBM Base**	**IP/IPX**	**IP/IPX/ IBM Base**	**Desktop**	**Desktop/ IBM Base**	**Enterprise**	**CFRAD**	**ISDN**
SNMP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Asynchronous support (SLIP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARA	—	—	—	—	Yes	Yes	Yes	—	—
Frame Relay (RFC 1490)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—
SMDS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—
X.25	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—
ISDN	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	—	—

	Feature Set								
Feature	IP	IP/IBM Base	IP/IPX	IP/IPX/ IBM Base	Desktop	Desktop/ IBM Base	Enterprise	CFRAD	ISDN
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
BGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
EGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
PIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
NHRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
ES-IS	—	—	—	—	—	—	Yes	—	—
IS-IS	—	—	—	—	—	—	Yes	—	—
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—
Transparent and translational bridging	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
Multiring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
LAN extension host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—
IPX	—	—	Yes	Yes	Yes	Yes	Yes	—	Yes
NLSP	—	—	Yes	Yes	Yes	Yes	Yes	—	—
IPXWAN 2.0	—	—	Yes	Yes	Yes	Yes	Yes	—	—
AppleTalk Versions 1 and 2	—	—	—	—	Yes	Yes	Yes	—	Yes
AURP	—	—	—	—	Yes	Yes	Yes	—	Yes
DECnet IV	—	—	—	—	Yes	Yes	Yes	—	—
DECnet V	—	—	—	—	—	—	Yes	—	—
Apollo Domain	—	—	—	—	—	—	Yes	—	—
Banyan VINES	—	—	—	—	—	—	Yes	—	—
ISO CLNS	—	—	—	—	—	—	Yes	—	—
XNS	—	—	—	—	—	—	Yes	—	—
SRB	—	Yes	—	Yes	—	Yes	Yes	—	—
RSRB	—	Yes	—	Yes	—	Yes	Yes	Yes	—
DLSw (RFC 1795)	—	Yes	—	Yes	—	Yes	Yes	Yes	—
DLSw+	—	Yes	—	Yes	—	Yes	Yes	—	—
SDLC	—	Yes	—	Yes	—	Yes	Yes	Yes	—
SDLLC	—	Yes	—	Yes	—	Yes	Yes	Yes	—
STUN	—	Yes	—	Yes	—	Yes	Yes	Yes	—
TG/COS	—	—	—	—	—	—	Yes	—	—
QLLC	—	—	—	—	—	—	Yes	—	—

	Feature Set								
Feature	IP	IP/IBM Base	IP/IPX	IP/IPX/ IBM Base	Desktop	Desktop/ IBM Base	Enterprise	CFRAD	ISDN
DSPU	—	—	—	—	—	—	Yes	—	—
Protocol translation	—	—	—	—	—	—	Yes	—	—
TN3270	—	—	—	—	—	—	Yes	—	—
LAT	—	—	—	—	—	—	Yes	—	—
XRemote	—	—	—	—	—	—	Yes	—	—
Telnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AutoInstall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—
DHCP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes

Table 7 Cisco 4000 Series Software Feature Sets

	Feature Set						
Feature	IP	IP/IBM Base	IP/IPX	IP/IPX/ IBM Base	Desktop	Desktop/ IBM Base	Enterprise
SNMP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Asynchronous support (SLIP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARA	—	—	—	—	—	—	—
Frame Relay (RFC 1490)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SMDS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HDLC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NHRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ES-IS	—	—	—	—	—	—	Yes
IS-IS	—	—	—	—	—	—	Yes
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes

	Feature Set						
Feature	**IP**	**IP/IBM Base**	**IP/IPX**	**IP/IPX/ IBM Base**	**Desktop**	**Desktop/ IBM Base**	**Enterprise**
Transparent and translational bridging	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiring	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN extension host	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
AppleTalk Versions 1 and 2	—	—	—	—	Yes	Yes	Yes
AURP	—	—	—	—	Yes	Yes	Yes
DECnet IV	—	—	—	—	Yes	Yes	Yes
DECnet V	—	—	—	—	—	—	Yes
Apollo Domain	—	—	—	—	—	—	Yes
Banyan VINES	—	—	—	—	—	—	Yes
ISO CLNS	—	—	—	—	—	—	Yes
XNS	—	—	—	—	—	—	Yes
Source-route bridging/ remote source-route bridging	—	Yes	—	Yes	—	Yes	Yes
DLSw+	—	Yes	—	Yes	—	Yes	Yes
SDLC	—	Yes	—	Yes	—	Yes	Yes
SDLLC	—	Yes	—	Yes	—	Yes	Yes
STUN	—	Yes	—	Yes	—	Yes	Yes
TG/COS	—	—	—	—	—	—	Yes
QLLC	—	—	—	—	—	—	Yes
DSPU	—	—	—	—	—	—	Yes
Protocol translation	—	—	—	—	—	—	Yes
TN3270	—	—	—	—	—	—	Yes
LAT	—	—	—	—	—	—	Yes
XRemote	—	—	—	—	—	—	Yes
Telnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AutoInstall	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 8 Cisco 3000 Series Software

Feature	Enterprise
SNMP	Yes
Asynchronous support (SLIP)	Yes
ARA	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
Source-route bridging	Yes
Remote source-route bridging	Yes

Feature	Enterprise
DLSw+	Yes
SDLC	Yes
SDLLC	Yes
STUN	Yes
TG/COS	Yes
QLLC	Yes
DSPU	Yes
AutoInstall	Yes
Telnet	Yes
Protocol translation	Yes
TN3270	Yes
LAT	Yes
XRemote	Yes
DHCP	Yes

Memory Requirements

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

For AGS+, MGS, and CGS routers to take advantage of the Release 10.3 features, they must have CSC/4 processor cards and 9.1(8)-level (or higher) system ROMs for netbooting.

For the other Cisco routers to take advantage of the Release 10.3 features, you must upgrade the code or main system memory as listed in Table 9. Some platforms have specific chip or architecture requirements that affect what can be upgraded and in what increments.

Table 9 Release 10.3 Memory Requirements

Router	Required Code Memory	Required Main Memory	Release 10.3 Runs from
Cisco 1000 Series Routers			
IP Set	2/4/8 MB optional Flash	4 MB RAM	RAM
IP/IPX/AT Set	2/4/8 MB optional Flash	4 MB RAM	RAM

Router	Required Code Memory	Required Main Memory	Release 10.3 Runs from
Cisco 2500 Series			
IP Set	4 MB Flash	2 MB RAM[1]	Flash
IP/IBM Set	4 MB Flash	4 MB RAM	Flash
IP/IPX Set	4 MB Flash	4 MB RAM	Flash
IP/IPX/IBM Set	8 MB Flash	4 MB RAM	Flash
Desktop Set	4 MB Flash	4 MB RAM	Flash
Desktop/IBM Set	8 MB Flash	4 MB RAM	Flash
Enterprise Set	8 MB Flash	6 MB RAM	Flash
CFRAD Set	4 MB Flash	2 MB RAM	Flash
ISDN Set	4 MB Flash	2 MB RAM	Flash
Cisco 3101, Cisco 3102, Cisco 3103	8 MB Flash	4 MB RAM	Flash
	4 MB Flash	8 MB RAM	RAM
Cisco 3104, Cisco 3204	8 MB Flash	4 MB RAM	Flash
	4 MB Flash	8 MB RAM	RAM
Cisco 4000			
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
IP/IPX/IBM 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
Cisco 4000-M			
IP Set	4 MB Flash	8 MB RAM	RAM
IP/IBM Set	4 MB Flash	8 MB RAM	RAM
IP/IPX Set	4 MB Flash	8 MB RAM	RAM
IP/IPX/IBM Set	4 MB Flash	8 MB RAM	RAM
Desktop Set	4 MB Flash	8 MB RAM	RAM
Desktop/IBM Set	4 MB Flash	8 MB RAM	RAM
Enterprise Set	4 MB Flash	8 MB RAM	RAM
Cisco 4500			
IP Set	4 MB Flash	8 MB RAM	RAM
IP/IBM Set	4 MB Flash	32 MB RAM	RAM
IP/IPX Set	4 MB Flash	8 MB RAM	RAM
IP/IPX/IBM Set	4 MB Flash	32 MB RAM	RAM
Desktop Set	4 MB Flash	32 MB RAM	RAM
Desktop/IBM Set	4 MB Flash	32 MB RAM	RAM
Enterprise Set	4 MB Flash	32 MB RAM	RAM

Router	Required Code Memory	Required Main Memory	Release 10.3 Runs from
Cisco 4500-M			
IP Set	4 MB Flash	8 MB RAM	RAM
IP/IBM Set	4 MB Flash	16 MB RAM	RAM
IP/IPX Set	4 MB Flash	8 MB RAM[2]	RAM
IP/IPX/IBM 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
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
IP/IPX/IBM 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
Cisco 7000, Cisco 7010	4 MB Flash	16 MB RAM	RAM
Enterprise Set	4 MB Flash	16 MB RAM	RAM
Enterprise/CIP2 Set	4 MB Flash	16 MB RAM	RAM
Cisco RSP7000	8 MB Flash	16 MB RAM	RAM
Enterprise Set	8 MB Flash	16 MB RAM	RAM
Enterprise/CIP2 Set	8 MB Flash	16 MB RAM	RAM
Cisco 7500	8 MB Flash	16 MB RAM	RAM
Enterprise Set	8 MB Flash	16 MB RAM	RAM
Enterprise/CIP2 Set	8 MB Flash	16 MB RAM	RAM
Source Route Switch	4 MB Flash	16 MB RAM	RAM
AGS+, MGS, CGS	—	16 MB RAM	RAM

1. For Cisco 2500 Access Servers (Cisco 2509 through Cisco 2512), 4 MB DRAM is the minimum recommended, and for the AS5100, 6 MB DRAM is the minimum recommended.
2. Sixteen MB DRAM is required if you have a CT1, CE1, or MBRI card installed.

Microcode Software

Table 10 and Table 11 list the minimum microcode versions for the AGS+, MGS, and CGS platforms, and Table 12 lists the current microcode versions for the Cisco 7000 series. Note that for the Cisco 7000 series, microcode software images are bundled with the system software image. Bundling eliminates the need to store separate microcode images. When the router starts up, the system software unpacks the microcode software bundle and loads the proper software on all the interface processor boards.

Table 13 lists the current Route Switch Processor (RSP) microcode versions for the Cisco 7500 series.

Table 10 Minimum Microcode Versions for the AGS+, MGS, and CGS with CCTL2

Processor or Module	Minimum Version Required
CSC-SCI	1.4
CSC-SCI HDX (half duplex)	5.0
CSC-MCI	1.11
CSC-R16M	3.2
CSC-1R/CSC-2R	1.6
CSC-ENVM	2.2
CSC-CCTL2	11.0[1]
CSC-C2MEC	10.0
CSC-C2HSCI	10.0
CSC-C2FCI	10.0
CSC-C2FCIT	10.0
CSC-C2CTR	10.0

1. CSC-CCTL2 Version 11.2 is available and recommended.

Table 11 Current Microcode Versions for the AGS+, MGS, and CGS with CCTL

Processor or Module	Minimum Version Required
CSC-SCI	1.4
CSC-SCI HDX (half duplex)	5.0
CSC-MCI	1.11
CSC-R16M	3.2
CSC-1R/CSC-2R	1.2
CSC-ENVM	2.2
CSC-CCTL	3.0
CSC-MEC (5.0)	1.1
CSC-MEC (5.1)	2.2
CSC-HSCI	1.0
CSC-FCI	2.0

Note For the Cisco 7000 series, all boards must use the Level 10 microcode that is bundled with the system image.

Table 12 Current Microcode Versions for the Cisco 7000 Series

Processor or Module	Current Bundled Microcode Version	Minimum Version Required
AIP (ATM Interface Processor)	10.17	10.2
CIP (Channel Interface Processor)[1]	20.12	10.0
CIP2 (second-generation Channel Interface Processor)[1]	20.12	20.8
EIP (Ethernet Interface Processor)	10.1	10.0
FEIP (Fast Ethernet Interface Processor)	10.5	10.0
FIP (FDDI Interface Processor)	10.2	10.0
FSIP (Fast Serial Interface Processor)	10.18	10.2
HIP (HSSI Interface Processor)	10.2	10.0
MIP (MultiChannel Interface Processor)	11.4	10.0
SP (Switch Processor)	10.15	10.2
SSP (Silicon Switch Processor, 512 KB)	10.15	10.2
SSP (Silicon Switch Processor, 2 MB)	10.15	10.3
TRIP (Token Ring Interface Processor)	10.4	10.0

1. When the **show microcode** command is issued, both CIP and CIP2 microcode are listed as "CIP" and are distinguished only by the target hardware version shown: CIP microcode has a 4.*x* target hardware version, while CIP2 has a 5.*x* target hardware version. Also note that the image name for CIP2 microcode contains the prefix "cipp-" while the CIP image name prefix is "cip-."

Table 13 Current RSP Microcode Versions for the Cisco 7500 Series

Processor or Module	Current Bundled Microcode Version	Minimum Version Required
AIP (ATM Interface Processor)	20.10	20.1
CIP (Channel Interface Processor)[1]	20.12	20.2
CIP2 (second-generation Channel Interface Processor)[1]	20.12	20.8
EIP (Ethernet Interface Processor)	20.3	20.0
FEIP (Fast Ethernet Interface Processor)	20.4	20.0
FIP (FDDI Interface Processor)	20.1	20.1
FSIP (Fast Serial Interface Processor)	20.5	20.1
HIP (HSSI Interface Processor)	20.0	20.0

Processor or Module	Current Bundled Microcode Version	Minimum Version Required
MIP (MultiChannel Interface Processor)	20.3	20.2
TRIP (Token Ring Interface Processor)	20.1	20.0

1. When the **show microcode** command is issued, both CIP and CIP2 microcode are listed as "CIP" and are distinguished only by the target hardware version shown: CIP microcode has a 4.*x* target hardware version, while CIP2 has a 5.*x* target hardware version. Also note that the image name for CIP2 microcode contains the prefix "cipp-" while the CIP image name prefix is "cip-."

New Software Features in Release 10.3(13)

This section describes new features and enhancements in Release 10.3(13) of the router products software.

Support for the CIP2

The Enterprise/CIP2 image is now available, which supports the second-generation Channel Interface Processor (CIP2). The CIP2 is available for use with the Cisco 7000 series routers. 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% performance increase)
- Increased memory options (CIP2 memory configurations come in 32 MB, 64 MB, and 128 MB)
- An on-board bootflash, 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 Switch Processor (RSP7000) and Cisco 7000 series chassis interface (RSP7000CI) combination

The Enterprise/CIP2 image is required if you will be using the CIP2.

Note When the **show microcode** command is issued, both CIP and CIP2 microcode are listed as "CIP" and are distinguished only by the target hardware version shown: CIP microcode has a 4.*x* target hardware version, while CIP2 has a 5.*x* target hardware version. Also note that the image name for CIP2 microcode contains the prefix "cipp-" while the CIP image name prefix is "cip-."

New Software Features in Release 10.3(9)

This section describes new features and enhancements in Release 10.3(9) of the router products software.

Note The first few maintenance releases of each new Cisco IOS software release are used to deliver additional new features. Early maintenance releases of Release 10.3 include several major new features. You should consider the importance you place on maximizing product capability versus maximizing operational stability as they you to deploy a new release. An early release of software should always be tried in a test network before being deployed in a production network.

Cisco RSP7000

The Cisco 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.

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

New Software Features in Release 10.3(6)

This section describes new features and enhancements in Release 10.3(6) of the router products software.

Cisco 7505

The Cisco 7505 is a five-slot, multiprotocol, multimedia router/bridge. Network interfaces reside on interface processors, which provide a direct connection between the Cisco Extended Bus (CyBus) and external networks. The Cisco 7505 has four interface processor slots (0 through 3) and one slot for the Route Switch Processor (RSP1).

The RSP1 is the main system processor module for the Cisco 7505. It combines all of the switched routing and high-speed switching functions of the separate Route Processor (RP) and Switch Processor (SP), which are used in the Cisco 7000 series routers. Because the RSP1 combines the RP and SP functions, four slots are available for interface processors, allowing greater port density. The RSP1 contains the central processing unit (CPU) and most of the memory components for the Cisco 7505.

The Cisco IOS software images reside in Flash memory, which is located either on the RSP1, in the form of a single in-line memory module (SIMM), or on up to two Personal Computer Memory Card International Association (PCMCIA) cards (called Flash memory cards) that insert in the two PCMCIA slots (slots 0 and 1) on the front of the RSP1.

Cisco 7513

The Cisco 7513 is a 13-slot router that supports multiprotocol, multimedia routing and bridging with a wide variety of protocols and any combination of Asynchronous Transfer Mode (ATM), Ethernet, Fast Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), serial, High-Speed Serial Interface (HSSI), channel attachment, and multichannel media.

Network interfaces reside on interface processors that provide a direct connection between the two Cisco Extended Buses (CyBuses) and the user's external networks. The Cisco 7513 has 13 slots: interface processor slots 0 through 5, Route Switch Processor (RSP2) slots 6 and 7, and interface processor slots 8 through 12.

The RSP2 is the main system processor module for the Cisco 7513. It combines all of the switched routing and high-speed switching functions of the separate Route Processor (RP) and Switch Processor (SP), which are used in the Cisco 7000 series routers. The RSP2 contains the central processing unit (CPU) and most of the memory components for the Cisco 7513.

The Cisco IOS software images reside in Flash memory, which is located either on the RSP2, in the form of a single in-line memory module (SIMM), or on up to two Personal Computer Memory Card International Association (PCMCIA) cards (called Flash memory cards) inserted in the two PCMCIA slots (slots 0 and 1) on the front of the RSP2.

Cisco 4700

The Cisco 4700, a new member to the Cisco 4000 series, increases performance for high-bandwidth applications through a 133 MHz IDT ORION RISC CPU and a unique fast secondary memory cache. The combination of the RISC CPU and the secondary cache makes the Cisco 4700 one of the most powerful modular access routers in the industry.

The Cisco 4700 is completely compatible with the existing Network Processor Modules (NPMs) for the Cisco 4000 series (with the exception of the NP-1E). Just like the Cisco 4000 and 4500 systems, the Cisco 4700 provides three high-speed NPM slots. Available NPMs include Ethernet, Token Ring, FDDI, serial, Multiple ISDN BRI, ATM, and ISDN PRI.

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.

Standard Serial Interface Processor and Service Provider MultiChannel Interface Processor on the Cisco 7000 Series

The Cisco 7000 series now supports the Standard Serial Interface Processor (SSIP) and Service Provider MultiChannel Interface Processor (SMIP).

Fast Ethernet Interface Processor on the Cisco 7500 Series

The Cisco 7500 series supports the Fast Ethernet Interface Processor (FEIP) card, which allows communication speeds of 100 Mbps.

Multivendor Flash SIMM Support

Beginning with Release 10.3(6), you can use Flash Single in-line memory modules (SIMMs) from multiple vendors, as long as the total size of each SIMM is equal (if both slots are used, where available), and the SIMMs are installed in one of the combinations shown in Table 14 (for Cisco 2500 series and Cisco 4000-M, 4500, 4500-M, 4700, and 4700-M platforms) or Table 15 (for the AccessPro PC card and Cisco 2517 router).

Multivendor Flash support is restricted to platforms that use Rxboot Version 10.2(7a) or later, and Cisco IOS Release 10.2(8) or later. Currently, the Cisco 3000 series platforms and the Cisco 4000 platform do not support the multivendor Flash feature.

Cisco 2500 series routers (non AccessPro) and Cisco 4000-M, 4500, 4500-M, 4700, and 4700-M routers have two slots for Flash SIMMs. Table 14 provides the supported SIMM configurations.

Table 14 Cisco 2500 Series and Cisco 4000-M, 4500, 4500-M, 4700, and 4700-M Flash SIMM Support

SIMM Size	Vendor	Flash Bank	Considerations
4 MB	Intel (1Mbx8)	single	None
4 MB/4 MB	Intel/Intel (1Mbx8)	dual	None
4 MB/4 MB	Intel/AMD (1Mbx8)	dual	This configuration requires Rxboot Version 10.2(7a) or later. It also requires Cisco IOS Release 10.3(6).
8 MB	Intel (2Mbx8)	single	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(6) or later • 10.2(2) or later
8 MB/8 MB	Intel/Intel (2Mbx8)	dual	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(6) or later • 10.2(2) or later
8 MB/8 MB	Intel/AMD (2Mbx8)	dual	This configuration requires Rxboot Version 10.2(7a) or later. It also requires Cisco IOS Release 10.3(6).
4 MB	AMD (1Mbx8)	single	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(11) or later • 10.2(7) or later • 10.3(4) or later
4 MB/4 MB	AMD/AMD (1Mbx8)	dual	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(11) or later • 10.2(7) or later • 10.3(4) or later
8 MB	AMD (2Mbx8)	single	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(11) or later • 10.2(7) or later • 10.3(4) or later

SIMM Size	Vendor	Flash Bank	Considerations
8 MB/8 MB	AMD/AMD (2Mbx8)	dual	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(11) or later • 10.2(7) or later • 10.3(4) or later

The AccessPro PC card and Cisco 2517 router have one slot for a Flash SIMM. Table 15 provides the supported SIMM configurations.

Table 15 AccessPro PC Card and Cisco 2517 Flash SIMM Support

SIMM Size	Vendor	Flash Bank	Considerations
4 MB	Intel (1Mbx8)	single	None
8 MB	Intel (2Mbx8)	single	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(6) or later • 10.2(2) or later
8 MB	Intel (1Mbx8)	dual	None
16 MB	Intel (2Mbx8)	dual	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(6) or later • 10.2(2) or later
4 MB	AMD (1Mbx8)	single	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(11) or later • 10.2(7) or later • 10.3(4) or later
8 MB	AMD (2Mbx8)	single	This configuration requires Rxboot Version 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(11) or later • 10.2(7) or later • 10.3(4) or later

New Software Features in Release 10.3(5)

This section describes new features and enhancements in Release 10.3(5) of the router products software.

Fast Ethernet Interface Processor on the Cisco 7000 Series

The Cisco 7000 series supports the Fast Ethernet Interface Processor (FEIP) card, which allows communication speeds of 100 Mbps.

Cisco 1004

The Cisco 1004 is an ISDN router similar to the Cisco 1003. The Cisco 1003 has a B interface that is connected to an NT1, which is connected to the phone company's ISDN line. The Cisco 1004 has a built-in NT1. The Cisco 1004 has one console port, one Ethernet 10BaseT port, one Basic Rate Interface (BRI) port, and one PCMCIA card slot. The BRI port is the interface between the NT1 and the phone company's ISDN line.

FLEX 2.0

FLEX Version 2.0 now supports PPP compression on the serial interface for a LAN Extender. If you enable PPP compression on the interface, you must also disable fast switching on the interface.

New Software Features in Release 10.3(4)

This section describes new features and enhancements in Release 10.3(4) of the router products software.

Cisco 2517

The Cisco 2517 router/hub combines Cisco IOS routing technology with intelligent unshielded twisted pair (UTP) Token Ring hub media technology from LanOptics Ltd. The Cisco 2517 is designed for a branch or remote office that needs to link a single Token Ring LAN to a corporate data network or the Internet. It has 11 UTP Token Ring hub ports, two synchronous serial WAN ports, and one ISDN BRI port.

Cisco 4500 ATM NPM

Asynchronous Transfer Mode (ATM) is available on the Cisco 4500 router, which has a network processor module (NPM). ATM on the Cisco 4500 is configured differently from the ATM Interface Processor (AIP) on the Cisco 7000. Refer to the *Router Products Configuration Guide* for configuration information.

Cisco 4000 and Cisco 4500 Channelized T1/Channelized E1/PRI NIM

The Cisco 4000 series and Cisco 4500 series support a channelized T1 network interface module (NIM) and a channelized E1 NIM. They can be used both as channelized T1/E1 and as the physical media for the ISDN PRI protocol.

Dual Flash Bank MIB Support

The dual Flash bank Management Information Base (MIB) is supported in Release 10.3(4).

New Software Features in Release 10.3(3)

This section describes new features and enhancements in Release 10.3(3) of the router products software.

System Management

- AutoInstall over Frame Relay
  - Point-to-point subinterfaces are supported at the existing router. With the extended **frame-relay interface-dlci** command, you can use AutoInstall over Frame Relay to specify the serial interface address of the new router being configured from the existing router. This change allows the new router to resolve its IP address and continue with the AutoInstall procedure.
  - DOS-based Trivial File Transfer Protocol (TFTP) servers are supported. To avoid confusion with similarly named DOS files from other vendors and applications, the network-confg file and the router-confg file are named cisconet.cfg and ciscortr.cfg, respectively, on DOS-based TFTP servers. That is, when using a DOS-based TFTP server with AutoInstall, the new router will attempt to resolve its host name using the cisconet.cfg file. If the new router cannot resolve its host name, it attempts to load the ciscortr.cfg from the DOS-based TFTP server.
- Buffer management—The buffer cache shared by all the public buffer pools was removed. Instead, each interface buffer pool has its own buffer cache. A new buffer size exists, and the **show buffers** output is enhanced.
- AAA/TACACS+ —This latest version of the Terminal Access Controller Access Control System (TACACS) combines enhanced functionality and new authentication, authorization, and accounting (AAA) features.

Interfaces

- Dynamic Host Configuration Protocol (DHCP)—DHCP manages a group of IP addresses that are dynamically allocated to users logging in on asynchronous lines using Serial Line Internet Protocol (SLIP) or PPP. After the connection is terminated, the address is recycled into the address pool to be used again.
- Cisco 1003 support—A router that provides one Ethernet and one BRI port.
- CHAP and PAP authentication is enhanced with new TACACS+ support.

Routing Protocols

- AppleTalk Control Protocol (ATCP) for PPP—Using ATCP, remote users dialing in on an asynchronous interface via PPP can run AppleTalk and IP natively on a remote Macintosh, access AppleTalk zones from the Chooser, use networked peripherals, and share files with other Macintosh users.
- Route Summarization—You can configure the router to advertise a single route for all redistributed routes into OSPF.
- OSPF Metric Calculation—OSPF calculates metrics for an interface based on the interface's bandwidth.

Wide-Area Networking

- Stacker compression over LAPB—Cisco now supports Stacker compression over Link Access Protocol, Balanced (LAPB) or multi-LAPB encapsulation, in addition to the previously supported predictor-algorithm compression. Stacker compression is recommended when the bottleneck is caused by line bandwidth.
- Frame Relay dial backup for multipoint subinterfaces—Both point-to-point and multipoint Frame Relay subinterfaces can be configured with a backup interface. This feature enables individual PVCs to be backed up in case of failure—the entire Frame Relay connection need not fail before the backup takes over. Backup is provided for subinterface failure only, not for loading of the line.
- DDR over Frame Relay—Access to Frame Relay networks is now available through dial-up connections as well as leased lines. Dial-up connectivity allows Frame Relay networks to be extended to sites that do not generate enough traffic to justify leased lines and also allows a Frame Relay network to back up another network or point-to-point line. DDR over Frame Relay is supported for synchronous serial and ISDN interfaces and for rotary groups, and is available for in-band, DTR, and ISDN dialers.
- Transparent bridging over DDR—Cisco routers have supported transparent bridging over DDR since Release 10.0.
- ISDN semipermanent connections (Germany only)—German networks allow semipermanent connections between customer routers with BRIs and the 1TR6 basic rate switches in the exchange. Semipermanent connections are offered at better pricing than leased lines. Configuring BRIs for semipermanent connection requires only a new keyword for the **dialer map** command used to set up network addressing.

New Software Features in Release 10.3(2)

This section describes new features and enhancements in Release 10.3(2) of the router products software.

Source Route Switch

The Cisco 7000 series Source Route Switch (SRS) provides source-route transparent bridging with IP host functionality. This feature is available on Cisco 7000 and Cisco 7010 platforms. These platforms can have two to three Source Route Switch Token Ring Interface Processors (SRS-TRIPs) and two SRS-TRIPs with one Source Route FDDI Interface Processor that are running the SRS feature set.

Making hardware connections to SRS-TRIP interface processors and SRS-FIP-MM is identical to making hardware connections to TRIP interface processors. For information about making hardware connections, refer to the *Cisco 7000 Hardware Installation and Maintenance* and *Cisco 7010 Hardware Installation and Maintenance* publications.

Note that the SRS-TRIP and SRS-FIP-MM are not interchangeable with the TRIP or FIP-MM.

Note Cisco 7000 series Source Route Switch systems do not include any routing functionality.

Cisco 2516

The Cisco 2500 series includes the new Cisco 2516 router. The Cisco 2516 is a router with hub functionality. It has 1 Ethernet interface (14 ports), 2 serial interfaces, and 1 ISDN BRI interface.

DLSw+

Data link switching plus (DLSw+) is Cisco Systems' data link switching (DLSw) solution that allows construction of any-to-any networks with thousands of routers, while remaining compatible with the new DLSw standard and with the industry's most widely adopted Remote Source-Route Bridging (RSRB). DLSw is an emerging SNA-over-IP routing standard that helps to integrate SNA and NetBIOS protocols within routable IP protocols. DLSw+ requires much simpler configuration and administration.

New Software Features in Release 10.3(1)

This section describes new features and enhancements in the initial Cisco IOS Release 10.3 of the router products software.

Backbone Protocol Routing Features

This section describes the backbone protocol routing features that are new in the initial release of Cisco IOS Release 10.3.

IP Features

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

- Next Hop Resolution Protocol (NHRP)—Routers and hosts can use NHRP to discover the addresses of other routers and hosts connected to a nonbroadcast, multiaccess (NBMA) network. NHRP provides an ARP-like solution whereby systems attached to an NBMA network can dynamically learn the addresses of the other systems that are part of that network. These systems can then directly communicate without requiring traffic to use an intermediate hop.
- Virtual private network—NHRP can be used to facilitate building a virtual private network. In this context, a virtual private network consists of a virtual Layer 3 network that is built on top of an actual Layer 3 network. The topology you can use over the virtual private network can be largely independent of the underlying network, and the protocols you run over it can be completely independent of it.
- Hot Standby Router Protocol (HSRP) enhancements—HSRP now allows multiple routers on a LAN to provide fast backup for each other. Another new HSRP feature is the ability to configure a router so that its Hot Standby priority changes based on the availability of its interfaces.
- BGP COMMUNITIES attribute—To facilitate and simplify the control of routing information in BGP, destinations can be grouped into communities upon which routing decisions can be based.
- SSE fast switching of IP access lists—The silicon switching engine (SSE) in the Cisco 7000 series can now process both standard and extended IP access lists. That is, packets passing either standard or extended IP output access list checks can be silicon switched. SSE switching of IP packets is not supported if input access lists are used.
- Classless routing—The router can now forward packets destined for a subnet of a network that has no network default route to the best supernet route. Without classless routing, the router discards any packet destined for a subnet it does not recognize if no network default route exists.

- Flexible netmask display—IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. This feature allows you to display the netmask in dotted decimal, hexadecimal, or bitcount format.
- Offset to routing metrics enhancement—You can now limit an offset list to a particular interface or apply an access list to it. An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP and IGRP.
- IP extended access list enhancements—Improvements include the following:
  - The **established** keyword is now independent of port number filtering. Previously, you could not use **established** and filter on a port number. This enhancement allows more granularity in the use of **established**.
  - Port filtering and the **established** keyword are no longer presented as options during configuration unless they are applicable.
  - The Cisco IOS software now recognizes many names for TCP and UDP port numbers (for example, FTP, gopher, and talk).
  - The keyword **any** is now an abbreviation for "0.0.0.0 255.255.255.255" in standard and extended access lists.
  - Port filtering now supports filtering on a range of port numbers.
  - ICMP messages can be filtered by type and code. In addition, the Cisco IOS software now recognizes the names of all ICMP messages, so these can be specified by name as well as number.
  - IGMP messages can now be filtered by message type (number) or message name (DVMRP, host-query, host-report, PIM, and trace).
  - Packets can now be filtered by precedence level. Levels can be selected by name or number. Known names are *critical*, *flash*, *flash-override*, *immediate*, *internet*, *network*, *priority*, and *routine*.
  - When IP extended access lists are used to control access to and from router services (for example, **access-class 101 in**), ICMP, IGMP, precedence, and type of service filtering are not performed.
  - You can now filter on source ports for TCP and UDP using all of the same operators as destination ports.
  - The protocols Enhanced IGRP, ipinip (IP in IP), and OSPF are now known to the parser. Previously, you had to use explicit protocol numbers.
- The **show ip access-list** command has been added. Its output is identical to **show access-list**, but is IP specific and allows you to specify a particular access list. With no argument, it displays all simple and extended IP access lists.

Transparent Bridging Feature

The following feature has been added to Cisco's transparent bridging software:

- Transparently bridged virtual LANs—This feature permits a bridge group to extend outside the router to identify traffic switched within a bridge group.The software identifies the traffic by "coloring" the packets and encapsulating them in an 802.10 header. This feature is designed to control the propagation of bridged traffic in a shared backbone environment and effects a virtual LAN topology.

DECnet Features

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

- Dial-on-demand routing (DDR)—DDR now supports static routing of the DECnet Phase IV protocol. This is useful over circuit-switched connections.
- Dynamic DECnet route advertisements—When DECnet IV areas need to interconnect over a DECnet/OSI (Phase V) backbone, this feature dynamically advertises these routes in the DECnet IV table only if the route exists at the other side of the Phase V backbone. It also eliminates the need to configure matching CLNS static routes for every DECnet area that is advertised.
- DECnet host name-to-address mapping—A unique DECnet host address can now have an alphanumeric name associated with it. The router maintains a cache of host name-to-address mappings for use by the **show**, **ping**, and related DECnet support operations. This cache speeds the conversion of names to addresses.

ISO CLNS Features

The following feature has been added to Cisco's ISO CLNS software:

- Dial-on-demand routing (DDR)—DDR now supports static routing of the OSI/CLNS protocol over ISDN.

Desktop Protocol Features

This section describes the desktop protocol features that are new in the initial release of Cisco IOS Release 10.3.

AppleTalk Feature

The following feature has been added to Cisco's AppleTalk software:

- AppleTalk interenterprise routing—This feature provides support for AppleTalk internets, or domains. AppleTalk interenterprise routing allows two or more AppleTalk domains to be connected through a domain router. The domain router resolves conflicting AppleTalk network numbers or cable ranges from different domains and reduces hop-count between domains. With this feature, multiple AppleTalk domains can be internetworked with minimal effort into security-based environments with large-scale applications.

Banyan VINES Feature

The following feature has been added to Cisco's Banyan VINES software:

- Dial-on-demand routing (DDR)—In addition to AppleTalk, CLNS, DECnet IV, IP, IPX, and transparent bridging, DDR now supports static routing of Banyan VINES over ISDN.

Novell IPX Features

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

- NetWare Link Services Protocol (NLSP)—NLSP is a link-state routing protocol based on the OSI IS-IS protocol. Cisco's implementation of NLSP also includes NLSP MIB variables and tools to redistribute routing and SAP information between NLSP and other IPX routing protocols such as RIP, SAP, and Enhanced IGRP.

- IPXWAN Version 2.0—Our routers support IPXWAN Version 2.0 as defined in RFC 1634. The major enhancements to IPXWAN Version 1.0 are the ability to negotiate the use of NLSP and support for unnumbered IPX links. IPXWAN Version 2.0 is supported over permanent serial lines, X.25 switched and permanent virtual circuits, and Frame Relay permanent virtual circuits.
- IPX floating static routes—Static routes are traditionally implemented to always take precedence over any dynamically learned routes to the same destination network. A floating static route is a statically configured route that can be overridden by dynamically learned routing information. IPX can use a floating static route to create a path of last resort for situations when no dynamic information is available.

Wide-Area Networking Features

This section describes the wide-area networking features that are new in the initial release of Cisco IOS Release 10.3.

ATM Features

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

- Transparent bridging over ATM—The Cisco IOS software supports transparent bridging of Ethernet and FDDI traffic across an ATM backbone. Transparent bridging over ATM is useful when the protocol being supported is not routed (for example, LAT or NetBIOS) or when the user's network cannot support a structured addressing scheme.
- ATM per virtual circuit counters—Per-virtual-circuit counters improve the accuracy of the statistics shown in the output of **show** commands by ensuring that autonomously switched packets are counted, as well as fast-switched and process-switched packets.
- ATM DXI enhancement—RFC 1483 defines two encapsulation methods for multiplexing protocols onto ATM virtual circuits:
  - Virtual circuit multiplexing: This method has no encapsulation layer. Instead, all packets within a virtual circuit are expected to be of a certain protocol type (for example, IP or IPX).
  - LLC/SNAP: LLC/SNAP is encapsulation layer used on LANs such as 802.3 and 802.5. It allows any arbitrary set of network-level protocols to be supported on a single virtual circuit.

  Cisco's RFC 1483 support is now compliant with the ATM DXI 1a standard and allows RFC 1483 multiprotocol encapsulation over a serial or HSSI interface. Before Release 10.3, this encapsulation was only available over a native ATM interface.
- ATM OAM support for F5 cells—F5 OAM cells are used for monitoring virtual circuits. The F5 OAM cell provides a virtual circuit-level loopback. The router responds to the cells, thereby demonstrating that the circuit is up and the router is operational.
- AppleTalk and CLNS fast switching over ATM—AppleTalk and CLNS are now fast switched over ATM. Novell IPX and IP can also be fast switched; IP can also be autonomously switched or SSE-switched.

Frame Relay Features

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

- AutoInstall over Frame Relay—Cisco's AutoInstall feature provides simple router installation at a remote site from a centralized management location. The central location connects to the remote router via a serial line and downloads a configuration file. This feature supports autoinstallation over Frame Relay encapsulation on a serial line.

- Frame Relay bridging—Cisco now supports RFC 1490 encapsulation over Frame Relay for transparent bridging.
- SNA Frame Relay Access Device (FRAD)—FRAD provides RFC 1490 support for SNA devices. It allows IBM devices attached via SDLC, Token Ring, and Frame Relay to connect to other IBM devices across a Frame Relay network. FRAD uses two methods:
  - Remote source-route bridging over Frame Relay using direct encapsulation in Frame Relay according to RFC 1490.
  - Conversion of SDLC and LLC2 to Frame Relay according to the method specified in RFC 1490. This version is compatible with IBM FEPs (running NCP 7.1 or higher) and AS/400s.
- Frame Relay dial backup per DLCI—This feature allows individual Frame Relay data link connection identifiers (DLCIs) on a given physical interface to be backed up by another physical interface. If a DLCI fails and it is configured for backup, another physical interface will be used to reestablish the connection.

ISDN and DDR Features

The following features have been added to Cisco's ISDN and DDR software:

- DDR over LAPB—It is now possible to run LAPB encapsulation over DDR links, including ISDN. This feature augments the current encapsulations available, which are PPP, HDLC, and X.25.
- Fast call rerouting for ISDN—This feature allows a Cisco ISDN router to almost instantaneously call a second or subsequent ISDN destination if the initial call fails.
- ISDN PRI E1—An E1 version of the MultiChannel Interface Processor card is now available. This card can be used as an ISDN Primary Rate Interface (PRI) with the ISDN PRI signaling software available in Release 10.3. Initially, the ISDN PRI signaling will provide support for I.421 Euro-ISDN signaling in Europe.
- DDR fast switching—Fast switching is now enabled on ISDN over DDR lines, which previously could do only process switching.

X.25 and LAPB

The following feature has been added to Cisco's X.25 and LAPB software:

- LAPB priority queuing and custom queuing.

IBM Functionality Features

This section describes the IBM networks software features that are new in the initial release of Cisco IOS Release 10.3.

- DownStream Physical Unit (DSPU)—In networks running full-stack SNA gateways, each client system appears as an SNA PU. Each PU has a DLC connection to an upstream (that is, toward the mainframe) SNA device. In addition, each PU has a management session with ACF/VTAM in the mainframe. Because of the resulting high overhead, many environments use a gateway simply to consolidate the PUs and provide the appearance of a single PU to the mainframe. To eliminate the need for a separate gateway to provide this function, the Cisco IOS software now supports DSPU concentration.

- Source-route bridging over FDDI—The Cisco IOS software now supports source-route bridging (SRB) from Token Ring to Token Ring over FDDI on the Cisco 7000 series platforms. Now when you use SRB over FDDI, traffic is autonomously switched. SRB over FDDI does not support remote source-route bridging (RSRB).
- Fast explorer enhancement—Local explorer traffic (that is, explorers that come in on and go out on local Token Rings) is now handled at the interrupt level instead of the process level.
- Remote source-route bridging/TCP enhancement—This feature speeds up the transfer between a Token Ring and a TCP connection by providing a more streamlined path through the Cisco IOS software, eliminating unnecessary copies, executing at interrupt level, and using the IP route cache.
- Path MTU Discovery—Path MTU Discovery is a method for maximizing the use of available bandwidth in the network between the end points of a TCP connection. Customers using TCP connections to move bulk data between systems on distinct subnets can benefit most by enabling this feature. This group might include customers using RSRB with TCP encapsulation, STUN, X.25 remote switching (also known as XOT or X.25 over TCP), and some protocol translation configurations.

Network Management Features

This section describes the network management features that are new in the initial release of Cisco IOS Release 10.3.

- Cisco Discovery Protocol (CDP)—CDP is a protocol- and media-independent device discovery protocol that runs on all Cisco-manufactured equipment. It allows you to query Cisco devices on the network without affecting their configuration. By using CDP on a Cisco router, a device can advertise its existence to others and receive information about all other devices on the same LAN (or on the remote side of a WAN).
- Open Shortest Path First (OSPF) Version 2 Management Information Base (MIB)—This MIB provides RFC 1253 support. RFC 1253 defines standard objects and variables for managing OSPF Version 2.
- Cisco IOS privilege levels—This feature allows an administrator to establish privilege levels for the user interface. The administrator can establish up to 16 levels of access. The multilevel passwords allow the administrator to specify different levels of security for different commands.
- Command aliases—The administrator can now create aliases for Cisco IOS commands.

Access Server Features Supported on the Router

This section describes the access server features that are new in the initial release of Cisco IOS Release 10.3.

- PPP/SLIP protocol translation on virtual terminals—This enhancement to the protocol translation software allows a user on a Telnet, X.25 PAD, or LAT terminal server to make an appropriate connection to a router running protocol translation and then run SLIP or PPP for packet-oriented traffic.
- Asynchronous mobility—Asynchronous mobility allows mobile users with modems to connect to their private networks via a public network. Asynchronous mobility supports most remote node protocols in the first version. This means a mobile user can connect to an IPX corporate network using a public network that supports only IP protocols. The public network can be either a large corporate network or the Internet.

- Enable password—This feature allows you to specify an additional layer of security over the **enable password** command, first by enforcing the use of two passwords, and then by storing the **enable secret** using a non-reversible cryptographic function.

Important Notes

This section describes warnings and cautions about using the Cisco IOS Release 10.3 software. It discusses the following topics:

- Upgrading to a New Software Release
- Using AIP Cards
- Booting Cisco 4000 Routers
- IP Multicast and Mrouted
- Forwarding of Locally Sourced AppleTalk Packets
- Cisco 1000 LAN Extender Issues
- Using Source-Route Transparent Bridging and Source-Route Bridging on Cisco 2500 and Cisco 4000 Routers
- Release 10.3(11a) Fixes Caveat CSCdi56364
- Filtering IP Packets Based Upon Source Port
- Release 10.3(13a) Fixes Caveat CSCdi66673
- SRB on Releases 10.3(13.1) through 10.3(15)
- Release 10.3(16a) Fixes Caveat CSCdi71609
- Release 10.3(18a) Fixes Caveat CSCdj04270
- Release 10.3(19a) Fixes Caveat CSCdj37314

Upgrading to a New Software Release

If you are upgrading to Cisco IOS Release 10.3 from an earlier Cisco IOS software release, you should save your current configuration file before configuring your router with the Cisco IOS Release 10.3 software.

You should also verify that you have the necessary amount of memory, including main and shared DRAM memory and Flash memory.

Using AIP Cards

Cisco 7000 series AIP cards that support E3, DS3, or TAXI connections and that were shipped after February 22, 1995 require Cisco IOS Release 10.0(9), 10.2(5), or 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 10.3 rxboot image is too large to fit in the ROMs. (Note that this is not a problem for Cisco 4500 routers.) Therefore, you have to use the 9.14 rxboot image. However, because the Release 9.14 rxboot image does not recognize new network processor modules, such as the MBRI, its use causes two problems:

- You cannot boot from a network server over BRI lines. Instead, you can either boot from a network server over other media or use the **copy tftp flash** command to copy images over BRI or other media to Flash memory. If you use the **copy tftp flash** command over a BRI interface, you must be running the full system image.
- If you use the rxboot image on a Cisco 4000 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
```

IP Multicast and Mrouted

Version 3.3 of mrouted, which was announced on August 26, 1994, has a multicast traceroute facility that does not work through Cisco routers. Cisco routers do have multicast tracing utilities that can be used to manage multicast internetworks. An interoperable solution will be provided in a maintenance release of Cisco IOS Release 10.3.

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

Cisco 1000 LAN Extender Issues

The following issues affect the use of the Cisco 1000 series LAN Extender:

- The Cisco 1002 LAN Extender does not always properly sense when the WAN interface cable is unplugged and therefore does not display the LED blink error code of 1 as described in the Cisco 1000 documentation. Instead, the error code displayed could be 2 (no clock) or 6 (no PPP link). If either of these errors is displayed, verify that the cable is properly connected.
- Because the Cisco 1001 and 1002 models of LAN Extender are designed to operate as DTE devices only, they require the DCE to provide both a transmit and receive clock. A DSU/CSU or modem eliminator usually provides DCE. The Cisco MCI and SCI cards, which are used in the AGS+ router, do not supply a receive clock to the DTE and therefore cannot be connected directly to a Cisco 1000 with a DCE cable. The workaround is to use a different serial card or to install a modem eliminator in the line that supplies both the transmit and receive bit clocks.

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

Certain products containing a particular revision of Token Ring controllers do not support source-route transparent bridging (SRT). SRT is the concurrent operation of source route bridging (SRB) and transparent bridging on the same interface. The issue is confined to products containing the Texas Instruments TMS380C26 Token Ring controller. 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 source-route bridge protocols such as SNA and NetBIOS, and transparently bridge other protocols, such as IPX. In the other situation, SNA or NetBIOS uses source-route bridging and Windows NT is configured to use NetBIOS over IP. Certain other configuration alternatives do not require SRT (contact the Technical Assistance Center).

As of Release 10.3(1), source-route bridging (SRB) in the following Cisco IOS features sets is no longer supported: IP, IP/IPX, and Desktop. In order to use SRB, you need one of the following feature sets: IP/IBM base, IP/IPX/IBM base, Desktop/IBM base, or Enterprise. 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, Desktop/IBM base, or Enterprise.

Release 10.3(11a) Fixes Caveat CSCdi56364

After the release of Cisco IOS Release 10.3(11), a caveat was discovered within the gs7- set of Cisco IOS images. It was determined that this caveat was significant enough to merit a rebuild of the gs7- images. The rebuild includes the caveat fix and is renumbered to 10.3(11a).

The defect is bug CSCdi56364 and is described as follows:

On Cisco 7000 series routers, problems can occur if you attempt to reload microcode. These problems include the router unexpectedly restarting or inconsistent behavior by the card for which the microcode was reloaded, or both. [CSCdi56364]

Release 10.3(11a) and all subsequent releases of the Cisco IOS software, including Release 10.3(12), include the fix for this caveat.

Filtering IP Packets Based Upon Source Port

When filtering, never use the source port of a TCP or UDP packet to provide source authentication. Although Cisco products offer the ability to filter TCP and UDP packets based upon the TCP/UDP source port, relying on such filters to provide security is inadvisable. There are well-known, established techniques that can be used to subvert filter policies that rely on this information. In short, the source port of a TCP or UDP packet should never be relied on for authentication purposes.

Release 10.3(13a) Fixes Caveat CSCdi66673

After the release of Cisco IOS Release 10.3(13), a caveat was discovered within the rsp- Cisco IOS 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 10.3(13a).

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
```

Release 10.3(13a) and all subsequent releases of the Cisco IOS software, including Release 10.3(14), include the fix for this caveat.

SRB on Releases 10.3(13.1) through 10.3(15)

The igs, xx and c4500 images that support source-route bridging (SRB) are not available in Cisco IOS Version 10.3(15) because of a defect that is described in CSCdi71493.

This problem is specific to Cisco 2500 series and 4000 series routers running Cisco IOS releases 10.3(13.1) through 10.3(15). The problem shows up when doing SRB and routing on the same router over differing media types, with one of them being Token Ring.

A code fix is available in the Cisco IOS 10.3(15.4) interim release. The fix is also available in Cisco IOS Release 10.3(16).

Release 10.3(16a) Fixes Caveat CSCdi71609

After the release of Cisco IOS Release 10.3(16), a caveat was discovered within the rsp- Cisco IOS 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 10.3(16a). Release 10.3(16a) includes 10.3(16) images plus the rebuilt rsp- images.

This defect is bug CSCdi71609 and is described as follows:

A serious bug has been found within various Cisco IOS software releases. 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.

This problem can be avoided by disabling both Backing-Store and Fair Queuing on existing Cisco IOS software releases with rsp- images.

Release 10.3(16a) and all subsequent releases of Cisco IOS software, including Release 10.3(17), include the fix for this caveat.

Release 10.3(18a) Fixes Caveat CSCdj04270

After the release of Cisco IOS Release 10.3(18), a caveat was discovered, and it was determined that this caveat was significant enough to merit a rebuild of the 10.3 images. The rebuild includes the caveat fix and is renumbered to 10.3(18a).

This defect is bug CSCdj04270 and is described as follows:

When microcode Flash override is configured, and a microcode reload occurs, the router crashes. A workaround is to disable the **microcode flash override** command in configuration.

Release 10.3(18a) and all subsequent releases of Cisco IOS software, including Release 10.3(19), include the fix for this caveat.

Release 10.3(19a) Fixes Caveat CSCdj37314

After the release of Cisco IOS Release 10.3(19), a caveat was discovered, and it was determined that this caveat was significant enough to merit a rebuild of the 10.3 images. The rebuild includes the caveat fix and is renumbered to 10.3(19a).

This defect is bug CSCdj37314 and is described as follows:

PPP/CHAP Authentication was broken for some configurations.

Cisco IOS Release 10.3(19a) includes the fix for this caveat.

Release 10.3(19a) Caveats

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(19a). These caveats apply to all 10.3 releases up to and including 10.3(19a). The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

Basic System Services

- If the transmit queue limit is set to a low value (for example, through priority queuing), traffic on the interface might be subject to delayed transmission. [CSCdi35399]
- Certain information in Cisco 7513 routers cannot be accessed. Media Access Control (MAC) starting addresses are not assigned, so a MAC address must be entered for every Dallas chip (the MAC cookie chips on the Route Switch Processor [RSP] platform arbiter boards) on every Cisco 7513. The address must be allocated from the "OUI keeper." [CSCdi35766]
- 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 will 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 *completely* unconfigure the old card before replacing it with the new card. 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 card. Once the information that is displayed by the **show** commands is self-consistent, the newly inserted card behaves normally. [CSCdi49800]
- A Cisco 2500 router might crash every few hours because of a software-forced crash. [CSCdi70494]
- The **show stacks** command fails to report the correct version of code running at the time of the last reload. This problem occurs when the Flash version of the Cisco IOS software does not match the running version of code. [CSCdi74380]
- The following problem has been observed in Cisco IOS Release 10.3(10) and later: A router develops a memory leak after the **priority-group** command is removed from an interface. The leak will not develop if the router is reloaded after the command is removed. [CSCdj19094]
- Systems will not recognize the following Intel boot Flash SIMMS during boot Flash format: 28F004S5 (device code A7), 28F008S5 (device code A6), and 28F016S5 (device code AA).

  If you want to run these boot Flash devices and use images prior to this bug fix, you must format boot Flash with an image containing this bug fix. Then you may load an older image onto the newly formatted boot Flash SIMM. [CSCdj20651]

IBM Connectivity

- DLSw incorrectly shows a device both as source and destination in the reachability cache, after a session outage and subsequent recovery. [CSCdi29129]
- The data-link switching (DLSw) ring-list is intermittently not recognized. [CSCdi33453]
- In certain environments, when using RSRB, the router might discard explorer frames. These single-route explorer frames (for example, with a RIF RD of C270) seem to be mishandled by the router and sent to unused interfaces. Removing the configuration from the unused interfaces seems to solve the problem. [CSCdi86652]
- With RSRB direct encapsulation over FDDI, and with multiple routers that provide parallel paths from ring to ring, a router that is configured to peer to two different routers might show only one path in the **show source** output. [CSCdi91746]
- After you upgrade a Cisco 2504 to 10.3(16), a Novell SAA gateway is no longer able to connect via DLSw to a remote FEP. In the XID negotiation, the SAA Gateway complains about the maximum number of outstanding "I" frames. [CSCdj14967]

Interfaces and Bridging

- High-end routers intermittently drop Sequenced Packet Exchange (SPX) keepalive packets between local Token Rings. [CSCdi36291]
- If a serial interface is set to loopback via a hardware signal, the interface will remain in loopback until the hardware signal is dropped and a **no loopback** interface configuration command is issued. [CSCdi47768]
- Version 1.6 Revision C0 EIP cards might cause cache parity errors on all Cisco 7500 series and Cisco RSP7000 systems. The cache parity errors can cause system reloads. The hardware revision and version can be determined from the **show diag** command output. This problem is resolved in RSP EIP microcode version 20.2 and higher. (The microcode has been changed to alleviate the hardware problem with the "f" transceivers. The board has been revised to 1.6 D0 to replace the "f" transceivers with the "fr" part.) [CSCdi52082]
- Occasionally, a Switch Processor (SP) or Silicon Switch Processor (SSP) card fails, causing CBUS-3-INITERR (8034) errors. To fix this problem, replace the hardware. [CSCdi65219]
- When processing IPX (NCP) keepalive (watchdog) packets, the router adds an extra byte to the packet when SSE switching is enabled. [CSCdi66651]
- On an RSP router, the "%CBUS-3-CTRUCHECK" error message might be displayed and the Token Ring interface might reset. To prevent this problem, upgrade to RSP TRIP microcode version 20.1. [CSCdi74639]
- A Cisco 4500 can have packets simultaneously in the input queue and the output queue when a message is received on an FDDI or Ethernet interface. This results in apparent loss of incoming traffic when serial queues are filled.

  A workaround is to increase the Ethernet or FDDI's input hold queue size to larger than the sum of the serial output hold queue sizes or to congestive discard thresholds. [CSCdi78997]
- When bridging IP and routing AppleTalk, assigning the bridge group to the LEX interface causes AARP entries to disappear and to no longer be resolved. [CSCdj22825]

IP Routing Protocols

- IP packets sent to the Hot Standby Router Protocol (HSRP) virtual MAC address are not received if the packet is Subnetwork Access Protocol (SNAP)-encapsulated and the receiving interface is part of the ciscoBus or Switch Processor (SP) complex. [CSCdi39274]
- IP cache is erroneously not invalidated for destinations that use the default routes after the next hop is down. To work around this problem, execute the **clear ip cache** command. [CSCdj26446]
- If Enhanced IGRP is running natively, and an interface goes down, Enhanced IGRP topology entries that are from the redistribution of connected routes might not clear. [CSCdj28874]

ISO CLNS

- If secondary addresses are configured on an unnumbered interface, the interface routes corresponding to these addresses are not advertised in IS-IS. A workaround is to number the interface. [CSCdi60673]

LAT

- On a Cisco 2514 router running protocol translation from X.25 to LAT, the following message is displayed when about 70 sessions have been configured:

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

  [CSCdi82343]
- When configuring LAT services and translate statements, the following error messages may be displayed:

  ```
  %Translate: Can't set up LAT service name Insufficient memory to store new identification.
  ```

  [CSCdj01752]

VINES

- On Cisco 4500 routers, physical broadcast packets received on a Token Ring interface on which a **bridge** *bridge-group* **address** command is configured are repeatedly sent to other Token Ring interfaces. VINES uses physical broadcast to exchange RTP information. This behavior occurs in releases after Release 10.3(7). The workaround is to upgrade to Release 11.0 or 11.1 and to turn on VINES routing, or to remove the above **bridge** command from the configuration. [CSCdi74089]

Wide-Area Networking

- The AIP cannot be configured to issue idle cells instead of unassigned cells. [CSCdi48069]
- On an ATM interface, the following error message might be displayed even if the burst size is 32:

  ```
  tx output hung(800E = queue full)
  ```

  [CSCdi92985]

Release 10.3(18) Caveats/Release 10.3(19a) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(18). These caveats apply to all 10.3 releases up to and including 10.3(18). For additional caveats applicable to Release 10.3(18), see the caveats section for Release 10.3(19a), which precedes this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(19a).

Basic System Services

- 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 never seen on RSP systems that do not have serial interfaces. [CSCdj08573]

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, and user IDs and passwords before sending. [CSCdj06881]

IBM Connectivity

- A Cisco 7000 series router with SP microcode might crash when a buffer copy by the SP makes the RP wait too long, causing a bus error. [CSCdi77785]
- 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]
- Rarely, a DLSw circuit might become stuck in a "remote_resolve" state. To get the circuit out of this state, disable then reenable DLSw. [CSCdj07098]

Interfaces and Bridging

- 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 on 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]

- OIR removal of a FIP from one slot into another will cause the FDDI to permanently remain in DOWN/DOWN. You must reload to restart the FDDI. OIR removal and replacement back into the same slot works fine. [CSCdi87221]
- If you have a Cisco 4000 connected to a FDDI ring and to a Token Ring with several servers and clients on both of the rings, packets that go from the FDDI ring to the Token Ring might be corrupted. There is no corruption of the protocol or the checksum. There is no corruption of packets going from the Token Ring to the FDDI ring. [CSCdj05331]

IP Routing Protocols

- Sometimes OSPF neighbor lists become corrupted, preventing OSPF from forming adjacencies. This problem might also cause the router to crash. [CSCdj16875]

Wide-Area Networking

- A router may reload without producing a stack trace, or otherwise behave unpredictably, when routing an X.25 call that contains 16 bytes of Call User Data. There is no known workaround. [CSCdj10216]

Release 10.3(17) Caveats/Release 10.3(18) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(17). These caveats apply to all 10.3 releases up to and including 10.3(17). For additional caveats applicable to Release 10.3(17), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(18).

Basic System Services

- On Ethernets that experienced output errors, you might also see XBUFHDR and INVRTN errors. [CSCdi75404]
- 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]

IBM Connectivity

- Rarely, DLSw+ reachability entries might get stuck in the VERIFY state. This problem is timer related and will generally occur after several months of operation. [CSCdi93217]

Interfaces and Bridging

- When pinging over synchronous DDR with HDLC stack compression, the router will unexpectedly reset. [CSCdi79832]

- 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 get the FDDI up again. (OIR removal and replacing into the same slot works fine.) [CSCdi87221]

IP Routing Protocols

- When the **show standby** command is issued on a Cisco 4700 with HSRP configured on a FDDI interface, the router shows an incorrect priority and tracking interface status.

  After a reload with the **standby track** command configured, the tracked interface may be in a wrong state, so the priority is wrong too.

  If you load a software image with the fix for this bug, you will initially need to deconfigure the **standby track** command and reconfigure it again. [CSCdi72254]
- During topology changes, a lot of OSPF update packets can be generated and flooded throughout the network and overload the network. This overload situation can cause OSPF to lose neighbors. [CSCdi85902]
- An extended access list that denies IP traffic and that does not require transport layer information may let fragments go through if the *log* option is configured. As a workaround, do not configure the *log* option. [CSCdj00711]

ISO CLNS

- Router memory leaks if a router receives a CLNS packet with an invalid destination address length. [CSCdi90052]

Novell IPX, XNS, and Apollo Domain

- 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]
- 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]

Release 10.3(16) Caveats/Release 10.3(17) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(16). These caveats apply to all 10.3 releases up to and including 10.3(16). For additional caveats applicable to Release 10.3(16), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(17).

AppleTalk

- The router crashes 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. These conditions are unlikely to occur, so this problem is rare. There is no workaround. [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 the Cisco 7500 router. To work around this problem and bridge between the AGS+ and the Cisco 7500, you should use CSC-C2FCIT cards in the AGS+ and use 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 has to 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. Cisco recommends that you do not use encapsulated bridging. [CSCdi46862]

- The **boot config nvram:** configuration command, which was added for the RSP platform, interacts improperly when the **service compress-config** command is enabled. The **boot config** command causes the NVRAM to lock up, and the router must be rebooted to free the NVRAM. [CSCdi52587]

- 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 Release 10.3, this problem has been fixed in maintenance releases 10.3(16a), 10.3(17), and later 10.3 releases.

  To avoid this problem, Cisco recommends that you upgrade all Release 10.3 RSP-based systems to Cisco IOS Release 10.3(16a), 10.3(17), or a later release.

  For those systems that cannot be upgraded, you can avoid this problem by disabling Backing Store. Disable Backing-Store on each interface with the command **no transmit-buffers backing-store**. Backing-Store defaulted to OFF in images beginning with 10.3(12.3). 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. [CSCdi71609]

- 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 route cache version is unnecessarily bumped when a card is inserted or removed. In a heavily-loaded configuration, recomputing the cache will cause a substantial throughput impact. [CSCdi81376]

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

- If source-route bridging (SRB) explorer traffic is so low that no explorer is forwarded on a Token Ring interface for 25 days, then the Token Ring interface stops forwarding SRB explorers. The **show source** command shows that the "flushed" count increments for every explorer received, while no "expl_gn" explorers are counted to the remote peers. This problem causes connectivity loss. On more recent products, such as the Cisco 7500 series, these symptoms can occur on very active Token Ring interfaces after the Cisco IOS software is reloaded. A short-term workaround is to reload the affected router. [CSCdi70559]
- 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]
- 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]
- If a BIND request is received before the Notify response has arrived, DSPU will reject the BIND request with sense code 0x80050000. [CSCdi76085]
- When using DLSw+ to communicate with non-Cisco devices, the Cisco platform might incorrectly handle incoming transport keepalive packets. [CSCdi78202]

Interfaces and Bridging

- In rare situations, on ciscoBus interfaces on a Cisco AGS+ router, the router might stop accepting packets after you enable transparent bridging. Issuing the **show controllers cbus** command shows a Receive Queue Limit (RQL) of 0 for the affected interface and an unusually large RQL value for other interfaces. Issuing the **show interface** *type number* command shows an Ignore counted for every packet received on the affected interfaces. To recover from this problem, reload the router. To work around the problem, disable transparent bridging on the affected interfaces. [CSCdi54727]

- In Cisco 7500 series routers, the following error message might be displayed while booting the system image from TFTP or Flash memory, 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 load a new system image that has the fix for this bug. [CSCdi73130]
- On Cisco 4500 routers, physical broadcast packets received on a Token Ring interface that has the **bridge** *group* **address** *mac address action interface* command configured are repeatedly sent to other Token Ring interfaces. VINES uses physical broadcast to exchange RTP information. This behavior occurs in releases later than Cisco IOS Release 10.3(7). The workaround is to upgrade to Cisco IOS Release 11.0 or 11.1 and to turn on VINES routing, or to remove the above **bridge** command from the configuration. [CSCdi74089]
- Token Ring drivers that are bridging packets might misclassify IPX broadcast packets as SRB explorer packets and flush them rather than switch them. This problem occurs on low-end products only (for example, IGS *xx* or Cisco 4500 series platforms). No other protocol packets are affected; this is an IPX broadcast issue only. [CSCdi75134]
- During EOIR handling, some unnecessary disable commands are sent to EIP interfaces, with a concomitant processing time penalty. [CSCdi81394]
- The FDDI interface driver can 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. There is a spurious indication from the driver that the SPF recalculation needs to take place. [CSCdi81407]
- A Cisco 4000 was restarted by a bus error at hd64570_RX_interrupt. [CSCdj32193]

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]
- If the HSSI interface on a Cisco 7000 series router experiences an interruption and the router is running EIGRP, the router could experience very high utilization. The problem was found in Cisco IOS Release 10.3(16a). [CSCdj15781]
- A router may crash when running ipcache_update. [CSCdj37007]

ISO CLNS

- After you remove a static CLNS route, ISO-IGRP prefix routes might count to infinity around a looped topology. The workaround is to use the command **no clns router iso-igrp domain** 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 reject the incorrect address and NLSP routing may fail. NLSP

routers should use the address Internal-Network.0000.0000.0001 when sending NLSP packets. On WAN media that require MAPs for IPX, this should be the next hop address in the map statement. [CSCdi68981]

- 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 workaround, clear the IPX Enhanced IGRP neighbors. [CSCdi72438]
- NLSP might unnecessarily reflood both changed and unchanged LSP fragments. Typically this is not a problem on LAN circuits. However, this can present bandwidth-related problems on low speed WAN circuits, especially as the size of the network increases.

  This flooding behavior might prevent you from seeing another problem: services may be missing from the SAP table until the next full SPF. This is not a problem when all neighbors are Cisco routers, but can be a problem when third party routers are present on the same link. [CSCdi74487]
- XNS routes sometimes randomly age out, causing network instability as networks become unreachable and then are relearned. There are no workarounds for this problem. This problem was introduced in Cisco IOS interim build 10.3(15.4), and does not exist in Releases 10.3(1) through 10.3(15). [CSCdi82925]

TCP/IP Host-Mode Services

- Your router might crash at PC 0x12CFA8, address 0xD0D0D11. [CSCdi70432]
- Non-TCP reverse connections to lines may corrupt memory, resulting in a software-forced crash. [CSCdi79310]

Wide-Area Networking

- Outbound OAM cells may cause CBUS-3-OUTHUNG errors on an AIP. This will cause a reset of the AIP board, in turn causing ATM traffic to be dropped for a few seconds. This occurs only if rate-queue 0 (zero) is explicitly *not* configured, which means that automatic rate-queue configuration is not used *and* the rate-queue 0 is not used. [CSCdi60941]

Release 10.3(15) Caveats/Release 10.3(16) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(15). These caveats apply to all 10.3 releases up to and including 10.3(15). For additional caveats applicable to Release 10.3(15), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(16).

AppleTalk

- Over a period of three to five weeks, an active communication server slowly runs out of I/O memory. This problem might be related to AppleTalk Remote Access Protocol (ARAP) or TACACS+ usage. [CSCdi61152]
- When ARAP is configured, sometimes the following messages display:

```
%SYS-2-INPUTQ: INPUTQ set, but no idb, ptr=xxxxx %SYS-2-LINKED: Bad enqueue of xxxxx in
queue yyyyy
```

After this message displays, the router might also reload. [CSCdi63635]

- The **arap logging** command requires additional debugging 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]

DECnet

- DECnet might fail to work properly when using an area number of 63 for layer-2 (L2) routers. If this failure happens, you might be unable to ping (DECnet) between two area routers if one router is using area 63.x. This router might report that the "attached" flag is false when you issue the **show dec** command, even though the **show dec route** command shows routes to the router.

  To work around this problem, use the **decnet attach override** command to force the router into an attached state. [CSCdi69247]

IBM Connectivity

- Some IBM Logical Link Control, type 2 (LLC2) implementation devices send a RNR message and drop the frame when they run out of buffer space. This causes no data traffic flow for 30 seconds. (Non-IBM LLC2 devices that use IEEE LLC2 will send REJ messages rather than RNR messages and no delay occurs.) [CSCdi49447]
- If you are using a direct Escon-attached Channel Interface Processor (CIP), the CIP might enter a boxed state if the router is reloaded. This problem is more likely to occur if the CIP is connected through a director, or if the CIP is taken off-line before the router is reloaded. To work around this problem, vary the device off-line before reloading the router. [CSCdi59440]
- When running CIP Systems Network Architecture (SNA) over data-link switching (DLSw), the LLC2 control blocks might not get freed even when the LLC2 session is lost and the DLSw circuit is gone. The workaround is to reload the router. [CSCdi62627]
- SNA sessions using Qualified Logical Link Control (QLLC) over X.25 permanent virtual circuits (PVCs) do not become active. The following tracebacks are a symptom of this problem: [CSCdi66340]

  ```
  %SYS-2-LINKED: Bad enqueue of 9600E8 in queue 88380.
  SNA: Alert xxxxx not sent, Focal point buffer overflowed.
  ```

- If a Cisco 7000 series router Channel Interface Processor (CIP) gets into a hung state, the Cisco IOS software might enter a loop trying to reset it. The following messages will be continually reported:

  ```
  %CBUS-3-CIPRSET: Interface Channel slot/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)
  ```

  These looping messages might overrun the logging buffer and negate the reason for the initial attempt at resetting the CIP. The looping might be so severe that a reboot of the router is required. [CSCdi66420]

- A router might reload if Seg-V violations at 0x0 occur while the router is getting tracebacks that point at data-link switching (DLSw). [CSCdi67085]
- The router crashes if NSP is configured and is trying to connect back to the owning host. [CSCdi69231]
- When using DLSw Fast Sequenced Transport (FST), end user sessions might be unable to switch over to an alternate LAN or peer path if there is a connectivity failure. [CSCdi70709]
- If a Cisco 2500 series or 4000 series router has source-route bridging (SRB) enabled on two or more interfaces, and if routing is occurring on any other interface, the router will drop packets causing session loss. [CSCdi71493]

Interfaces and Bridging

- When you perform buffer changes on a serial interface with Switched Multimegabit Data Service (SMDS) encapsulation, these changes are not saved if you reload. [CSCdi62516]
- The **source-bridge** *ring-number* command erroneously allows you to configure a ring-number mismatch. To work around this problem, ensure that all bridge devices on a ring use 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 High-Level Data Link Control [HDLC] to Switched Multimegabit Data Service [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.

  One possible workaround for this problem is to issue the **microcode reload** command. [CSCdi66450]
- If you reseat a MultiChannel Interface Processor (MIP) card, your encapsulation configuration might be erased. [CSCdi66915]
- 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 is passed uncompressed. This can result in compression ratios that are lower than expected. [CSCdi71367]

IP Routing Protocols

- IPX Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) updates do not propagate if the maximum transmission unit (MTU) size is less than the IPX Enhanced IGRP packet size. [CSCdi65486]
- Processing of input offset lists in Enhanced IGRP is erroneously disabled, so offset list processing is not available. [CSCdi65889]
- If you have neighbor statements pointing to a subnet broadcast address, your router might fail to send updates to that broadcast address. [CSCdi67411]

Novell IPX, XNS, and Apollo Domain

- IPX Service Advertisement Protocol (SAP) table entries use too much memory (as much as 300% too much). [CSCdi65740]

Wide-Area Networking

- Integrated Services Digital Network (ISDN) NET3 cannot handle incoming FACILITY messages when a call is connected. [CSCdi60340]
- Dialing into an asynchronous line and starting a Serial Line Internet Protocol (SLIP)/Point-to-Point Protocol (PPP) session might fail even though the same IP address was previously allocated successfully for the same user. [CSCdi63143]
- Using ATM Interface Processor (AIP) microcode version 20.8 might cause the AIP board to lock into a state where it transmits corrupted packets. This problem also occurs if you use AIP microcode version 10.15 of Router Processor (RP)-based platforms.

  This problem causes the **debug atm** error "ATM(ATM9/0.1): VC(1) Bad SAP ..." at the receive side of the ATM virtual circuit (VC). The transmission of data is usually affected in one direction only. The problem might 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 switched virtual circuit (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 to issue the command **clear int atm 5/0** on the transmit side. [CSCdi67812]
- When dialing into an AS5200 from an I-Courier modem over sync ISDN and then starting a PPP session, the router may crash. This occurs only when login is done on a non-async interface and when extended TACACS is enabled. A workaround for non-async interfaces is to use AAA/TACACS+. [CSCdi68257]
- A router might crash if it attempts to process a corrupted or malformed Frame Relay Local Management Interface (LMI) message. The problem is independent of platform type. The cause of corrupted LMI messages is currently unknown. [CSCdi68330]

Release 10.3(14) Caveats

Release 10.3(14) was not officially released.

Release 10.3(13) Caveats/Release 10.3(15) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(13). These caveats apply to all 10.3 releases up to and including 10.3(13). For additional caveats applicable to Release 10.3(13), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(15).

Additionally, one caveat was resolved in a special release prior to 10.3(15), as well as in Release 10.3(14). This release was named 10.3(13a) and is described in the following paragraphs.

Cisco IOS Release 10.3(13a)

The Cisco IOS Release 10.3(13) VIP feature set images were rebuilt to include a single defect fix, and were renumbered to 10.3(13a). 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
```

AppleTalk

- Routers send NBP lookup (LkUp) packets for nonextended networks and also fail to convert NBP BrRq packets to NBP FwdReq packets. This behavior is not in compliance with specifications.

  If your router is directly connected to a Phase 1 (non-Phase 2) router in compatibility mode, you can use the **appletalk proxy-nbp** *network zone* command to allow the router to convert NBP FwdReq packets to NBP LkUp packets that are sent to the Phase 1 router. [CSCdi61668]

- A router configured with AppleTalk and Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) takes too long to age out routes, even when the link is down. This causes too long of a convergent time for features like backup interface. [CSCdi62796]

- IPTalk does not function correctly. No IPTalk packets are processed through the router. [CSCdi64165]

Basic System Services

- Cisco 7500 series routers cannot fast switch packets of a size greater than 8192 bytes. These packets are switched at the process level, a lower performance path. [CSCdi60295]
- If you issue the **snmp-server party** and **snmp-server context** configuration commands, the system will sometimes reload. Neither of these commands verify that the configured OID is not already in use, which permits multiple records to be configured with the same OID. This violates the rule that each record must have a unique OID. To work around this problem, do not configure OIDs that conflict with the initial party and context OIDs as specified in RFC 1447. [CSCdi63694]
- A Route Switch Processor (RSP1, RSP2, or RSP7000) might crash if the system receives a reserved exception. If this crash occurs, the following messages will display:

```
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 08000000
*** 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
```

  You might also get errors that cause a switching complex restart if an EIP port receives a runt packet. If this happens, you will see error messages such as: [CSCdi66673]

```
Jun 17 10:50:23.329: %RSP-2-QAERROR: reused or zero link error, write at addr 0308 (QA)
 log 260308C0, data A816FFFF 00000000
```

IBM Connectivity

- If remote source-route bridging is configured on a Cisco 4500-M router or a Cisco 4700 router, the router might restart with the error message "%ALIGN-1-FATAL: Illegal access to a low address." [CSCdi35905]
- In a parallel SDLLC network, sometimes ACTPU responses are not received by the host. [CSCdi55142]
- Valid multicast explorers that should be handed to the protocol stack are instead diverted to the source-route bridging (SRB) module, and are then flushed by the SRB explorer control mechanism. The flushing can be avoided by raising the explorer maxrate value to a high number. However, this might cause instability in the network. [CSCdi59090]
- DLSW NetBIOS cannot connect to Windows NT. [CSCdi62784]
- Configuring **dlsw remote-peer** *cost* has no effect on peer selection. All peers shown in **show dlsw capabilities** show equal costs. [CSCdi64537]
- If you are using Synchronous Data Link Control with data-link switching plus, sessions will fail to be reestablished after a physical unit is reset. [CSCdi64828]
- A Cisco 7000 series router or Cisco 4000 series router that is running remote source-route bridging (RSRB) might crash with the message "%ALIGN-1-FATAL: Illegal access to low address from srb_enq." [CSCdi65489]

Interfaces and Bridging

- If a packet has a Hot Standby Router Protocol (HSRP) destination MAC address, it is process switched, regardless of the route-cache status on the interface. [CSCdi44437]
- You might sometimes get the following message if the interface cable is changed or if the remote end goes down and then comes back up:

```
PC2PR2#show interface serial 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
```

  To resolve this problem, try the following workarounds in the order listed. Note that a router reload is not needed.

  — Workaround #1: The first suggested workaround allows the problem interface to be brought on line without resetting every interface in the ciscoBus complex.

    To work around, enter the ciscoBus test mode, select the problem interface, and read a portion of the interface processor memory.

    The following 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 00000: 0001 FFFC
FSIP Mem 00004: 0000 01C6
FSIP Mem 00008: 0000 049A
FSIP Mem 0000C: 0000 049A
FSIP Mem 00010: 0000 049A
FSIP Mem 00014: 0000 049A
FSIP Mem 00018: 0000 049A
FSIP Mem 0001C: 0000 049A
FSIP Mem 00020: 0000 049A
```

  — Workaround #2: If workaround #1 fails to bring the interface up, issue the **microcode reload** command. This workaround resets all the interfaces in the ciscoBus complex. [CSCdi57573]

- If you issue the **smt-queue-threshold** command, Fiber Distributed Data Interfaces (FDDIs) will begin to drop Station Management (SMT) frames. This causes the interface to intermittently drop out, which causes ring instability. Also, the **no smt-queue-threshold** command does not work. To turn off this faulty function, you must remove the FDDI interface, reboot the router, issue the **write memory** command, and then bring back the interface. [CSCdi62177]
- A router running Frame Relay crashes at “bridge_enq” even when bridging is not configured. [CSCdi63140]
- FSIP microcode does not recognize DCE leads during a cutover from a Cisco 2501 serial port. [CSCdi64735]

IP Routing Protocols

- OSPF fails under the following conditions: An external LSA with a non-zero forwarding address is defined, the router has a non-OSPF route for the forwarding address, and then the non-OSPF route is removed. When the route is removed, OSPF crashes. There is no workaround for the problem. However, in general, no more than one routing protocol should be run over the same topology, so no non-OSPF route for forwarding addresses should exist, and the crash will not happen. [CSCdi61864]
- A directly connected route might disappear from the IPX Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) topology table if the interface that is configured for IPX Enhanced IGRP goes down and comes back up in a brief period of time (for example, 2 seconds). The workaround to this problem is to issue the commands **shut** and **no shut** for the interface. [CSCdi65345]

Novell IPX, XNS, and Apollo Domain

- Rarely, NetWare Link Services Protocol (NLSP) will not report information learned from the Routing Information Protocol (RIP) or Service Access Protocol (SAP). [CSCdi45425]
- If you define a static IPX route using the peer address of an IPX WAN neighbor, the route might fail with a message about multicast addresses. The workaround to this problem is to avoid using eight-digit IPX internal network numbers with an odd-numbered first byte. Use a seven-digit or shorter length IPX internal address to avoid this error message. [CSCdi61993]
- Using IPX-Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) can cause a memory leak if a link with an Enhanced IGRP neighbor is flapping. The Service Advertisement Protocol (SAP) updates get queued and backed up, thus using increasingly more memory. [CSCdi66169]

Wide-Area Networking

- The global command **printer** *printername* **line** *line#* will not function correctly unless either the **newline-convert** option or **formfeed** option is on. [CSCdi63342]
- Password Authentication Protocol (PAP) authentication fails when using TACACS+ as an authentication method for the Point-to-Point Protocol (PPP). [CSCdi66077]

Release 10.3(12) Caveats/Release 10.3(13) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(12). These caveats apply to all 10.3 releases up to and including 10.3(12). For additional caveats applicable to Release 10.3(12), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(13).

AppleTalk

- AppleTalk Remote Access (ARA) connection failures occur at higher rates with the use of 28,800 kbps modems (for example, V.34, V.fc, and V.FAST modems). These connection failures result in “bad exit” and “forced quit” error messages. [CSCdi57713]

- A MacIP server will not give an IP address to MacIP clients if the next address to give out is currently being use by a genuine IP device. This happens because the MacIP server does not skip over that IP address and assign the next available address. [CSCdi61526]

Basic System Services

- Sometimes runt ethernet packets are not correctly processed. [CSCdi55978]
- Configuring custom/priority queuing on an MBRI interface causes performance degradation. [CSCdi56473]
- Backing store queuing is turned on by default, which might cause serious performance degradation during peak activity if you have a router with slow interface processors and the outbound traffic rate exceeds the media speed. To help alleviate this problem, turn backing store queuing off if you have a router which allows you to do so (for example, if you have a Route Switch Processor [RSP]). [CSCdi57740]
- An RSP router can sometimes crash with a "reserved exception" error. [CSCdi58658]
- The AutoInstall feature does not work in an RSP. [CSCdi59063]
- If you reload or issue the **configure memory** command after issuing the **aaa authorization exec** command, you might lose your configuration. However, if you do not issue the **aaa accounting exec start-stop tacacs+** command during configuration, this problem will not occur. [CSCdi60172]

DECnet

- A router running DECnet might present ALIGN-3-SPURIOUS error messages. This problem will occur if the adjacency between neighbors expires. This is a cosmetic problem and has no other impact on the router. [CSCdi60716]

EXEC and Configuration Parser

- The **write memory** and **copy running-config startup-config** commands work at privilege level 15. However, the remaining **write** and **copy running-config** commands still operate at the users' current privilege level, because of security considerations. [CSCdi55809]

IBM Connectivity

- Removing remote source-route bridging (RSRB) peers might cause the router to suspend indefinitely. [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]
- 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]
- If a new CIP internal LAN interface is added following a dBus internal error, the CIP Virtual Port x/2 might not be found. To work around this problem, reload the router. [CSCdi54224]
- You might encounter a problem with Frame Relay access support (FRAS) and receive the message "IBM: Unknown L3 PID, fr_doencap failed." To work around this problem, you should use Cisco IOS Release 10.3(7.5) or lower. [CSCdi58769]

- If your router is using promiscuous TCP peers, the router might crash with the message "System restarted by bus error at PC 0xD0D0D0D, address 0x0." The crash occurs when peer structures get deleted because of transmission line problems, peer routers reloads, or other connection problems, while still being used by TCP. The workaround to this problem is to define static peers. [CSCdi58842]
- The **lnm resync** command does not work on Cisco 7000 series routers if the router is configured for IBM automatic spanning tree (AST) support. [CSCdi59890]
- Data-link switching (DLSw) Ethernet 802.5 frames will be corrupted after a logical link control (LLC) retransmission. [CSCdi60102]
- The router might sometimes crash with the message, "System restarted by bus error at PC 0xD0D0D0D, address 0x0." This crash happens if you are using promiscuous TCP peers and the peer structures get deleted while still being used by TCP. This might occur if you have transmission line problems, peer router reloads, or other line problems. The work around to this problem is to define static peers. [CSCdi61278]
- Connections cannot be established when you use IBM process-switched features such as RSRB/TCP, DLSw+/TCP, etc., because of dropped packets. The router displays "dropped Routed protocol" messages if you enable **debug source-bridge error**. [CSCdi62738]

Interfaces and Bridging

- Cisco 4500 routers cannot bridge IPX unicast packets between Ethernet and Fiber Distributed Data Interface (FDDI) environments. [CSCdi53363]
- If you issue the **show controllers cache** command and press the space bar to page down, the router will suspend indefinitely. The only workaround is to power cycle the router. [CSCdi56241]
- 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]
- NetBIOS SABME (set asynchronous balanced mode extended) messages are not correctly bridged from FDDI to serial lines using High-Level Data Link Control (HDLC) encapsulation, even though the bridging of SABME messages from FDDI to Ethernet works correctly. [CSCdi58733]
- If **fddi encapsulate** is configured on an FDDI Interface Processor (FIP) interface, the router may reload with a bus error. The error happens if encapsulated packets are in Ethernet-like format. This problem is specific to 10.3 only. [CSCdi59182]
- If IPX broadcast packets are present on a Token Ring that is attached to a Cisco 4000, Cisco 4500, or Cisco 4700 router, and neither IPX routing nor bridging is configured on the router, the router will lose other broadcast packets on the Token Ring. This can cause secondary failures in protocols such as Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) and Intermediate System-to-Intermediate System (IS-IS). To work around this problem, configure **ipx routing**. It is not necessary to assign any IPX addresses in the router, so it will not actually participate in IPX. [CSCdi61501]
- If your router passes compressed, bridged traffic on HDLC WAN links, you will receive many errors such as "Decompression size error." The router sometimes also crashes when processing these packets. [CSCdi63245]

IP Routing Protocols

- If an Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) candidate default route is overwritten by another protocol, the Enhanced IGRP topology table might 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]
- 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. [CSCdi61491]
- The Open Shortest Path First (OSPF) protocol might crash if there are parallel intra-area paths. [CSCdi62870]
- If your router passes compressed, bridged traffic on High-Level Data Link Control (HDLC) WAN links, many errors of the type "Decompression size error" might occur. The router might also crash when processing these packets. [CSCdi63245]

ISO CLNS

- A router reload may occur when Connectionless Network Service (CLNS) traffic is fast-switched. [CSCdi57629]
- If your router is under a heavy load and you use Intermediate System-to-Intermediate System (IS-IS) or NetWare Link Services Protocol (NLSP), packets might be dropped unnecessarily. [CSCdi58433]
- If a non-Cisco router is running IS-IS on a level-1-only circuit and the router is sending End System-to-Intermediate System (ES-IS) End System Hello (ESH) messages, a Cisco router might not recognize the ESH messages. A workaround is to filter out the ESH packets using the **clns adjacency-filter es** configuration command in conjunction with setting an appropriate filter. The filter should specify a wildcard (**) in the last byte of the address. [CSCdi58621]
- 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 to this problem is to manually clear the adjacency database using the **clear clns neighbors** command on the reconfigured router and on all of its neighboring routers. You can also restart the router to work around this problem. [CSCdi58953]

Novell IPX, XNS, and Apollo Domain

- IPX Simple Network Management Protocol (SNMP) requests sent to the router might accumulate in the input queue when SNMP is disabled. These packets are not processed, which can cause input queues to fill up. [CSCdi57589]
- Infrequently, Intermediate System-to-Intermediate System (IS-IS) and NetWare Link Services Protocol (NLSP) link-state packets (LSPs) are not transmitted on point-to-point interfaces. [CSCdi58613]
- If you issue the **no ipx router eigrp** *autonomous system number* command, the router might reload if there are a lot of service access points (SAPs) defined in the router and if the SAP table was changing while the command was performed. [CSCdi60174]
- Sometimes an damaged IPX packet is received which has an incorrect IPX length in the IPX header, but the CRC field is correct. When this happens, the packet is erroneously processed and padded to the length specified in the IPX header, instead of being correctly discarded. [CSCdi63412]

- An alignment error exists, particularly for IPX frames routed from Token Rings with multiring enabled. This alignment error exists both in process switched paths and in some fast-switched paths. [CSCdi63741]
- 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. [CSCdi63771]

VINES

- The Cisco 1001 LAN Extender does not work with VINES if a remote LAN is connected to a core router through the LAN Extender. [CSCdi57934]
- VINES clients than run Oracle application programs cannot connect to a server, because packets are reordered when the VINES route cache is enabled. A workaround is to use process switching for applications which can not handle out-of-sequence packets. [CSCdi59059]

Wide-Area Networking

- The amount of free system memory might decrease if you issue the **dialer hold-queue** command over an ISDN interface. [CSCdi58402]
- Serial lines that use Switched Multi-megabit Data Service (SMDS) encapsulation might encounter SegV catastrophic failures if the lines are enabled after a router reboot. [CSCdi60761]

Release 10.3(11) Caveats/Release 10.3(12) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(11). These caveats apply to all 10.3 releases up to and including 10.3(11). For additional caveats applicable to Release 10.3(11), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(12).

Additionally, one caveat was resolved in a special release prior to 10.3(12), as well as in Release 10.3(12). This special release was named 10.3(11a) and is described in the following paragraphs.

Cisco IOS Release 10.3(11a)

The Cisco IOS Release 10.3(11) gs7- images were rebuilt to include a single defect fix, and were renumbered to 10.3(11a). The defect is bug CSCdi56364 and is described as follows:

On Cisco 7000 series routers, problems can occur if you attempt to reload microcode. These problems include the router unexpectedly restarting or inconsistent behavior by the card for which the microcode was reloaded, or both. [CSCdi56364]

AppleTalk

- AppleTalk print jobs fail when an AppleTalk packet traveling from ATM to Ethernet receives an improper 802.3 packet length. This problem can cause the AppleTalk Printer Access Protocol to fail, and HP LaserJet printers with the AppleTalk compatible HP JetDirect card will discard these packets. [CSCdi53747]

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 compatible only with Cisco 7000 series routers. [CSCdi44138]
- A Cisco 7500 series router might suspend indefinitely if Frame Relay interfaces are active at the same time as MultiChannel Interface Processor (MIP) channel groups. [CSCdi49868]
- Sometimes optimum switching is disabled upon router reboot. [CSCdi54567]
- A memory leak might occur on Cisco 7000 routers if small buffers are created but are not properly trimmed. This is most likely to occur if remote source-route bridging (RSRB) or explorer packets are received with a wrong Subnetwork Access Protocol (SNAP) type value. [CSCdi54739]
- Under some conditions, Simple Network Management Protocol (SNMP) queries of the Cisco Environmental Monitor Management Information Base (MIB) can cause the system to reload. This occurs when an SNMP get-request operation tries to retrieve instance 0 of an object in the ciscoEnvMonSupplyStatusTable. Because 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-request operations that specify instance 0 for objects in the Cisco Environmental Monitor MIB. Instead, applications should either use SNMP get-request operations starting with instance 1, or else use SNMP get-next-request or get-bulk-request operations. [CSCdi55599]

DECnet

- When DECnet conversion is enabled, discard routes are inserted into the Connectionless Network Service (CLNS) routing table. [CSCdi40503]

IBM Connectivity

- In certain mixed-vendor bridge environments, the automatic spanning tree (AST) never becomes active if a Cisco device is the root bridge. Bridge protocol data units (BPDUs) are constantly exchanged, but the spanning tree topology never develops or becomes active. [CSCdi53651]
- A LAN Network Manager (LNM) might fail to link to a router's source bridge, after a Token Ring interface is shut down on a remote router. The **show lnm bridge** command continues to display an active link to the LAN network manager. This problem does not occur with bridges that are locally linked to the LAN manager. To work around, first remove and then reconfigure the **source-bridge** command from the Token Ring interface. [CSCdi53954]
- A Cisco 4500 series or Cisco 7500 series router might crash if downstream physical unit (DSPU) debugging is enabled. [CSCdi54277]
- On a Cisco 7500 router, IPX routes are not received from Fiber Distributed Data Interfaces (FDDIs) when remote source-route bridging (RSRB) traffic is passed. [CSCdi54402]
- Some NetBIOS applications that require a UI frame in response to an Add Name Query are not able to connect using a data-link switching (DLSw) peer-on-demand. This problem occurs if the NetBIOS circuit is the initial circuit that triggers the peer-on-demand connection. [CSCdi54796]
- New Systems Network Architecture (SNA) sessions fail to connect to a front-end processor, when duplicate ring numbers are in the Routing Information Field (RIF). To work around, issue the **clear rif-cache** command. [CSCdi55032]

- Packets might be dropped if they are received for a Fast-Sequenced Transport (FST) promiscuous peer while that peer is still setting up the connection. [CSCdi55219]
- Issuing a **no source-bridge remote-peer** command might sometimes cause the bus error "address 0xd0d0d0d0" and a router reload. [CSCdi55919]
- Connections to dependent logical units (DLUs) with downstream physical unit (DSPU) or Advanced Peer-to-Peer Networking (APPN) across RSRB might fail when the remote service access point (SAP) address is not enabled at the destination router. The workaround is to enable the remote SAP address. [CSCdi56660]
- DLSw Fast-Sequenced Transport (FST) encapsulation does not work over a WAN Token Ring or over FDDI. [CSCdi57207]

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 via the command **no ipx pad-process-switched-packets**.

  — Configure the router for autonomous switching instead of silicon switching engine (SSE) switching via the commands **no ipx route-cache sse** and **ipx route-cache cbus**.

  — Turn off SSE switching via the command **no ipx route-cache sse**. [CSCdi42802]
- A Cisco 7000 series router with a Silicon Switch Processor (SSP) might reload if you configure access lists (to be used for packet filtering) that contain an entry matching all IP packets, followed by two or more entries. To work around, remove all access list entries following the entry that matches all packets. (This workaround will not change the behavior of the access list.) [CSCdi50886]
- Very rarely, a router will repeatedly display the following error message:

  ```
  %SYS-6-STACKLOW: Stack for level CXBus Interfaces running low, 0/1000
  ```

  When this behavior occurs, the router might also eventually suspend indefinitely. [CSCdi54119]
- When you boot a Cisco 7500 router, the FIP Fiber Distributed Data Interface (FDDI) might momentarily beacon the FDDI ring. This can cause ring instability. [CSCdi54444]
- If a Token Ring Interface Processor (TRIP) is present in Cisco 7000 series routers, Token Rings that beacon frequently can degrade router performance. [CSCdi55758]
- After starting connection management (CMT), the router waits only 1 second for a FDDI interface to come up. This wait might not be long enough, because some FDDI rings require the router to wait five seconds instead. [CSCdi55837]

IP Routing Protocols

- A small delay occurs between the time Open Shortest Path First (OSPF) marks a link-state advertisement (LSA) as deleted and the time the LSA is actually removed. Within this small window, if OSPF receives an old copy of the LSA with a higher sequence number, OSPF cannot resolve the conflict and is unable to remove the LSA. The old LSA copy is most likely received from some new neighbors through database exchange. You will observe a self-originated LSA stuck in the database. [CSCdi48102]

- OSPF sometimes puts incorrect information in the source field for stub routes. This prevents the Border Gateway Protocol (BGP) from advertising the stub route to peers, because the route will not be synchronized. [CSCdi49377]
- The system might fail when a **no router eigrp** *as-number* command is issued and summary routes are present. A workaround is to turn off auto-summary and deconfigure all manual summaries before deconfiguring Enhanced Interior Gateway Routing Protocol (Enhanced IGRP). [CSCdi57814]
- Attempting to copy an empty startup configuration to the network causes the router to reload. [CSCdi58040]

ISO CLNS

- There is no method for altering the transmission rate of Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs) in cases where the rate would add undue load to the receiving system. [CSCdi54576]
- If IS-IS is running, and a Connectionless Network Service (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 might suspend indefinitely. A workaround is either to disable IS-IS before removing the static route, or to enable IS-IS on the point-to-point interface before removing the static route. [CSCdi56815]

Novell IPX, XNS, and Apollo Domain

- If there are more than 42 neighbors on a single LAN interface, Intermediate System-to-Intermediate System (IS-IS) and NetWare Link Services Protocol (NLSP) will be unable to establish neighbor adjacencies. The workaround is to limit the number of neighbors to 42 or fewer. [CSCdi56547]
- IPX Service Advertising Protocol (SAP) tables might not accurately reflect SAP entries learned locally, if you simultaneously configure IPX Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) and IPX Routing Information Protocol (RIP)/SAP. Some SAP entries might appear in the SAP table as derived from Enhanced IGRP rather than from RIP/SAP, even when the local LAN is not running Enhanced IGRP. [CSCdi56588]
- If you turn off an interface that is running IPX and immediately turn it back on, the router might reload. [CSCdi57683]
- The router might reload when running IPX Enhanced IGRP, because of illegal access to memory. [CSCdi57728]

Wide-Area Networking

- Groups of 4 ports on a Cisco 2511 might have data set ready (DSR) behaving in unison to a single stimulus. Reloading the router is the only workaround. [CSCdi49127]
- Rarely, a heavily loaded X.25 link that is experiencing congestion can enter a state where it oscillates between sending RNR (receive not ready) and REJ (reject) messages. [CSCdi55677]

Release 10.3(10) Caveats/Release 10.3(11) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(10). These caveats apply to all 10.3 releases up to and including 10.3(10). For additional caveats applicable to Release 10.3(10), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(11).

Basic System Services

- If you set the maximum transmission unit (MTU) to larger than 8192 on a Cisco 7500 or Cisco RSP7000 interface, the MTU change will fail with the error message "can't carve anything." [CSCdi50133]
- Transparent bridging with Cisco 7500 series routers might fail if a frame crosses a High-Level Data Link Control (HDLC) link. [CSCdi52360]

IBM Connectivity

- 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 large networks, this behavior might result in explorer storms as well as suboptimal routes. [CSCdi45116]
- When the **dlsw icanreach mac-exclusive** and **dlsw icanreach mac-address** commands are issued to specify a single MAC address to be filtered, all traffic is filtered instead. [CSCdi45773]
- A Cisco router might report inaccurate traffic statistics. In particular, non-broadcast frame counts might be incorrect if the router is acting as a source bridge on a Token Ring. [CSCdi46631]
- An incorrect timer reference causes explorer frames to be flushed on interfaces, even when the maximum data rate for explorers on the interface is not exceeded. [CSCdi47456]
- Physical Unit 2.0 (PU 2) stations might not become active if they are Synchronous Data Link Control (SDLC) attached to a Cisco 4000 router via data-link switching (DLSw). The router might go into the slow poll mode and eventually quit polling the stations. To clear the condition, reactivate the serial port. A workaround is to configure slow poll for the interface. [CSCdi47552]
- The number of downstream physical units (DSPUs) that can be added to a router configuration is erroneously limited to 256. [CSCdi49448]
- If a Cisco 4700 has a large number of local "icanreach" nodes, issuing the **show dlsw reachability** command causes data-link switching plus (DLSW+) to crash. [CSCdi50102]
- If there are two DLSw priority peers (the "priority" keyword is given in the remote peer definition), when one peer is reloaded the other peer might crash. [CSCdi50155]
- If the **multiring** command is executed on low-end platforms, invalid Routing Information Field (RIF) entries will be cached. [CSCdi50344]
- A DLSw peer-on-demand connection might not be disconnected even after all Logical Link Control (LLC) connections are disconnected between the peers. [CSCdi50574]
- If you remove a DLSw configuration by configuring **no dlsw local-peer**, and then you add the DLSw configuration back, a memory leak in the middle buffer can occur. [CSCdi51479]

- If you apply a **source-bridge output-lsap-list** command to a Token Ring interface when **source-bridge explorer-fastswitch** is enabled, packets permitted by the output-lsap-list might be dropped. The workaround is to issue the **no source-bridge explorer-fastswitch** command. [CSCdi51754]
- When a large number of frames are simultaneously sent by an end station to a router via DLSw, the following message might appear on the console:

  ```
  DLSW:CPUHOG in CLS background, PC=0x60549f3c
  ```

  Because the CPU is occupied for a significant period of time to process the storm of frames, protocols that involve polling might lose their connections. [CSCdi52382]
- After a DLSw Ethernet retransmission, LLC frames are corrupted. If this occurs, you will be unable to establish or drop an Ethernet session. [CSCdi52934]

Interfaces and Bridging

- When a Cisco 7000 router Ethernet interface is the root of a spanning tree and User Datagram Protocol (UDP) flooding is configured with turbo flooding, packet loops occur. The workaround is to disable turbo flooding. [CSCdi45659]
- On a Cisco 7000, bandwidth management functions are not working correctly, resulting in degraded MEMD buffer management. [CSCdi52227]

IP Routing Protocols

- Running multiple Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) autonomous systems might consume all available memory in the router. [CSCdi36031]
- Packet corruption might occur when fast-switching IP packets from ATM interfaces to Token Ring interfaces that are configured with the **multiring** command. [CSCdi49734]
- If you issue the configuration command **no router ospf** *process-id* on an AGS+ router, the router might reload. [CSCdi51283]
- If two autonomous systems are configured with IP and Enhanced IGRP, and then an interface address is moved from one autonomous system to the other, Enhanced IGRP will fail to operate on that interface. The workaround is to first delete the IP address using the **no ip address** command before configuring the new address. [CSCdi52078]
- Sometimes Enhanced IGRP will stop transmitting packets. This will cause widespread and continuous outages, as every route that goes active will be stuck in active. The workaround is to deconfigure and restart Enhanced IGRP, or to reload the system. [CSCdi53466]

ISO CLNS

- If two routers running intermediate system (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 lost. This is caused by a deficiency in the IS-IS protocol specification. [CSCdi48351]
- Sometimes ISO–Interior Gateway Routing Protocol fails to install parallel routes in the Connectionless Network Service (CLNS) prefix table. [CSCdi50714]
- Issuing a CLNS ping to one of the router's own addresses will cause the router to reload if **debug clns packet** is on. A workaround is to not have this debug on when pinging to one of the router's own addresses. [CSCdi50789]

TCP/IP Host-Mode Services

- Occasionally, random lines on a Cisco ASM/4 modem might pause indefinitely in a Carrier Dropped state. The only way to clear the line is to reload the ASM. [CSCdi44663]
- Opening hundreds of simultaneous Telnet connections over a serial link might cause the router to reload with a watchdog timeout error. [CSCdi47841]

VINES

- On serverless segments, the Vines Sequenced Routing Update Protocol (SRTP) does not send the redirect to the correct network number (Layer 3) address. A sniffer trace of this packet will show the message "abnormal end of Vines SRTP." A workaround is to turn off Vines redirects on the serverless segment interface. [CSCdi50536]

Wide-Area Networking

- When a router is configured for Integrated Services Digital Network (ISDN) services, the router might sometimes reload with the following message: [CSCdi45085]

  ```
  System was restarted by error - Illegal Instruction, PC 0x300D646
  ```

- Transparent bridging over point-to-point ATM subinterfaces might fail with error messages such as "hybridge_input ATM1/0.3: unexpected idb type ..." The workaround is to replace the point-to-point subinterfaces with multipoint subinterfaces. [CSCdi46514]
- A Cisco 4000 series router with ISDN BRI interfaces might run out of timer blocks and crash. The **show isdn memory** command can be used to see if memory is not being freed. [CSCdi47302]
- If chat script operations fail over asynchronous interfaces, a reload might occur during later operations because data was left in an inconsistent state. [CSCdi47460]
- Sometimes a Cisco 4000 series router with an MBRI will stop transmitting on an ISDN interface. Only a reload of the router can correct this. [CSCdi50628]
- International calls that are placed using the Australian Primary Rate switch type primary-ts014 might incorrectly tag the format of the called address field. As a result, calls that are placed to locations outside of Australia are rejected as "unassigned". [CSCdi50927]

Release 10.3(9) Caveats/Release 10.3(10) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(9). These caveats apply to all 10.3 releases up to and including 10.3(9). For additional caveats applicable to Release 10.3(9), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(10).

AppleTalk

- Routing Table Maintenance Protocol (RTMP) routes are sometimes not aged correctly, resulting in a continually increasing update time. Although the RTMP path is updated, the route in the routing table is not. As a result, the user does not see the route timer and state change. [CSCdi34053]

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 7513 router running source-route bridging (SRB) with a high volume of traffic might reload with no message to the console. [CSCdi45887]
- Issuing the **microcode reload** command over a Telnet connection might cause a router to enter an infinite loop. [CSCdi47580]
- The electrically erasable programmable read-only memory (EEPROM) in some chassis interfaces is misprogrammed. A **show diagbus** command indicates that the chassis interface incorrectly has "07" in the first byte of the EEPROM, instead of "01." The system software does not recognize chassis interfaces that have this error. At startup, the following message appears:

  ```
  %CI-3-CTRLRTYPE: Wrong controller type 10 %CI-4-NOTFOUND: Chassis Interface not found
  ```

  The output of the **show version** command indicates:

  ```
  WARNING: Chassis Interface not present
  ```

  When these messages appear, the **show environment** commands do not work, and no environmental monitoring takes place. [CSCdi48075]

Communication Server

- The **service hide-telnet-address** command does not hide the telnet address in the Connection Closing message. The **busy-message** command does not suppress the Connection Closing message. [CSCdi47740]

DECnet

- DECnet Phase IV-to-Phase V conversion might introduce incorrect area routes into the ISO Interior Gateway Routing Protocol (IGRP), if there are DECnet L2 routes on the DECnet side. These area routes show up 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 that are related to source-route bridging (SRB) might 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]
- 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]
- 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 can cause congestion. [CSCdi47561]
- 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 XID packets. This problem causes the NetView log to get congested and run out of storage, which might bring down the host. [CSCdi47803]
- When Synchronous Data-Link Control (SDLC) attached Physical Unit 2.1 (PU 2.1) devices are connected over data-link switching plus (DLSw+), if the host device does not respond because the application is down, the DLSW+ circuit does not correctly disconnect. This problem causes the circuit at the SDLC end to be in a Contact Pending state even with no circuit at the host end. This is cleared by shutting down the SDLC interface at the router or by reloading the PU 2.1 device. [CSCdi48227]
- 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]
- Connections to a host cannot be established from a DSPU using virtual telecommunications access method (VTAM) through a Cisco 3172 Channel Interface Processor (CIP). [CSCdi49872]

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]
- Basic Rate Interface (BRI) commands might not be recognized by a system with both MBRI and CT1/CE1 network processor modules installed. A workaround is to remove the CT1/CE1 module. [CSCdi43998]
- Transparent bridging and the HSRP protocol cannot be simultaneously enabled on Fast Ethernet interfaces. Random crashes occur, which can result in image or memory corruption. [CSCdi48646]
- Serial interfaces that are down but not administratively disabled might periodically reset with the error “(8010) disable - fsip_reset()”. [CSCdi49431]

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]

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, 4700, or 7500). [CSCdi44688]

Novell IPX, XNS, and Apollo Domain

- When an Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) route is advertised back into RIP, the delay within the EIGRP cloud is not taken into account properly in the *tics* metric value of the route when it is redistributed into RIP. The RIP advertised route might then look closer than it really is. [CSCdi49360]
- When an interface goes down, services which are not learned over that interface are erroneously marked as down and poisoned. This can cause excessive Service Advertising Protocol (SAP) packet generation as packets are first flooded to indicate the downed services, and then flooded again to indicate the newly learned services, in a short period of time. [CSCdi49369]
- If IPX Enhanced IGRP is running, the command sequence

  interface serial

  no ipx network

  no ipx routing

  might cause the router to reload. [CSCdi49577]

TN3270

- TN3270 does not assume the appropriate 132 x 27 dimensions when set up as a Model 5 (MOD5) terminal. [CSCdi44497]

VINES

- VINES servers located downstream might unexpectedly lose routes that were learned via Sequenced Routing Update Protocol (SRTP). This behavior results from improper handing of network sequences numbers by the system. Issuing a **clear vines neighbor** or disabling SRTP are suggested workarounds. [CSCdi45774]
- A Cisco router reloads when it receives incorrectly formatted Interprocess Communications Protocol (IPC) packets from the VINES application software “Streetprint.” The VINES IPC length field should contain the number of bytes that follow the long IPC header in a data packet, but “Streetprint” incorrectly set the IPC length in each IPC message to the total number of bytes of all IPC messages. [CSCdi47766]

Wide-Area Networking

- When routing an X.25 call request packet containing a Calling/Called Address Extension facility, sometimes the Calling/Called Address Extension facility is inadvertently modified. [CSCdi41580]
- 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 a Cisco 4000 with a Basic Rate Interface (BRI) has the **isdn tei powerup** configuration flag set, the watchdog timeout will crash the router. A workaround is to configure the router with the **isdn tei first-call** command. [CSCdi45360]
- 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]
- When booting a router on which all ATM interfaces are in a No Shut state, you need to issue the **shutdown** and **no shutdown** commands on one of the ATM interfaces to allow ATM signaling to correctly function. [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]

Release 10.3(8) Caveats/Release 10.3(9) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(8). These caveats apply to all 10.3 releases up to and including 10.3(8). For additional caveats applicable to Release 10.3(8), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(9).

Basic System Services

- Fast switching with some encapsulations might cause the router to crash. The workaround is to disable fast switching. [CSCdi45414]
- The router might reload if a user is authenticating access with the Terminal Access Controller Access Control System (TACACS) or extended TACACS with Password Authentication Protocol (PAP). This reload occurs if the interface is not an asynchronous line and the principal user's username and password also exist in the local database. [CSCdi45530]
- Issuing Simple Network Management Protocol (SNMP) sets to the *writeNet*, *hostConfigSet*, or *netConfigSet* variables might cause the router to reload. The workaround is to not issue sets to these variables. [CSCdi45948]

- Polling the following Management Information Base (MIB) variable causes the Cisco 7000 router's CPU utilization to exceed 90%: [CSCdi45961]

  ```
  .iso.org.dod.internet.private.enterprises.cisco.local.linterfaces.
  lifTable.lifEntry.locIfOutputQueueDrops
  ```

- Using Hot Standby Router Protocol (HSRP) in heavy traffic conditions might cause cBus resets and the error report "RSP-3-ERROR." [CSCdi46654]

Communication Server

- The TN3270 feature might crash if a terminal width greater than 100 characters is configured before connecting to a host application. [CSCdi44586]
- The line printer daemon (LPD) will terminate a job if the control file sent from the host identifies the job as a postscript job. [CSCdi45881]

EXEC and Configuration Parser

- If **fddi valid-transmission-time** is configured for other than the default and saved to nonvolatile RAM (NVRAM), the router will reload at the next boot time (when the command is read from NVRAM by the boot monitor). If a non-default time is required, boot only that portion of the configuration using the **boot host** command to work around the problem. [CSCdi37664]

IBM Connectivity

- When an SDLLC or Qualified Logical Link Control (QLLC) virtual ring is configured, explorer frames might be incorrectly forwarded to the interface corresponding to the third ring listed in the Routing Information Field (RIF). [CSCdi43378]
- On low-end systems for a data terminal equipment (DTE) router interface, the following error might occur after a router reload. Synchronous Data Link Control (SDLC) packets are identified as High-Level Data Link Control (HDLC) packets by the serial driver, until a **shut**/**no shut** command sequence is performed for the interface. This error causes occasional packet drops without a trace, if the byte pattern happens to match that of other protocols. This error can also cause significant performance problems. [CSCdi43686]
- Source-route bridging (SRB) bridged packets might be dropped when a router is configured for remote source-route bridging (RSRB) direct, and when priority/custom queuing is enabled on the output serial interface. A workaround is to disable priority/custom queuing on the serial interface. [CSCdi44430]
- The Cisco AGS+ router intermittently reboots if the router has at least one 2-port Token Ring card and one 4-port Token Ring card and if **source-bridge explorer-fastswitch** is set to ON. [CSCdi45131]
- Using data-link switching (DLSw) might cause traceback messages to occur. [CSCdi45407]
- When a router is configured for Data Link Switching Plus (DLSw+) with SDLC and an application is taken down on the host system, the SDLC controller will not respond. To recover, reload the SDLC-attached controller. Issuing a **show interfaces** command on the router indicates that the interfaces are in the XIDSENT state. [CSCdi46028]
- Outbound access lists are not always applied to fast switched explorer frames. [CSCdi46182]
- A router configured for downstream physical unit (DSPU) might crash while making DSPU configuration changes. [CSCdi46820]

- DSPU/remote source-route bridging (RSRB) connections sometimes cannot be established. [CSCdi46949]

Interfaces and Bridging

- Secure Data Exchange (SDE) encapsulation used with bridged virtual LANs (VLANs) might be corrupted in some environments. This corruption results in lost traffic between VLAN-connected networks. The environments known to be affected include connections across High-Speed Serial Interfaces (HSSIs), Token Rings, and Fast Serial Interface Processors (FSIPs). The SDE encapsulation works correctly across Ethernet and Fiber Distributed Data Interface (FDDI) connections. [CSCdi36792]
- With two routers on a ring, Open Shortest Path First (OSPF) neighbors disappear after a few hours because the Internet Protocol (IP) process does not receive the multicast packet for OSPF hellos. [CSCdi38185]
- Enabling the silicon switching engine (SSE) for IP might cause the system to crash. The workaround is to perform the **no ip route-cache sse** command. [CSCdi44414]
- When bridging is configured on interfaces not capable of SSE bridging, then SSE bridging for all interfaces on the router is disabled. The workaround is to use cBus bridging. [CSCdi45124]

IP Routing Protocols

- A router running Open Shortest Path First (OSPF) might reload when configuring a controller T1 with a channel-group time-slot assignment. [CSCdi43083]
- Attempts to route Internetwork Packet Exchange (IPX) packets by Routing Information Protocol (RIP) or by Enhanced Interior Gateway Routing Protocol (IGRP) might fail on primary serial interfaces. Failure can occur when the subinterfaces were configured for IPX routing before their primary interface was. [CSCdi44144]
- When using Enhanced Interior Gateway Routing Protocol (EIGRP), IP summary routes might be incorrect, making the affected networks unreachable.

ISO CLNS

- If an intermediate system (IS)-IS link-state packet (LSP) is not regenerated for 24.8 days, it cannot be transmitted for another 24.8 days. This problem can happen only in extremely stable IS-IS networks. [CSCdi45179]
- Occasionally, issuing the **show isis route** command causes the router to reload. [CSCdi45496]

Novell IPX, XNS, and Apollo Domain

- If **ipx sap-incremental** is configured, a router may end up with fewer service access point (SAP) entries than actually exist if the interface goes down and then comes back up. This problem occurs more often when there are many SAP entries in the network environment. [CSCdi46224]

Protocol Translation

- A router might reload if it is translating between Transmission Control Protocol (TCP) and local-area transport (LAT)/X.25 protocols, and if the **access-class** command has been used to specify an extended access list. To work around this problem, do not use extended access lists when translating between protocols. [CSCdi44853]

TCP/IP Host-Mode Services

- The ATM Interface Processor (AIP) card of the Cisco 7000 series routers does not map the virtual path identifier-virtual channel identifier (VPI-VCI) pair used in an ATM connection, unless the router initiates the switched virtual circuit (SVC). There are two symptoms.

  The first symptom occurs when a new VPI-VCI pair is opened to the router from an ATM switch. In this case, the AIP does not pass this information to the Route Processor (RP) and a reply to the incoming traffic is not sent back on the VPI-VCI pair just opened. Rather, the AIP card opens a new VPI-VCI pair and sends it back to the switch, creating unidirectional SVCs. This behavior is inefficient.

  The second more serious symptom involves the cells carrying packets that are responses to those in a VPI-VCI pair opened by a sending router. These cells return on a new, unidirectional VPI-VCI pair for which the router has no mapping. In this case, the incoming cells are missed, requiring retransmissions to complete the intended communications. [CSCdi32192]

- On a Cisco AGS+ router or Cisco 7000 router, if **ip tcp header-compression** is turned on for Fiber Distributed Data Interface (FDDI) or serial interfaces, the following error message might display: [CSCdi38666]

  ```
  %LINK-3-TOOBIG: Interface Serialxx, Output packet size of 1528 bytes too big
  ```

- Basic Rate Interface (BRI) interfaces might stop placing calls after a period of normal operation. To re-enable the interface, reload the router. [CSCdi42098]

- Integrated Services Digital Network (ISDN) interfaces on an MBRI card might stop functioning, if the following error message is reported:

  ```
  %SYS-3-HARIKARI: Process ISDN top-level routine exited...
  ```

  To restart ISDN, reload the router. [CSCdi42578]

- With **encapsulation lapb** or **encapsulation x25** configured, under certain conditions the command **lapb n1** *bits* disappears from the working configuration, and N1 falls back to the default. This is most likely to occur after an interface reset or a reload. [CSCdi44422]

- After downloading a host-specific configuration file, using AutoInstall over Frame Relay with point-to-point subinterfaces, might result in a router reload. [CSCdi44643]

- A serial interface running X.25 encapsulation under heavy load conditions might stop sending the Link Access Procedure, Balanced (LAPB) protocol. [CSCdi46024]

- IGRP protocol routing broadcasts sometimes fail to dial static routes on Point-to-Point Protocol (PPP) backup interfaces. A workaround is to configure SNMP or *syslog* to a host on the remote side. [CSCdi46312]

- Routers with the **isdn switch-type basic-net3** command in use with Integrated Services Digital Network (ISDN) Basic Rate Interfaces (BRIs), might experience BRI port failures. A reload of the router is required to use the BRI interface. [CSCdi46668]

Release 10.3(7) Caveats/Release 10.3(8) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(7). These caveats apply to all 10.3 releases up to and including 10.3(7). For additional caveats applicable to Release 10.3(7), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(8).

AppleTalk

- Issuing the command **show appletalk route** *network*, where *network* is an AppleTalk proxy network, causes the system to halt. [CSCdi44235]

Basic System Services

- A Cisco 4000 router with 32 MB of memory, will only count 16 MB in the global free pool. [CSCdi40056]

IBM Connectivity

- When using **local-ack**, the following error messages may result in a router reload or loss of session: [CSCdi34930]

```
%SYS-2-NOTQ: unqueue didn't find 11CA40 in queue 63C3C -Process=3D "*Sched*", ipl=3D 4
-Traceback=3D 3050154 302854C 332869A 331DB8C 3311628 3304C50 303C4E8 3104F5E
```

- DSPU sends TEST (P) in response to a NULL XID (P) on connect-ins, causing problems with certain LLC2 implementations. [CSCdi40809]
- The Cisco 4500 might reload if a TEST (F) or NULL XID (F) is received while the X.25 SVC for the QLLC connection is down. [CSCdi40851]
- IPX all stations broadcasts explorers will not be fast switched when IPX is source-route bridged. [CSCdi41043]
- The router's serial interface driver software occasionally drops SDLC frames if the bit patterns are identical to HDLC LEX frames. Dropping occurs on interfaces using STUN-basic encapsulation with non-IBM SNA data traffic (for example, COMM10 CNS protocol). Note that there is no indication in the router when this problem occurs. The router does *not* increment the interface "drop" counter or the STUN "drop" counters. Detection is only possible with a media tracing tool. [CSCdi41558]
- The Find Name NetBIOS broadcast is sent from the Token Ring interfaces even though the proxy-explorer and NetBIOS name caches are configured on the interface. To workaround, run back-level software. [CSCdi41972]
- Although routers with sufficient memory and CPU horsepower should support more than 1000 LLC2 sessions, the actual number of sessions allowed is erroneously limited to significantly fewer. [CSCdi42181]
- Using the source-route-bridging (SRB) proxy-explorer feature with SRB autonomous switching on FDDI may cause incoming packets to be dropped by the FDDI interface. Work-around is to disable the SRB proxy-explorer feature or disable SRB autonomous switching on the FDDI interface. [CSCdi44095]

- The data portion of a multicast IPX explorer packet might be corrupted when being fast-switched. [CSCdi44672]

Interfaces and Bridging

- For a given bridge table entry, bridging may fail to forward packets to one destination, although packets to other destinations will be properly forwarded.This can be seen by a **show bridge nnnn.nnnn.nnnn** command. The TX count increments, but the RX count stays constant. The workaround is to issue a **clear bridge** command. [CSCdi42445]
- At times stations are not able to establish connectivity over transparent bridging because some DLC frames are not forwarded when they should be. [CSCdi42690]
- The Cisco 4000 series routers with FDDI network interface modules (NIMs) might reload under certain stressful conditions. [CSCdi43618]
- When configuring SLIP or PPP framing on the auxiliary port of a router, "Low memory modified by Input Helper" messages erroneously appear in the system error log. [CSCdi43970]

ISO CLNS

- Open System Interconnection (OSI) end system adjacencies sometimes do not appear in an IS-IS protocol Level-1 pseudonode LSP. This is especially likely to occur when there is only one router on the LAN containing the end systems. [CSCdi43236]

Novell IPX, XNS, and Apollo Domain

- Configuring IPX on the router when the router has low memory might cause the command shell to crash. [CSCdi42363]
- The **ipx routing** command does not enable the IPX RIP protocol if **no ipx routing** is configured. The workaround is to not configure **no ipx routing**. [CSCdi42953]

TCP/IP Host-Mode Services

- BOOTP attempts might fail over an asynchronous VTY PPP connection when **async-bootp** commands are used. This is because of an incorrect User Datagram Protocol (UDP) checksum on the BOOTP reply. [CSCdi41168]

VINES

- Under heavy loads, the VINES router system process may not run frequently enough for proper VINES operation. Symptoms include a high amount of route and neighbor flappage. Reducing the load on the router may help alleviate the problem. [CSCdi41922]
- When using Cisco 2500 series terminal servers with PPP, packets might pass after IPCP has completed negotiation, but before the interface is declared up. This might cause problems with applications that send out immediate requests, since the response may be dropped by the terminal server due to the interface being down. The workaround is to place a slight pause after IPCP has been negotiated and before sending out requests. [CSCdi37400]
- When using multiple BRIs in a rotary group, the router may unnecessarily dial extra B channels, even though the load on some of the B channels in use is less than the configured threshold. [CSCdi39713]

- TN3270 and TELNET user sessions might be dropped unexpectedly from the Cisco 2509 and Cisco 2511 access server asynchronous ports, because of an inactivity timeout. [CSCdi41542]
- Routers with an ISDN BRI interface might have problems with B channels, or might run out of call control blocks, because B channels might be assigned that are already in use. The router rejects these calls with a "Channel Unacceptable" cause. If the router runs out of call control blocks, severe errors will likely occur. [CSCdi42123]
- ISDN routers with a PRI or BRI interface may crash when receiving a Layer 3 Status Enquiry message with a "Display IE" in the message. [CSCdi42382]
- The system may halt unexpectedly after issuing a **clear vines neighbor** command. [CSCdi42431]
- Hardware flow control may be inadvertently disabled on the Cisco 2509, 2510, 2511 and 2512 routers' asynchronous ports after issuing a **configure network** or a **copy tftp running-config** command. To restore flow control, simply issue the line configuration command **flowcontrol hardware** on all of the lines. [CSCdi43306]
- For systems with AIP microcode version 10.10 and earlier, if sub-interfaces are defined on ATM interfaces, and if the command **atm pvc aal5mux ip** is performed for each sub-interface, the permanent virtual circuits (PVCs) may not show up in the active configuration. Therefore, the PVCs will not come up, unless a **config memory** is performed. [CSCdi43387]
- A Sequenced Routing Update Protocol (SRTP) update sent in response to a client request for specific networks, will omit the last network specified in the request. [CSCdi44517]

Release 10.3(6) Caveats/Release 10.3(7) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(6). These caveats apply to all 10.3 releases up to and including 10.3(6). For additional caveats applicable to Release 10.3(6), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(7).

AppleTalk

- IPTalk clients running Columbia AppleTalk Package (CAP) cannot start up because a nonstandard NBP packet generated by the client is not forwarded by the system. There is no workaround. [CSCdi39096]

Basic System Services

- IPX SAP process may consume more memory than required causing a memory leak and potential memory exhaustion. [CSCdi38381]
- On the AGS+, Cisco 7000, and Cisco 7500 platforms, the command **buffers huge size [size]** has no effect. [CSCdi38912]
- When using Protocol Translation for virtual asynchronous connections, the system may restart and display the message "System was restarted by error - Illegal Instruction, PC 0x0". [CSCdi40681]

IBM Connectivity

- The SNA packet is lost during fragmentation if no buffer is available to store the fragmented packet. The SNA application will recover and resend the packet without disconnecting the session. [CSCdi27730]
- With SRB configured (local only), the router occasionally appends random data to the end of LLC2 RR frames being bridged through the router. Some LLC2 devices will reject these padded frames causing loss of sessions. [CSCdi38486]

TCP/IP Host-Mode Services

- An access server can accept a new reverse TCP connection while being in the hangup state for the previous connection. This will cause the new connection to be closed shortly after being established. This happens when the **modem cts-required** command is configured. [CSCdi39085]

Wide-Area Networking

- Frame Relay DLCIs that are deleted using the **no frame-relay interface dlci** command are not actually deleted from the system. [CSCdi39555]
- When using DTR dialing and PPP encapsulation, DTR does not stay “low” after the call is disconnected. [CSCdi39576]
- Routers with an ISDN BRI interface may not properly answer incoming calls. This may occur if a **clear interface bri x** command is entered while calls are established or if the ISDN TEI flag is configured for first-call. The incoming call will be accepted, but the Layer 3 connect message will not be sent to the network. [CSCdi39627]
- In rare circumstances, an SDLLC connection failure can cause the router to reload. [CSCdi39832]
- When a serial PPP link from a Cisco 7000 router to a LEX box goes protocol down, the LEX continues to forward frames from the serial interface. [CSCdi39882]
- Routers with an ISDN PRI interface may have channels put into an “out-of-service” condition, which prevents the channels from accepting or placing calls. This occurs predominantly on the DMS-100 switches. [CSCdi40762]
- On Cisco 2509 through Cisco 2512 devices, asynchronous lines stop accepting input under certain conditions. One of these conditions occurs when a user connected to a LAT host types a Control-C character. A **clear line x** or change to the line parameters will cause the line to start accepting input again. [CSCdi40994]

Release 10.3(5) Caveats/Release 10.3(6) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(5). These caveats apply to all 10.3 releases up to and including 10.3(5). For additional caveats applicable to Release 10.3(5), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(6).

AppleTalk

- The system may halt unexpectedly when **show appletalk route detail** is given. [CSCdi36007]
- When a Macintosh dials into an asynchronous port on a Cisco 2511 access server using ATCP and tries to print to a device off the Ethernet of the Cisco 2511, the device crashes with the message “System restarted by error - Line 1111 Emulator, PC 0xD7A”. [CSCdi37588]

Basic System Services

- A TTY line configured for software flow control on a Cisco 2509 through 2512 access server will occasionally garble data when connecting to a remote host using the telnet protocol. [CSCdi35487]
- When using autoselect PPP in conjunction with TACACS+ authorization, the routing table will contain the host route for the default IP address assigned on the asynchronous interface even if TACACS+ and IPCP have assigned a different address to the client. [CSCdi37366]

DECnet

- When DECnet connect initiate packets are sent over a DDR link, the router tries to open a DDR link. In the meantime, however, DECnet thinks there is no route to the destination and returns the packet to the sender, thereby terminating the connection. A second connect initiate session is needed for the connect to get across. [CSCdi33368]
- The DECnet fast-switching code path cannot handle a static route that points to another DECnet address (in other words, the static route has no outgoing interface information). [CSCdi38977]

EXEC and Configuration Parser

- You cannot assign a privilege exec level to the command **terminal download** [CSCdi38824]

IBM Connectivity

- NetBIOS connections occasionally fail to connect through remote source-route bridging when local acknowledgment is enabled. The workaround is to disable local acknowledgment. [CSCdi37525]
- LLC2 parameters on IETF are not recognized when entered. [CSCdi37921]
- DSPU does not recognize the 2-byte ACTLU RSP as a valid response and, therefore, does not activate the LU. [CSCdi38299]

- The DLSw+ state machine can hang so that on an SDLC line, a **show dls circuit** command will show one index in a HALT PENDING NOACK state and another at DISCONNECT PENDING. During this state, no DLSw+ traffic will flow over these circuits. A **clear dls circuit** command has no effect, requiring a router reload to recover. [CSCdi39046]

Interfaces and Bridging

- Very intermittently, the FSIP controller detects a spurious error on the transmit buffer size resulting in a controller fatal error. [CSCdi30344]
- Cisco 7000 series routers using SDLC Multidrops should ignore data carrier detect signals. [CSCdi32813]
- On the BRUT partner product (Cisco 2500 variant co-developed with DEC) when an Ethernet interface goes down, the output of a **show interface** command still shows the interface as being up. The SNMP replies are also incorrect. [CSCdi37135]

IP Routing Protocols

- When the eigrp process receives a hello packet from a neighbor, it tries to send an update packet, but this process of sending an update packet can be suspended by the eigrp process. When the eigrp process gets scheduled again to send the update packet the neighbor may be dead and all of the internal data structures for that peer (neighbor) could have been erased, which confuses the eigrp process and results in the generation of wrong bus address. [CSCdi35257]
- The router does not remove LSAs that are MAXAGE, either because the local router ignores the acknowledgment or the remote router fails to generate an acknowledgment. This behavior prevents the router from relearning a route that becomes available again. [CSCdi36150]
- In a misconfigured or malfunctioning Token Ring bridging environment, pinging the Hot Standby Router Protocol (HSRP) virtual IP address can cause the ICMP echo request packets to be massively replicated. [CSCdi38170]
- Extended IP access lists that use UDP destination ports can have an incorrect configuration generated for them. [CSCdi39192]

ISO CLNS

- When Phase IV/V conversion is enabled and the Phase IV source and Phase V destination are on the same interface of the router, the router may crash. This is caused by the router's attempt to send a Phase V redirect to the Phase IV host. [CSCdi37236]

Protocol Translation

- Virtual asynchronous interfaces, such as those used for SLIP or PPP over packet assembler/disassembler (PAD) connections, may stop sending packets. [CSCdi36149]
- When using one-step translation without requiring a login, per-user access lists cannot be assigned by extended TACACS for a virtual asynchronous interface. [CSCdi37678]

TCP/IP Host-Mode Services

- The router can erroneously drop packets (generating ICMP ttl-expired messages) from serial interfaces when TCP header compression is configured on those interfaces. [CSCdi37637]

VINES

- When **vines single-route** is enabled, the metric for alternative routes is recorded incorrectly. The workaround is to disable **vines single-route**. [CSCdi39054]

Release 10.3(4) Caveats/Release 10.3(5) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(4). These caveats apply to all 10.3 releases up to and including 10.3(4). For additional caveats applicable to Release 10.3(4), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(5).

AppleTalk

- The problem that prevents the router from invalidating the old cache entries was corrected. [CSCdi35967]

DECnet

- When a DECnet MOP remote console connection is attempted from a VAX to a Cisco router, the process begins, gets connected and goes as far as issuing the password prompt. Then the connection is broken quickly. [CSCdi36500]

IBM Connectivity

- RSRB remote peers configured for direct and TCP encapsulation exhibit memory leak in a dead state. It takes an hour for the dead peer to consume the entire memory. The workaround is to manually remove the dead peers. [CSCdi32752]
- If (R)SRB is configured on more than two CTR Token Ring interfaces in an AGS+, the third interface will stop accepting packets after a number of explorers arrive at the interface. This is due to an incorrect reallocation of CBUS buffers by the fast explorer code. The workaround is to configure the global command **no source-bridge explorer-fastswitch** and then reload the router. [CSCdi36539]
- The **source-bridge proxy-explorer** command causes broadcast storms on the network when an explorer is sent for a nonexistent destination MAC address. A trace of the Token Ring shows excessive LLC explorer frames and the router console does not accept keyboard input. It has to be reloaded to recover. The workaround is to remove the **source-bridge proxy-explorer** command from the Token Ring interfaces. [CSCdi36718]

IP Routing Protocols

- Using EIGRP-IP, if a default network is known through an interface that is shut down, **show ip eigrp top act** shows the default network via the down interface and CPU utilization for EIGRP can get as low as 40% to 50%. [CSCdi36032]
- Access lists using the **tacacs-ds** keyword will not be parsed correctly in 10.3(4). This bug was introduced in CSCdi34944, which was integrated into 10.3(3.4). [CSCdi36962]

Novell IPX

- Display IPX routes may cause the router to reload when IPX EIGRP routes are being deleted. [CSCdi34380]
- Large **ipx output-sap-delay** and **output-rip-delay** settings may keep normal updates from running. Four new commands are added. The commands **ipx default-output-rip-delay** and **ipx default-output-sap-delay** set global defaults for all interfaces. Currently, the default is 0 ms; in the future this may be 55 ms. The commands **ipx triggered-rip-delay** and **ipx triggered-sap-delay** set per interface values for the interpacket gap in Flash and poison RIP/SAP updates. This value overrides the output-rip/sap-delay setting and is recommended to be a small value, if a large normal interpacket gap is configured. [CSCdi34411]
- Routes and services learned over IPX unnumbered point-to-point links will age out and disappear. Using a numbered interface is a workaround for RIP/SAP. This was broken by CSCdi33838 in 10.3(3.3). [CSCdi36047]

Wide-Area Networking

- When the **ppp use-tacacs** command was used, the behavior of CHAP Authentication for PPP connections did not comply with RFC 1334. Rather than always retransmit the same reply code when receiving multiple CHAP RESPONSE messages, our implementation sent a query to the TACACS server for authentication every time. Because successive TACACS queries may yield different results (if the server becomes unreachable, for example), our behavior did not comply with the RFC. The new behavior is to cache the reply code to a CHAP RESPONSE message and retransmit the same reply if multiple copies of a RESPONSE message are received. [CSCdi31925]
- When the session-timeout interval expires, the Protocol Translator now closes the outgoing PAD connection, return the terminal line to an idle state, and displays the following message: [Connection to idle too long; timed out]. [CSCdi34009]
- When doing bandwidth-on-demand over rotary groups of async or serial lines, traffic stops while a line is being dialed. [CSCdi34276]
- Under some unknown conditions, some X.25 data packets may incorrectly have the D bit set, which will cause a connection to be reset. [CSCdi35036]
- A received X.25 call that has user-specified data in the Call User Data field and no destination address (length of 0) is ambiguous. The X.25 routing table should be checked to see if the call can be routed, and if no route matches, the call should then be treated as destined for the router. The router is not treating received calls with the null destination address as routable. [CSCdi35754]
- Some of async line scripts incorrectly hang up the line. These include the Line Activation script, Network Connection script and in some cases the User Command script. [CSCdi35773]

Release 10.3(3) Caveats/Release 10.3(4) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(3). These caveats apply to all 10.3 releases up to and including 10.3(3). For additional caveats applicable to Release 10.3(3), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(4).

AppleTalk

- The problem that prevents the router from running in pre-FDDITalk mode is corrected. [CSCdi33270]

Basic System Services

- Using point-to-point LAPB compression seems to generate a memory leak. The workaround is removing the command **compress predictor** from the configuration. The problem with the predictor (RAND) compression algorithm was fixed. [CSCdi32109]

IBM Connectivity

- The system may reload when using an IBM LAN Manager to change the ring number of the Token Ring interface. [CSCdi30096]
- For SNA sessions, **llc2 local-window** is set to 8 even though the default is 7. For NetBIOS sessions, if the value of *packet-count* is set to 1 or 6 with **llc2 local-window** *packet-count*, the value of 8 is set instead by error. [CSCdi33845]

Interfaces and Bridging

- In high traffic environments, FSIP Version 10.8 will get FCICMDFAIL messages and may eventually get 8010 fsip_reset due to multiple command timeouts. The command timeout was caused by a long path in the FSIP firmware during the memd read on transmit. FSIP Version 10.8 fixed this problem by splitting the memd read on transmit into 32-byte chunks and enabling interrupts between the chunks. [CSCdi27451]
- On a Cisco 2500, DTR is held high on a shutdown interface when a DTE cable is attached. [CSCdi34135]

IP Routing Protocols

- If an IGRP or RIP routing process is configured, but no routing update has been sent in the last 24 days (e.g. if there are no “line protocol up” interfaces available) then routing updates may be suppressed for up to 24 days before resuming. [CSCdi33918]
- When OSPF is running and the system is attached to multiple areas, but not to the backbone area, the system is not able to select the best path for a destination that can be reached by an interarea route through different nonbackbone areas. [CSCdi35004]
- The following problem occurs when more than one serial interface is configured to be on the same subnet, and this subnet falls in the range of the **network** command. If some of the serial interfaces are not functional (for example, are shutdown), OSPF is not aware of it and might use this non-functional interface as the output interface in an SPF calculation. The result is that OSPF selects the wrong output interface for routing to an other border area router, as shown by **show ip ospf border-router**. It further causes summary and external routes not to be installed in the IP routing table. [CSCdi35182]

Novell IPX

- IPX static routes tied to an interface should be allowed on subinterfaces. [CSCdi35588]

Protocol Translation

- An X.25 RESET REQUEST received on a virtual circuit used for TCP PAD protocol translation causes the connection to pause indefinitely. [CSCdi33374]

Wide-Area Networking

- On the Cisco 2509, Cisco 2510, Cisco 2511, and Cisco 2512, if the carrier is lost while an asynchronous channel configured for hardware flow control has output held (because CTS is low), the channel can be left in an unusable state. [CSCdi27841]
- A router running X.25 and receiving unknown local or remote facilities may pause indefinitely in some circumstances. [CSCdi33178]
- This problem results from the AARP frames, to an SMDS interface, would be sent with a type 4(HW_SMDS) SMDS address. The SMDSTalk specification states that SMDS AARP entries use type 14(HW_SMDSTALK) address type. This created an incompatibility with other vendor implementations.

  The fix requires the newer Cisco IOS releases to send out type 14 address types with AARP packets and is compatible with other vendors. This is only an issue for ATALK users running in Extended mode with Dynamic ATALK address resolution enabled.

  Caution This fix creates an incompatibility with the existing ATALK/SMDS base when sending AARP in Extended mode. Users *must* upgrade all routers to the newer Cisco IOS releases to interoperate. The workaround until all routers are running Cisco IOS software with this fix is to run AppleTalk on SMDS with a non-extended configuration. See CCO, under techtips and AppleTalk for sample configurations. [CSCdi33586]

- This problem was preventing BOOTP UDP traffic coming into an AIP interface from being forwarded to other interfaces. BOOTP was not getting onto the other networks from ATM. [CSCdi33911]
- Invalid packets received on an SMDS interface are discarded incorrectly, and remain counted against the input queue, causing the interface to stop receiving traffic. [CSCdi34116]
- The command **autocommand ppp** produces the error message “%Unable to find address for you” upon startup of the connection. This problem first appeared in Release 10.3(2.0.1). To work around the problem for async connections only, use the line configuration command **autocommand ppp default**. There is no workaround for virtual asynchronous connections. [CSCdi34519]

Release 10.3(2) Caveats/Release 10.3(3) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(2). These caveats apply to all 10.3 releases up to and including 10.3(2). For additional caveats applicable to Release 10.3(2), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(3).

AppleTalk

- The following error messages and traceback are displayed on the console of a router that configures with AppleTalk:

  ```
  %SYS-2-BADSHARE errors in datagram_done pool_getbuffer and atalk %SYS-2-BADSHARE: Bad
  refcount in datagram_done, ptr=xxxx, count=0 -Traceback= xxxxxxxx xxxxxxxx xxxxxxxx
  ```

  If this message is displayed, contact Cisco Systems. Include the text and the traceback of this message as well as the information from the **show version** command. [CSCdi29127]

Basic System Services

- The Cisco 4500 may crash occasionally when doing multiple **write mem** or **write net** commands. [CSCdi29920]
- TACACS notify requests do not use the user-configurable retransmit and timeout parameters. [CSCdi30113]
- SLARP can cause the system to reload on routers that have dual Flash bank. [CSCdi30588]

IBM Connectivity

- In a large Token Ring bridging environment that uses automatic spanning tree, a bridge can incorrectly declare itself as a root. [CSCdi29517]
- Turning on proxy explorers can cause the router to be in a hung state because it put the packets on the same ring more than once, which is a violation of SRB protocol. [CSCdi32284]

Interfaces and Bridging

- Process-level flooding performance of transparent or source-route translational bridging deteriorates when interfaces of large MTUs such as FDDI and Token Ring are present on the router. Process-level flooding is used when the output interface is configured either for priority queueing or in a source-bridge ring group. This problem may be alleviated somewhat by increasing the initial, minimum, and maximum numbers of huge buffers. [CSCdi31501]

IP Routing Protocols

- The command [**no**] **ip summary-address** can cause the router to reload. [CSCdi23646]
- This bug was introduced in Release 10.3(1). The configuration of **ip ospf dead-interval** is lost after reload. No workaround is available. If necessary, the command can be reconfigured after reload to ensure proper operation. This fix solves the problem. [CSCdi31279]

Novell IPX

- The command **ipx gns-reply-disable** does not function properly and may cause a system reload. The workaround is to use a Get Nearest Server (GNS) filter on this interface, which denies all GNS replies. [CSCdi31875]

VINES

- Metric values in VINES ICP metric notification packets are bitshifted four positions. This causes higher metric values and can cause timeout delays during the retransmission process. [CSCdi30821]
- Source route information contained in SRTP Redirect packets may not be placed in the router's RIF cache with multiring configured on the interface. This causes loss of connectivity with the client workstation across the source-route bridge on the Token Ring. [CSCdi30962]

Wide-Area Networking

- DLCI's cannot be reassigned to subinterfaces from a primary interface. [CSCdi28765]
- For the **x25 route** command, allow an option **xot-source**, which takes an interface name as a parameter. This causes XOT TCP connections to use the IP address of the specified interface as the source address of the TCP connection, allowing the connection to move to a backup interface without terminating the TCP session. [CSCdi28892]
- The Defense Data Network (DDN) and Blacker Front End Emergency (BFE) modes do not encode the needed local facilities when originating a call. [CSCdi31252]
- A router with a BRI interface using basic-net3 switch type will ignore incoming calls with the High Layer Compatibility element. This will cause problems for routers calling from Norway, using basic-nwnet3, because the HLC must be used in calls. Incoming calls with HLC will be accepted by all the net3 switch versions. [CSCdi31517]

Release 10.3(1) Caveats/Release 10.3(2) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(1). For additional caveats applicable to Release 10.3(1), see the caveats sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROMs or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.3(2).

Basic System Services

- The router cannot detect a shortage of buffer elements and thus does not create new ones. This causes the router to drop packet even though there are ample packet buffers. The **show buffers** command output shows many buffer element misses. [CSCdi29379]
- A portion of the scheduler can interfere with the periodic timer interrupt resulting in a corrupted PC. This can cause a Cisco 4500 to reload. The likelihood of this problem occurring increases in applications that use many processes, such as IPX SAP updates across many interfaces. [CSCdi30044]

EXEC and Configuration Parser

- The router crashes if the output stream from a **show appletalk zone** command is waiting at a "More" prompt and the router deletes routes or zones at the same time. [CSCdi28127]

IBM Connectivity

- When the system is source-route bridging Novell packets, the RIF cache is not updated as Novell packets are passed through the system. When the RIF entry is aged out for the Novell network nodes, a loss of session may occur. [CSCdi14618]
- When IPX routing is enabled on a Token Ring interface and there is a source-route bridge network behind the ring, a **multiring ipx all** command is used to cache the RIF in the router. During normal operation all is well. But when a station is moved from one ring to another ring (for example, from 0B8 to 0B1), the station cannot reach the server. Looking at the RIF cache on the AGS+, it is fine. However, analyzing the frames with a Sniffer, we can see the "create connection request" from the station with a good RIF field but the answer from the AGS+ shows the previous RIF (the RIF before the station was moved). The workaround is to disable the IPX route cache or to clear the IPX cache when a station is moved. This is a general problem with all routed protocols. The RIF code does not inform the routing protocols when an entry in the table changes. Therefore, the cache entries become invalid. [CSCdi17099]
- When using prioritization with remote source-route bridging, the number of packets in the TCP queue for a given peer can exceed the number specified in the maximum output TCP queue length (specified with the **source-bridge tcp-queue-max** command). The workaround is to turn off prioritization. [CSCdi27718]

Interfaces and Bridging

- SSE switching cannot be configured for IP unless the interface has an IP address (or is unnumbered). This means that it is not possible to SSE switch out a Frame Relay interface where the primary interface is not given an address. The workaround is to make the primary interface unnumbered. [CSCdi29955]

IP Routing Protocols

- If you are using candidate default routes in IP Enhanced IGRP, be aware that there is a backwards compatibility problem between Cisco versions earlier than Releases 9.21(5), 10.0(5), 10.2(1), and later Cisco versions. Upgrade all routers to Release 9.21(5), 10.0(5), and 10.2(1) or later.

  The problem is as follows: When routers running the later versions are directly attached with neighbors running the earlier version, some Enhanced IGRP internal routes appear as candidate default routes in the routers running the later version. This can lead to the gateway of last resort being incorrectly set. If your autonomous system relies upon Enhanced IGRP to set the gateway of last resort, traffic that is routed through the gateway of last resort is likely to loop.

  (A candidate default route is a route that is tagged by the advertiser of the route to indicate to receivers that they should consider the route as the default route. A router that is selected as the gateway of last resort is one that advertises the best metric for candidate default routes.)

  A complete fix to the backwards compatibility problem is available as of Releases 9.21(6), 10.0(5), and 10.2(1). Routers running a version older than those versions cannot mark Enhanced IGRP internal routes as candidate default routes. [CSCdi23758]

VINES

- The VINES address the router retains to assign to clients is not incremented after it is assigned to a client until the router receives an update (RTP or SRTP) from the client. This leaves a short window in which duplicate address assignments can occur. [CSCdi29886]
- There is no form of modem control that offers the capabilities of **modem cts-required** or **modem callout** that also allows simultaneous HW flow control. [CSCdi26270]
- When using LQM with PPP on a system that does autonomous switching, like a Cisco 7000, if the PPP quality is set too high, the link may go down if significant amounts of the traffic are autonomously switched. There is a race condition at reboot where a Cisco 7000 may sometimes not start PPP when it reboots. [CSCdi28655]
- In certain traffic loading conditions on async lines (generally, an async line with receive and transmit looped) while using reverse Telnet, garbage characters may be output on the line. [CSCdi29696]
- If an ASM async interface is configured with the **flowcontrol hardware in** command, the CTS line does not honor flow control requests. Issue the **flowcontrol hardware** command to cause correct operation. [CSCdi30054]

Novell IPX

- When a new adapter is inserted into the router after it is booted, the interface short name is missing from commands like **show ipx server**. [CSCdi27331]
- In a network with a mixture of routers running 9.1 and 9.21 or later Cisco images, where one or more of the 9.1 units are using ipx helper-address network.ffff.ffff.ffff where network is some network other than -1. IPX NetBIOS filters will not be enforced on the helpered packets when they are received on the 9.21 or later units. [CSCdi30101]

Microcode Revision History

The following sections describe each revision of microcode for the Cisco 7000 series Switch Processor (SP) and for each interface processor.

ATM Interface Processor (AIP) Microcode Revision Summary

AIP Microcode Version 10.5

Modification

AIP Version 10.5 fixes the following bug:

- AIP cards that support E3, DS3, or TAXI connections occasionally stop functioning in high-temperature situations because of a timing problem in the AIP hardware. [CSCdi29885]

AIP Microcode Version 10.7

Modification

AIP Version 10.7 fixes the following bug:

- Previous versions of the AIP code rejected cells with the congestion experienced bit set. The code no longer rejects such cells. [CSCdi36762]

AIP Microcode Version 10.8

Modification

AIP Version 10.8 fixes the following bug:

- Previous versions of the AIP code did not work properly with the 2 MB SSP.

AIP Microcode Version 10.9

Modification

AIP Microcode Version 10.9 adds the following:

- JT2 PLIM support.

AIP Microcode Version 10.10

Modification

AIP Microcode Version 10.10 fixes the following bug:

- Ethernet packets that are too short are sent by a Catalyst 5000 if a short packet originates on an FDDI ring and is routed to the Catalyst 5000 by a Cisco 7000 router via an Emulated LAN (ELAN). To work around, turn off fast switching (**no ip route-cache**) on the ATM interface on the Cisco 7000 router. [CSCdi41868]

AIP Microcode Version 10.11

Modification

AIP Microcode Version 10.11 fixes the following bug:

- AIP interface fails to establish Permanent Virtual Channels (PVCs) after reload until a **config memory** command is performed. [CSCdi43387]

AIP Microcode Version 10.12

Modification

AIP Microcode Version 10.12 fixes the following bug:

- The AIP card of the Cisco 7000 series routers does not map the virtual path identifier/virtual channel identifier (VPI/VCI) pair used in an ATM connection unless the router is initiating the switched virtual circuit. [CSCdi32192]

AIP Microcode Version 10.13

Modification

AIP Microcode Version 10.13 fixes the following bug:

- Ping functions fail when SMDS is configured. [CSCdi45807]

AIP Microcode Version 10.14

Modification

AIP Microcode Version 10.14 fixes the following bugs:

- 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 10.15

Modification

AIP Microcode Version 10.15 fixes the following bug:

- 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

Modification

AIP Microcode Version 10.16 fixes the following bugs:

- Bad SAP messages are received. [CSCdi67812]
- Online Insertion and Removal (OIR) events cause ATM traffic to be lost. [CSCdi66076]

AIP Microcode Version 10.17

Modification

AIP Microcode Version 10.17 fixes the following bugs:

- 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]

Channel Interface Processor (CIP) Microcode Revision Summary

CIP Microcode Version 10.6

Modifications

CIP Microcode Version 10.6 fixes the following bugs:

- On the parallel channel, in rare conditions, a duplicate packet might be sent to the host and the intended packet lost. [CSCdi31205]
- The CIP will breakpoint with the message “SCB chain out of sequence” with a parallel channel interface if it receives a host reset while disconnected and chaining. [CSCdi31207]

CIP Microcode Version 10.7

Modifications

CIP Microcode Version 10.7 fixes the following bugs:

- When the PCA daughter card did not have a BUS & TAG cable connected at boot time, spurious noise could confuse the card into incorrectly determining that the test “wrap plug” was connected. [CSCdi36464]
- The parallel channel adapter may not come back online after it detects the host dropping OP OUT. [CSCdi37182]

- If the CIP gets a reset at the wrong moment, it may write bad parity to the RAM. Because the memory is only initialized by a power-on reset or by a reset of the whole router (code reload), the bad parity stays in memory for a long time. A simple microcode reload would not fix it. The next time the CPU reads the memory location with the bad parity, it will take a cache error exception, which in turn will lead to another microcode reload. As of now, the workaround is to either reload the 7000 or (as a less drastic measure) remove the CIP and re-insert. This forces the CIP to go through its power-on reset routine, which initializes all RAM and the board. If the parity error occurs before the operational code is downloaded, it can only be fixed with a new ROM. [CSCdi29830]
- A Test I/O command may take a device offline. [CSCdi33491]
- For a PCA adapter card, the Link Failure count is being erroneously incremented. When OP OUT is down and the PCA is configured and running, it will present a link failure to the CIP card approximately every 3 seconds. There is no loss of functionality. The link failure count should only be incremented once every time it detects OP OUT to be down. [CSCdi33714]
- CIP PCA bad cable can appear as a wrap plug. Make sure wrap diagnostics only run when a wrap plug is installed. [CSCdi33716]
- On a bus/tag channel, if a device has been configured and active on the channel, a system reset may cause the device to be placed in a bad state. [CSCdi34346]

CIP Microcode Version 10.8

Modifications

CIP Microcode Version 10.8 fixes the following bugs:

- When using RIP (ROUTED) to provide a redundant IP datagram mode (CLAW) connection to the host and both CLAW connections define the host with the same IP address, loss of one of the CLAW connections at the CLAW protocol layer could cause both connections to be ineffective in providing a redundant configuration. [CSCdi31491]
- Calling into the CIP console via the RP's serial ports and modem, and then disconnecting while still in the CIP console mode (if-console), causes perpetual cycling of output from the modem, to the modem. This continuous input to the CIP console could cause the CIP to crash. It is good practice to quit the CIP console before disconnecting the remote modem connection. [CSCdi38466]
- If the host ends a read operation before all data has been transferred, in some cases the CIP may crash with a SCBCHAIN indication. [CSCdi39639]
- Running some versions of CIP microcode can cause certain individual CIPs to crash with a cache parity error. All versions of CIP microcode which contain VPLD version 4.28 are at risk. This affects cip10-7, cip11-0 and cip11-1. If the CIP crashes because of this problem, it will dump the trace table whose last line will look like this:

  ```
  %CIP3-0-MSG: %DEBUGGER-0-TRACE_DATA: 800XXXXX  0004 ...
  ```

  To verify that a crash was caused by this problem, the entire crash dump output (roughly 180 lines) should be provided to Cisco Technical Assistance Center (TAC). [CSCdi40754]
- If a CIP in a Cisco 7500 router (RSP) crashes, it only displays the first part of the crash dump before being reset by the RSP. This is caused by an interrupt timeout. [CSCdi40895]

- With CIP microcode versions earlier than CIP 10.8 and system code later than 10.2(8.4), 10.3.(6.1), or 11.0(1.1), a microcode reload or a system reload could cause the static route for the claw or offload commands to fail to be added. This only happens on a PCA interface that is configured and in the “no shut” state at the time of the reload. [CSCdi41992]

CIP Microcode Version 10.9

Modifications

CIP Microcode Version 10.9 fixes the following bugs:

- Some CIP cards will run for long periods of time (weeks or months) and then hang without any error condition indicated on the host or router console. This is due to the CBUS FIFOs erroneously resetting prior to each direct memory access (DMA) transfer. [CSCdi43981]
- VPLD v4-32 too slow for old, old Altera parts. [CSCdi44782]

CIP Microcode Version 20.5

Modifications

CIP Microcode Version 20.5 fixes the following bugs:

- CIP does not perform MEMD buffer header integrity checks. [CSCdi46103]
- CIP attempts to connect to the host via a device in the busy state. The asynchronous connection code needs a check for the busy bit in the devices control block, and if the bit set, to deny the connection. [CSCdi46226]
- If the Bus Out cable has a defect, a parity error will to be detected by the CIP, and the CIP may need to be reloaded. [CSCdi44111]

CIP Microcode Version 20.6

Modifications

CIP Microcode Version 20.6 fixes the following bugs:

- CIP IPC requires at least one interface to be completely up before allowing access to MEMD. [CSCdi48381]
- When a cancel occurs during a command chained operation after status was presented and before the next command was presented, the PCA presents this cancel as if nothing was active. This may result in an SCB_CHAIN error. [CSCdi49057]
- Following a purge or stop of the TCPIP stack on an MVS, when the user restarts TCP/IP, the PCA channel connection won’t come up. The subchannel remains in a Path Not Operational state. A **shut**/**no shut** or a reload must be performed on the CIP interface to get it working. [CSCdi49464]

CIP Microcode Version 20.8

Modification

CIP Microcode Version 20.8 fixes the following bugs:

- A fatal error output can occur, causing a dBus interrupt (DBUSINTERR) to occur. [CSCdi55033]
- Telnet sessions that use the CIP offload function can hang during periods of peak usage. [CSCdi55044]
- Extra dBus polling can occur when the I/O pending bit is erroneously set. [CSCdi58927]
- A port adapter logout is impossible when adapter tasks become stuck. [CSCdi57233]
- The offload function cannot be configured unless a virtual interface is up. [CSCdi58177]

CIP Microcode Version 20.9

Modification

CIP Microcode Version 20.9 fixes the following bugs:

- If the router switches a packet to the CIP for the virtual port adapter (interface channel *slot*/2) using the wrong virtual circuit number, the CIP crashes with the following error message: [CSCdi61532]

  ```
  %CIP5-3-MSG: %CONFIG-3-WRONGINT: VCN 0(0000) not for port adapter 2
  ```

- If the CIP gets a packet greater than 4K from a Route Processor (RP) or Route Switch Processor (RSP), the CIP might stop functioning properly and might eventually crash with fatal errors. If this problem occurs, you will see the following message:

  ```
  CLAW-6-TOOBIG: 4352 byte IP datagram exceeds CLAW MTU for device
  ```

  To work around this problem, reload the router. [CSCdi64874]

- On a CIP with CSNA and TCP Offload both in use, TCP sessions might randomly quit with the remote client appearing to have requested disconnect. [CSCdi63044]
- Sometimes a mainframe cannot send packets to a CIP. [CSCdi66108]
- When a CIP reads 7 MB/sec from MEMD in an RSP platform, occasionally the CIP detects a bad transfer and produces messages such as: [CSCdi54732]

  ```
  *Apr 15 14:21:58: %CIP10-0-MSG: %DMA-0-BADFIFO: FIFO failure detected during transfer (40
  0001)
  ```

CIP Microcode Version 20.10

Modification

CIP Microcode Version 20.10 fixes the following bugs:

- Parity and interrupts functions are disabled while flushing on an hw5 CIP. [CSCdi55192]
- Each configured device (pair) does not have the minimum requirement of 16 transmit (tx) buffers. [CSCdi54042]
- Issuing CIP console commands could cause DBUS errors. [CSCdi67549]

- Inadequate diagnostics are available for the ESCON port adapter. [CSCdi71938]
- ESCON link-level errors might cause the CIP to hang. [CSCdi69548]
- There is no ability to put individual subchannels into a command retry. [CSCdi45356]

CIP Microcode Version 20.11

Modification

CIP Microcode Version 20.11 fixes the following bugs:

- Multiple resets could cause loss of transmit buffers. [CSCdi72853]
- The exe2sim function does not support COFF format. [CSCdi72894]
- A CIP Fatal Error 35 occurs after SHUTDOWN is issued on the channel interface. [CSCdi74491]
- A crash might occur at <putc+b8> lhu $v0,8($zero). [CSCdi74911]
- The CIP interface Buffer Counter becomes corrupted when RXCURR is greater than RXHIGH. [CSCdi75138]
- During request in path, inbound-to-host performance drops. [CSCdi76020]
- ADAPTER-0-DIAGDATA module 1221 error FE14 occurs when using the new ESCON diagnostics. [CSCdi84660]

CIP Microcode Version 20.12

Modification

CIP Microcode Version 20.12 fixes the following bugs:

- Previously, the CIP microcode allocated 64 buffers for each CLAW device, and the number of buffers per CLAW would increased if there was a sudden burst of traffic and a large number of routes being passed to host-based TCP/IP stacks.

  With the fix for this bug, for each CLAW statement, the CIP microcode will retain the static 64 buffers that are 4096 in size. However, each 4096 byte buffer can be segmented into either 4 smaller buffers of 1024 bytes each or eight smaller buffers of 512 bytes each. When buffers are allocated in this fashion, the 4096 byte buffer is reassembled after all of the smaller chunks are freed. [CSCdj03799]

- During the recovery of certain ESCON link errors, the CIP might crash with a FATAL-ERROR, after the ESCON adapter reports a device level error at a time when there is no active device. When this problem occurs, the FATAL-ERROR is preceeded by the following error message:

  ```
  CCA-0-DEV_ERR2: Device error but no active defined device
  ```

  The only work-around, short of replacing the microcode with the microcode that has this problem fixed, is to determine and resolve the reason for the ESCON link error. [CSCdj21031]

Channel Interface Processor, Second-Generation (CIP2) Microcode Revision Summary

CIP2 Microcode Version 20.8

CIP2 Microcode Version 20.8 was released on June 8, 1996.

CIP2 Microcode Version 20.9

Modification

CIP2 Microcode Version 20.9 fixes the following bugs:

- If the router switches a packet to the CIP2 for the virtual port adapter (interface channel *slot*/2) using the wrong virtual circuit number, the CIP2 crashes with the following error message: [CSCdi61532]

  ```
  %CIP5-3-MSG: %CONFIG-3-WRONGINT: VCN 0(0000) not for port adapter 2
  ```

- If the CIP2 gets a packet greater than 4K from a Route Processor (RP) or Route Switch Processor (RSP), the CIP2 might stop functioning properly and might eventually crash with fatal errors. If this problem occurs, you will see the following message:

  ```
  CLAW-6-TOOBIG: 4352 byte IP datagram exceeds CLAW MTU for device
  ```

  To work around this problem, reload the router. [CSCdi64874]

- On a CIP2 with CSNA and TCP Offload both in use, TCP sessions might randomly quit with the remote client appearing to have requested disconnect. [CSCdi63044]
- Sometimes a mainframe cannot send packets to a CIP. [CSCdi66108]
- When a CIP2 reads 7 MB/sec from MEMD in an RSP platform, occasionally the CIP2 detects a bad transfer and produces messages such as: [CSCdi54732]

  ```
  *Apr 15 14:21:58: %CIP10-0-MSG: %DMA-0-BADFIFO: FIFO failure detected during transfer (40
  0001)
  ```

CIP2 Microcode Version 20.10

Modification

CIP2 Microcode Version 20.10 fixes the following bugs:

- Parity and interrupts functions are disabled while flushing on an hw5 CIP. [CSCdi55192]
- Each configured device (pair) does not have the minimum requirement of 16 transmit (tx) buffers. [CSCdi54042]
- Issuing CIP console commands could cause DBUS errors. [CSCdi67549]
- Inadequate diagnostics are available for the ESCON port adapter. [CSCdi71938]
- ESCON link-level errors might cause the CIP to hang. [CSCdi69548]
- There is no ability to put individual subchannels into a command retry. [CSCdi45356]

CIP2 Microcode Version 20.11

Modification

CIP2 Microcode Version 20.11 fixes the following bugs:

- Multiple resets could cause loss of transmit buffers. [CSCdi72853]
- The exe2sim function does not support COFF format. [CSCdi72894]
- A CIP Fatal Error 35 occurs after SHUTDOWN is issued on the channel interface. [CSCdi74491]
- A crash might occur at <putc+b8> lhu $v0,8($zero). [CSCdi74911]
- The CIP interface Buffer Counter becomes corrupted when RXCURR is greater than RXHIGH. [CSCdi75138]
- During request in path, inbound-to-host performance drops. [CSCdi76020]
- ADAPTER-0-DIAGDATA module 1221 error FE14 occurs when using the new ESCON diagnostics. [CSCdi84660]

CIP2 Microcode Version 20.12

Modification

CIP2 Microcode Version 20.12 fixes the following bugs:

- Previously, the CIP microcode allocated 64 buffers for each CLAW device, and the number of buffers per CLAW would increased if there was a sudden burst of traffic and a large number of routes being passed to host-based TCP/IP stacks.

  With the fix for this bug, for each CLAW statement, the CIP microcode will retain the static 64 buffers that are 4096 in size. However, each 4096 byte buffer can be segmented into either 4 smaller buffers of 1024 bytes each or eight smaller buffers of 512 bytes each. When buffers are allocated in this fashion, the 4096 byte buffer is reassembled after all of the smaller chunks are freed. [CSCdj03799]

- During the recovery of certain ESCON link errors, the CIP might crash with a FATAL-ERROR, after the ESCON adapter reports a device level error at a time when there is no active device. When this problem occurs, the FATAL-ERROR is preceeded by the following error message:

  ```
  CCA-0-DEV_ERR2: Device error but no active defined device
  ```

  The only work-around, short of replacing the microcode with the microcode that has this problem fixed, is to determine and resolve the reason for the ESCON link error. [CSCdj21031]

Ethernet Interface Processor (EIP) Microcode Revision Summary

EIP Microcode Version 10.1

Modification

EIP Microcode Version 10.1 fixes the following bug:

- Allows for other stations to burst back-to-back packets on the wire without the router trying to initiate a transmit. The packets must be separated by the effective interframe gap time for the router to defer to the burst. The effective interframe gap time is 9.6 microseconds plus whatever transmitter delay is configured. The transmitter delay now configures two parameters: the lower 8 bits are used to compute an effective interframe gap time; the upper 8 bits are the number of bursted packets to defer to before initiating a transmit.

Fast Ethernet Interface Processor (FEIP) Microcode Revision Summary

FEIP Microcode Version 10.0

Modification

FEIP Microcode Version 10.0 introduced support for 100 BaseTX Ethernet interfaces.

FEIP Microcode Version 10.1

Modifications

FEIP Microcode Version 10.1 fixes the following bugs:

- A CyBus DMA problem, a CyBus parity problem, and a PCI register timeout problem were addressed.
- RSP support was made more robust.
- The collision and deferred counters were fixed.
- Performance enhancements were introduced.
- ISL support was introduced.

FEIP Microcode Version 10.2

Modification

FEIP Microcode Version 10.2 fixes the following bug:

- A hardware manufacturing change affected margin timing. [CSCdi40448]

FEIP Microcode Version 10.3

Modification

FEIP Microcode Version 10.3 fixes the following bug:

- Serial interfaces that are down but not administratively disabled might periodically reset and display the error “8010 - disable fsip_reset.” [CSCdi49431]

FEIP Microcode Version 10.4

Modification

FEIP Microcode Version 10.4 fixes the following bug:

- The FX port adapter is not supported. [CSCdi48337]

FEIP Microcode Version 10.5

Modification

FEIP Microcode Version 10.5 fixes the following bugs:

- FEIP MII interface fails to reset if there is OIR of another card in the router. [CSCdi82350]
- You are unable to ping/Telnet HSRP virtual address on FastEthernet. [CSCdi92485]

Fiber Distributed Data Interface (FDDI) Interface Processor (FIP) Microcode Revision Summary

FIP Microcode Version 10.2

Modification

FIP Microcode Version 10.2 fixes the problem of the FIP possibly going into TRACE mode upon reboot of a neighboring station.

Fast Serial Interface Processor (FSIP) Microcode Revision Summary

FSIP Microcode Version 10.7

Modifications

FSIP Microcode Version 10.7 fixes the following bugs:

- Priority queuing on a Cisco 7000 serves the low (and normal, medium, ...) queues even if the high queue is filled all the time. [CSCdi28181]
- When a serial line is highly utilized and the idle code is set to mark (not Flags), the show interface display may show a high number of aborts. [CSCdi28278]

FSIP Microcode Version 10.8

Modification

FSIP Microcode Version 10.8 fixes the following bug:

- In high-traffic environments, FSIP8 will get FCICMDFAIL messages and may eventually get 8010 fsip_reset because of multiple command timeouts. The command timeout was caused by a long path in the FSIP firmware during the memd read on transmit. FSIP Microcode Version 10.8 fixes this problem by splitting the memd read on transmit into 32-byte chunks and enabling interrupts between the chunks.

FSIP Microcode Version 10.9

Modification

FSIP Microcode Version 10.9 fixes the following bug:

- Under high traffic conditions, the FSIP may fail with the following error: %CBUS-3-INITERR: Interface x, error(D104). This error would cause all cBus boards to be reset. When this error condition occurs, the affected interface is now reset and a frame error will be counted on the interface. [CSCdi33079]

FSIP Microcode Version 10.10

Modifications

FSIP Microcode Version 10.10 fixes the following bugs:

- Data carrier detect signals are not ignored on high-end Cisco platforms as needed for SDLC Multidrops. [CSCdi32813]
- A 3725 may not IPL when connected to a Cisco 7000 router. The SDLC line is in a down/down state because RTS is not present when the 3725 is IPL'd. [CSCdi38317]

FSIP Microcode Version 10.11

Modifications

FSIP Microcode Version 10.11 fixes the following bugs:

- SDLC Multidrops need the router to ignore DCD for high-end platforms. [CSCdi32813]
- A Cisco 3725 using FSIP might be unable to transmit via a serial driver, because a request-to-send (RTS) gets dropped and the port is declared to be in a down/down state. [CSCdi38317]

FSIP Microcode Version 10.12

Modification

FSIP Microcode Version 10.12 fixes the following bug:

- FSIP counts alarm signals hundreds or thousands more times than they actually occur. [CSCdi42881]

FSIP Microcode Version 10.13

Modification

FSIP Microcode Version 10.13 fixes the following bug:

- FSIP resets with error 8010, “disable - fsip_reset.” [CSCdi49431]

Note FSIP 10.14 and FSIP 10.15 microcode versions were never released.

FSIP Microcode Version 10.16

Modification

FSIP Microcode Version 10.16 fixes the following bugs:

- Transmitter-delay does not work on FSIP DCE interfaces. [CSCdi58196]
- Using FSIP might cause a ciscoBus restart. [CSCdi58194]

FSIP Microcode Version 10.17

Modification

FSIP Microcode Version 10.17 fixes the following bug:

- FSIP does not recognize DCE 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 bug:

- In DCE mode, FSIP looks for DCD and DSR up before declaring the line UP. FSIP should only look for DCD. [CSCdi64735]

HSSI Interface Processor (HIP) Microcode Revision Summary

HIP Microcode Version 10.2

Modification

HIP Microcode Version 10.2 fixes the following bug:

- A router running a non-Bufferin image from system ROMs cannot load an unbundled Bufferin HIP microcode from Flash memory. [CSCdi28580]

MultiChannel Interface Processor (MIP) Microcode Revision Summary

MIP Microcode Version 11.0

Modification

MIP Microcode Version 11.0 introduced support for Channelized E1.

MIP Microcode Version 11.1

Modification

MIP Microcode Version 11.1 does not include any functional changes or bug fixes. It incorporates some code modifications that will facilitate future functional changes.

MIP Microcode Version 11.2

Modifications

MIP Microcode Version 11.2 fixes the following bugs:

- This problem will occur with certain pieces of equipment in the field that will inject all 0's in Timeslot 16 when receiving a remote alarm. Most of these can be configured for which pattern to inject. [CSCdi36414]
- Australia homologation testing for Layer 1 is different from NET5 homologation—Australia adds some Layer 1 specific issues. Australian homologation for PRI requires the monitoring of errors, and if the error rate is greater than 10.3, RAI signaling is sent out. In order to accomplish it, a code and a keyword for the controller E1 framing command is added. These commands are used as follows:

  ```
  controller E1 1/0
  framing crc4 Australia
  ```

  or

  ```
  controller E1 1/0
  ```

MIP Microcode Version 11.3

Modification

MIP Microcode Version 11.3 fixes the following bug:

- MIP select takes too long. [CSCdi38132]

MIP Microcode Version 11.4

Modification

MIP Microcode Version 11.4 fixes the following bug:

- The MIP board drops packets in severely bursty traffic. [CSCdi46383]

Switch Processor (SP) Microcode Revision Summary

SP Microcode Version 10.8

Modifications

SP Version 10.8 fixes the following bugs:

- LAN Network Manager (LNM) cannot link to images across a Token Ring interface. [CSCdi29096]
- Pinging directly attached nodes on a Token Ring network fails. [CSCdi29228]
- Remote source-route bridging and autonomous switching do not work. [CSCdi29383]

SP Microcode Version 10.9

Modifications

SP Microcode Version 10.9 fixes the following:

- Flooding through FDDI has been fixed (part of CSCdi23977).
- The problem of intermittent (random) MEMA corruption during flooding has been fixed.
- A Multibus time-out no longer occurs when the inbound interface is removed from an autonomous bridge group while flooding is in progress.
- Support for LAN emulation has been added.
- An error handling problem that occurred when the IPX hop count was invalid has been fixed.
- The Tx Reserve error messages “803C - tx0_reserve” and “803D - tx1_reserve” have been improved.

SP Microcode Version 10.10

Modification

SP Microcode Version 10.10 fixes the following bug:

- During SSE switching, the 802.3 length field contained the actual packet length, including any padding required to send the frame over the Ethernet. Some Novell applications (specifically RCONSOLE) check the 802.3 length against the IPX protocol packet length. When padding is present, these two lengths do not agree and RCONSOLE reports an error. With this release, the 802.3 length matches the IPX frame length for all packet lengths. [CSCdi30876]

SP Microcode Version 10.11

Modification

SP Microcode Version 10.11 fixes the following bug:

- MTU values set by system code are overridden by the microcode. [CSCdi30592]

SP Microcode Version 10.12

Modifications

SP Microcode Version 10.12 fixes the following bugs:

- When cBus bridging is configured and there are more than 14 station MAC addresses in the bridge cache having the same least significant byte, then the system is vulnerable to a multibus timeout bus error under certain traffic conditions. When cBus bridging is configured on serial and FDDI interfaces, traffic bridged from a serial interface to an FDDI interface will be incorrectly encapsulated.
- Multiring and LAN Network Manager (LNM) on FDDI do not work on Cisco 7000 routers. [CSCdi33782]
- The **ipx ping** command fails to SSE switch if the packet length size is between 61 and 70 bytes. [CSCdi36115]
- When autonomous bridging is turned on for FDDI and HSSI, the packets from HSSI to FDDI are corrupted. [CSCdi36271]
- If the cBus has more than two MTU-sized pools with an SSP, a transmit hang will cause the SSP to crash. [CSCdi36490]

SP Microcode Version 10.13

Modifications

SP Microcode Version 10.13 fixes the following bugs:

- IP packets sent to the HSRP virtual MAC address are not received if the packet is SNAP-encapsulated and the receiving interface is part of the cBus or Switch Processor (SP) complex. [CSCdi39274]
- ISL classification support for the Fast Ethernet Interface Processor (FEIP) was added.

SP Microcode Version 10.14

Modifications

SP Microcode Version 10.14 fixes the following bugs:

- IPX packets might be corrupted if autonomous switched. [CSCdi39790]
- Connecting AIPs back-to-back might cause packet loss. [CSCdi42703]
- IP SSE switched out serial interfaces are not correctly accounted for. [CSCdi32500]
- The multibus I/O crashes at address 0x1110C14C. [CSCdi46295]

SP Microcode Version 10.15

Modifications

SP Microcode Version 10.15 fixes the following bugs:

- Turning on **ipx route-cache sse** can produce 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. [CSCdi42802]
- The microcode is missing the spXX-XX.lst file. [CSCdi52289]

Silicon Switch Processor (SSP) Microcode Revision Summary

SSP Microcode Version 10.8

Modifications

SSP Microcode Version 10.8 fixes the following bugs:

- LAN Network Manager (LNM) cannot link to images across a Token Ring interface. [CSCdi29096]
- Pinging directly attached nodes on a Token Ring network fails. [CSCdi29228]
- Remote source-route bridging and autonomous switching do not work. [CSCdi29383]

SSP Microcode Version 10.9

Modifications

SSP Microcode Version 10.9 fixes the following bugs:

- Flooding through FDDI has been fixed (part of CSCdi23977).
- The problem of intermittent (random) MEMA corruption during flooding has been fixed.
- A Multibus time-out no longer occurs when the inbound interface is removed from an autonomous bridge group while flooding is in progress.
- Support for LAN emulation has been added.

- An error handling problem that occurred when the IPX hop count was invalid has been fixed.
- The Tx Reserve error messages “803C - tx0_reserve” and “803D - tx1_reserve” have been improved.

SSP Microcode Version 10.10

Modification

SSP Microcode Version 10.10 fixes the following bug:

- During SSE switching, the 802.3 length field contained the actual packet length, including any padding required to send the frame over the Ethernet. Some Novell applications (specifically RCONSOLE) check the 802.3 length against the IPX protocol packet length. When padding is present these two lengths do not agree and RCONSOLE reports an error. With this release, the 802.3 length matches the IPX frame length for all packet lengths. [CSCdi30876]

SSP Microcode Version 10.11

Modification

SSP Microcode Version 10.11 fixes the following bug:

- MTU values set by system code are overridden by the microcode. [CSCdi30592]

SSP Microcode Version 10.12

Modifications

SSP Microcode Version 10.12 fixes the following problems:

- When cBus bridging is configured and there are more than 14 station MAC addresses in the bridge cache having the same least significant byte, then the system is vulnerable to a multibus timeout bus error under certain traffic conditions. When cBus bridging is configured on serial and FDDI interfaces, traffic bridged from a serial interface to an FDDI interface will be incorrectly encapsulated.
- Multiring and LAN Network Manager (LNM) on FDDI do not work on Cisco 7000 routers. [CSCdi33782]
- The **ipx ping** command fails to SSE switch if the packet length size is between 61 and 70 bytes. [CSCdi36115]
- When autonomous bridging is turned on for FDDI and HSSI, the packets from HSSI to FDDI are corrupted. [CSCdi36271]
- If the cBus has more than two MTU-sized pools with an SSP, a transmit hang will cause the SSP to crash. [CSCdi36490]

SSP Microcode Version 10.13

Modifications

SSP Microcode Version 10.13 fixes the following problems:

- IP packets sent to the HSRP virtual MAC address are not received if the packet is SNAP-encapsulated and the receiving interface is part of the cBus or SP complex. [CSCdi39274]
- ISL classification support for the Fast Ethernet Interface Processor (FEIP) was added.

SSP Microcode Version 10.14

Modifications

SSP Microcode Version 10.14 fixes the following bugs:

- IPX packets might be corrupted if autonomous switched. [CSCdi39790]
- Connecting AIPs back-to-back might cause packet loss. [CSCdi42703]
- IP SSE switched out serial interfaces are not correctly accounted for. [CSCdi32500]
- The multibus I/O crashes at address 0x1110C14C. [CSCdi46295]

SSP Microcode Version 10.15

Modifications

SSP Microcode Version 10.15 fixes the following bugs:

- Turning on **ipx route-cache sse** can produce 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. [CSCdi42802]
- The microcode is missing the spXX-XX.lst file. [CSCdi52289]

Token Ring Interface Processor (TRIP) Microcode Revision Summary

TRIP Microcode Version 10.1

Modifications

TRIP Microcode Version 10.1 fixes the following problems:

- Some catastrophic errors would cause a flood of error messages. The number of messages has been reduced.
- This version significantly reduces the load on a queue that at overflow causes the interface to be placed in a reset state (CTRUCHECK).
- The processing of some extremely rare events in noisy networks caused the card to cease operation.

- Token Ring interfaces kept too many buffers locally (very low receive queue limits) if SRB was enabled.

TRIP Microcode Version 10.2

Modifications

TRIP Microcode Version 10.2 fixes the following bugs:

- Extremely rarely, a CTRUCHECK error occurs as a result of a command queue overflow. This code reduces the load on this queue by deferring functions of a noncritical nature. [CSCdi31131]
- Two problems were fixed that very rarely cause Token Ring interfaces to cease transmitting. These errors require that the interface be reinitialized. The message logged by the system is "800E output hung" or "800E tx queue full". [CSCdi31121]

TRIP Microcode Version 10.3

Modifications

TRIP Microcode Version 10.3 fixes the following problems:

- The DMA engine appears to "clock in" the memd address an extra time or increment the memd address an extra time. The obvious symptom of this problem is an "800E" error message.
- Transmit frames have invalid Access Control bytes (bit 0x10 set).
- A SpyGlass problem causes Adapter Checks.

TRIP Microcode Version 10.4

Modifications

TRIP Microcode Version 10.4 fixes the following problems:

- The SpyGlass command queue overflows, and you will observe a "ctrucheck" state.

RSP Microcode Revision History

The following sections describe each revision of microcode for each Cisco 7500 series interface processor.

ATM Interface Processor (AIP) Microcode Revision Summary

AIP Microcode Version 20.2

Modifications

AIP Version 20.2 fixes the following bugs:

- The AIP should set the OAM cell length to 56 bytes.

- The AIP rejects cells with a congestion experienced bit set.
- Initial JT2 PLIM support was added.

AIP Microcode Version 20.3

Modification

AIP Version 20.3 fixes the following bug:

- Fast-switched frames from FDDI to ATM-LANE are not padded. Illegal (too short) Ethernet packets are forwarded by a Catalyst 5000, if the packets originate on an FDDI ring and are routed to the Catalyst 5000 by a Cisco 7000 router via an emulated LAN (ELAN). The workaround is to turn off fast switching using the **no ip route-cache** command on the ATM interface on the Cisco 7000 router. [CSCdi41868].

AIP Microcode Version 20.4

Modification

AIP Version 20.4 fixes the following bug:

- AIP interface fails to establish Permanent Virtual Channels (PVCs) after reload until a **config memory** command is performed. [CSCdi43387]

AIP Microcode Version 20.5

Modification

AIP Version 20.5 fixes the following bug:

- The AIP card of the Cisco 7000 series routers does not map the virtual path identifier/virtual channel identifier (VPI/VCI) pair used in an ATM connection unless the router is initiating the switched virtual circuit. [CSCdi32192]

AIP Microcode Version 20.6

Modification

AIP Version 20.6 fixes the following bug:

- Ping functions fail when SMDS is configured. [CSCdi45807]

AIP Microcode Version 20.7

Modification

AIP Version 20.7 fixes the following bugs:

- 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 Version 20.8 fixes the following bug:

- 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

Modification

AIP Microcode Version 20.9 fixes the following bugs:

- Bad SAP messages are received. [CSCdi67812]
- ATM traffic is lost with Online Insertion and Removal (OIR) events. [CSCdi66076]

AIP Microcode Version 20.10

Modification

AIP Microcode Version 20.10 fixes the following bugs:

- 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]

Channel Interface Processor (CIP) Microcode Revision Summary

CIP Microcode Version 20.3

Modifications

CIP Microcode Version 20.3 fixes the following bugs:

- Some CIP cards will run for long periods of time (weeks or months) and then hang without any error condition indicated on the host or router console. This is caused by the CBUS FIFOs erroneously resetting prior to each direct memory access (DMA) transfer. [CSCdi43981]
- VPLD v4-32 is too slow for old Altera parts. [CSCdi44782]

CIP Microcode Version 20.5

Modifications

CIP Microcode Version 20.5 fixes the following bugs:

- CIP does not perform MEMD buffer header integrity checks. [CSCdi46103]
- CIP attempts to connect to the host via a device in the busy state. The asynchronous connection code needs a check for the busy bit in the devices control block, and if the bit set, to deny the connection. [CSCdi46226]
- If the Bus Out cable has a defect, a parity error will to be detected by the CIP, and the CIP may need to be reloaded. [CSCdi44111]

CIP Microcode Version 20.6

Modifications

CIP Microcode Version 20.6 fixes the following bugs:

- CIP IPC requires at least one interface to be completely up before allowing access to MEMD. [CSCdi48381]
- When a cancel occurs during a command chained operation after status was presented and before the next command was presented, the PCA presents this cancel as if nothing was active. This may result in an SCB_CHAIN error. [CSCdi49057]
- Following a purge or stop of the TCPIP stack on an MVS, when the user restarts TCP/IP, the PCA channel connection won't come up. The subchannel remains in a Path Not Operational state. A **shut**/**no shut** or a reload must be performed on the CIP interface to get it working. [CSCdi49464]

CIP Microcode Version 20.8

Modification

CIP Microcode Version 20.8 fixes the following bugs:

- A fatal error output can occur, causing a dBus interrupt (DBUSINTERR) to occur. [CSCdi55033]

- Telnet sessions that use the CIP offload function can hang during periods of peak usage. [CSCdi55044]
- Extra dBus polling can occur when the I/O pending bit is erroneously set. [CSCdi58927]
- A port adapter logout is impossible when adapter tasks become stuck. [CSCdi57233]
- The offload function cannot be configured unless a virtual interface is up. [CSCdi58177]

CIP Microcode Version 20.9

Modification

CIP Microcode Version 20.9 fixes the following bugs:

- If the router switches a packet to the CIP for the virtual port adapter (interface channel *slot*/2) using the wrong virtual circuit number, the CIP crashes with the following error message: [CSCdi61532]

  ```
  %CIP5-3-MSG: %CONFIG-3-WRONGINT: VCN 0(0000) not for port adapter 2
  ```

- If the CIP gets a packet greater than 4K from a Route Processor (RP) or Route Switch Processor (RSP), the CIP might stop functioning properly and might eventually crash with fatal errors. If this problem occurs, you will see the following message:

  ```
  CLAW-6-TOOBIG: 4352 byte IP datagram exceeds CLAW MTU for device
  ```

  To work around this problem, reload the router. [CSCdi64874]

- On a CIP with CSNA and TCP Offload both in use, TCP sessions might randomly quit with the remote client appearing to have requested disconnect. [CSCdi63044]
- Sometimes a mainframe cannot send packets to a CIP. [CSCdi66108]
- When a CIP reads 7 MB/sec from MEMD in an RSP platform, occasionally the CIP detects a bad transfer and produces messages such as: [CSCdi54732]

  ```
  *Apr 15 14:21:58: %CIP10-0-MSG: %DMA-0-BADFIFO: FIFO failure detected during transfer (40
  0001)
  ```

CIP Microcode Version 20.10

Modification

CIP Microcode Version 20.10 fixes the following bugs:

- Parity and interrupts functions are disabled while flushing on an hw5 CIP. [CSCdi55192]
- Each configured device (pair) does not have the minimum requirement of 16 transmit (tx) buffers. [CSCdi54042]
- Issuing CIP console commands could cause DBUS errors. [CSCdi67549]
- Inadequate diagnostics are available for the ESCON port adapter. [CSCdi71938]
- ESCON link-level errors might cause the CIP to hang. [CSCdi69548]
- There is no ability to put individual subchannels into a command retry. [CSCdi45356]

CIP Microcode Version 20.11

Modification

CIP Microcode Version 20.11 fixes the following bugs:

- Multiple resets could cause loss of transmit buffers. [CSCdi72853]
- The exe2sim function does not support COFF format. [CSCdi72894]
- A CIP Fatal Error 35 occurs after SHUTDOWN is issued on the channel interface. [CSCdi74491]
- A crash might occur at <putc+b8> lhu $v0,8($zero). [CSCdi74911]
- The CIP interface Buffer Counter becomes corrupted when RXCURR is greater than RXHIGH. [CSCdi75138]
- During request in path, inbound-to-host performance drops. [CSCdi76020]
- ADAPTER-0-DIAGDATA module 1221 error FE14 occurs when using the new ESCON diagnostics. [CSCdi84660]

CIP Microcode Version 20.12

Modification

CIP Microcode Version 20.12 fixes the following bugs:

- Previously, the CIP microcode allocated 64 buffers for each CLAW device, and the number of buffers per CLAW would increased if there was a sudden burst of traffic and a large number of routes being passed to host-based TCP/IP stacks.

  With the fix for this bug, for each CLAW statement, the CIP microcode will retain the static 64 buffers that are 4096 in size. However, each 4096 byte buffer can be segmented into either 4 smaller buffers of 1024 bytes each or eight smaller buffers of 512 bytes each. When buffers are allocated in this fashion, the 4096 byte buffer is reassembled after all of the smaller chunks are freed. [CSCdj03799]

- During the recovery of certain ESCON link errors, the CIP might crash with a FATAL-ERROR, after the ESCON adapter reports a device level error at a time when there is no active device. When this problem occurs, the FATAL-ERROR is preceeded by the following error message:

  ```
  CCA-0-DEV_ERR2: Device error but no active defined device
  ```

  The only work-around, short of replacing the microcode with the microcode that has this problem fixed, is to determine and resolve the reason for the ESCON link error. [CSCdj21031]

Channel Interface Processor, Second-Generation (CIP2) Microcode Revision Summary

CIP2 Microcode Version 20.8

CIP2 Microcode Version 20.8 was released on June 8, 1996.

CIP2 Microcode Version 20.9

Modification

CIP2 Microcode Version 20.9 fixes the following bugs:

- If the router switches a packet to the CIP2 for the virtual port adapter (interface channel *slot*/2) using the wrong virtual circuit number, the CIP2 crashes with the following error message: [CSCdi61532]

  ```
  %CIP5-3-MSG: %CONFIG-3-WRONGINT: VCN 0(0000) not for port adapter 2
  ```

- If the CIP2 gets a packet greater than 4K from a Route Processor (RP) or Route Switch Processor (RSP), the CIP2 might stop functioning properly and might eventually crash with fatal errors. If this problem occurs, you will see the following message:

  ```
  CLAW-6-TOOBIG: 4352 byte IP datagram exceeds CLAW MTU for device
  ```

  To work around this problem, reload the router. [CSCdi64874]

- On a CIP2 with CSNA and TCP Offload both in use, TCP sessions might randomly quit with the remote client appearing to have requested disconnect. [CSCdi63044]
- Sometimes a mainframe cannot send packets to a CIP. [CSCdi66108]
- When a CIP2 reads 7 MB/sec from MEMD in an RSP platform, occasionally the CIP2 detects a bad transfer and produces messages such as: [CSCdi54732]

  ```
  *Apr 15 14:21:58: %CIP10-0-MSG: %DMA-0-BADFIFO: FIFO failure detected during transfer (40
  0001)
  ```

CIP2 Microcode Version 20.10

Modification

CIP2 Microcode Version 20.10 fixes the following bugs:

- Parity and interrupts functions are disabled while flushing on an hw5 CIP. [CSCdi55192]
- Each configured device (pair) does not have the minimum requirement of 16 transmit (tx) buffers. [CSCdi54042]
- Issuing CIP console commands could cause DBUS errors. [CSCdi67549]
- Inadequate diagnostics are available for the ESCON port adapter. [CSCdi71938]
- ESCON link-level errors might cause the CIP to hang. [CSCdi69548]
- There is no ability to put individual subchannels into a command retry. [CSCdi45356]

CIP2 Microcode Version 20.11

Modification

CIP2 Microcode Version 20.11 fixes the following bugs:

- Multiple resets could cause loss of transmit buffers. [CSCdi72853]
- The exe2sim function does not support COFF format. [CSCdi72894]

- A CIP Fatal Error 35 occurs after SHUTDOWN is issued on the channel interface. [CSCdi74491]
- A crash might occur at <putc+b8> lhu $v0,8($zero). [CSCdi74911]
- The CIP interface Buffer Counter becomes corrupted when RXCURR is greater than RXHIGH. [CSCdi75138]
- During request in path, inbound-to-host performance drops. [CSCdi76020]
- ADAPTER-0-DIAGDATA module 1221 error FE14 occurs when using the new ESCON diagnostics. [CSCdi84660]

CIP2 Microcode Version 20.12

Modification

CIP2 Microcode Version 20.12 fixes the following bugs:

- Previously, the CIP microcode allocated 64 buffers for each CLAW device, and the number of buffers per CLAW would increased if there was a sudden burst of traffic and a large number of routes being passed to host-based TCP/IP stacks.

  With the fix for this bug, for each CLAW statement, the CIP microcode will retain the static 64 buffers that are 4096 in size. However, each 4096 byte buffer can be segmented into either 4 smaller buffers of 1024 bytes each or eight smaller buffers of 512 bytes each. When buffers are allocated in this fashion, the 4096 byte buffer is reassembled after all of the smaller chunks are freed. [CSCdj03799]

- During the recovery of certain ESCON link errors, the CIP might crash with a FATAL-ERROR, after the ESCON adapter reports a device level error at a time when there is no active device. When this problem occurs, the FATAL-ERROR is preceeded by the following error message:

  ```
  CCA-0-DEV_ERR2: Device error but no active defined device
  ```

  The only work-around, short of replacing the microcode with the microcode that has this problem fixed, is to determine and resolve the reason for the ESCON link error. [CSCdj21031]

Ethernet Interface Processor (EIP) Microcode Revision Summary

EIP Microcode Version 20.1

Modification

EIP Microcode Version 20.1 fixes the following bug:

- Use of Hot Standby Router Protocol (HSRP) in heavy traffic situations can cause "RSP-3-ERROR" reports and cBus resets. [CSCdi46654]

EIP Microcode Version 20.2

Modification

EIP Microcode Version 20.2 fixes the following bug:

- Version 1.6 Rev C0 EIP cards might cause cache parity errors on all Cisco 7500 series and RSP7000 systems. The cache parity errors can cause system reloads. [CSCdi52082]

EIP Microcode Version 20.3

Modification

EIP Microcode Version 20.3 fixes the following bug:

- A router might reload by reserved (SegV) exception, including XBUFHDR errors, INVRTN errors, and GETBUF errors. A stack trace shows “RSP-3-XBUFHDR: corrupt bufhdr,” “SYS-3-DMPMEM,” and “reserved exception.” [CSCdi75404]

Fast Ethernet Interface Processor (FEIP) Microcode Revision Summary

FEIP Microcode Version 20.1

Modification

FEIP Version 20.1 fixes the following bug:

- A hardware manufacturing change affected margin timing. [CSCdi40448]

FEIP Microcode Version 20.2

Modification

FEIP Microcode Version 20.2 fixes the following bug:

- Serial interfaces that are down but not administratively disabled might periodically reset and display the error “8010 - disable fsip_reset.” [CSCdi49431]

FEIP Microcode Version 20.3

Modification

FEIP Microcode Version 20.3 fixes the following bug:

- The FX port adapter is not supported. [CSCdi48337]

FEIP Microcode Version 20.4

Modification

FEIP Microcode Version 20.4 fixes the following bug:

- FEIP MII interface fails to reset if there is OIR of another card in the router. [CSCdi82350]
- You are unable to ping/Telnet HSRP virtual address on FastEthernet. [CSCdi92485]

Fast Serial Interface Processor (FSIP) Microcode Revision Summary

FSIP Microcode Version 20.2

Modification

FSIP Version 20.2 fixes the following bugs:

- When using the X.21 protocol, DTE devices erroneously send data when Control is OFF. [CSCdi45512]
- Transmitter-delay does not work on FSIP DCE interfaces. [CSCdi58196]
- Using FSIP might cause a ciscoBus restart. [CSCdi58194]

FSIP Microcode Version 20.3

Modification

FSIP Version 20.3 fixes the following bugs:

- 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 DCE leads during a cutover from a Cisco 2501 serial port. [CSCdi64735]

FSIP Microcode Version 20.4

Modifications

FSIP Microcode Version 20.4 fixes the following bugs:

- 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 bought 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 00000:  0001 FFFC
FSIP Mem 00004:  0000 01C6
FSIP Mem 00008:  0000 049A
FSIP Mem 0000C:  0000 049A
FSIP Mem 00010:  0000 049A
FSIP Mem 00014:  0000 049A
FSIP Mem 00018:  0000 049A
FSIP Mem 0001C:  0000 049A
FSIP Mem 00020:  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.

```
ramki_7500(config)#mic rel
```

  [CSCdi57573]

- 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 bugs:

- A serial interface stays line down when the remote side toggles. [CSCdi57573]
- The FSIP gets lost from the chassis if you perform an Online Insertion and Removal (OIR) of a VIP2. [CSCdi73130]

MultiChannel Interface Processor (MIP) Microcode Revision Summary

MIP Microcode Version 20.3

Modification

MIP Microcode Version 20.3 fixes the following bug:

- MIP drops packets in bursts. [CSCdi46383]

Token Ring Interface Processor (TRIP) Microcode Revision Summary

TRIP Microcode Version 20.1

Modifications

TRIP Microcode Version 20.1 fixes the following problems:

- The SpyGlass command queue overflows with a “ctrucheck” symptom.
- 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” (signifying output stuck).
- The prototype Access Control byte is invalid (bit 0x10 set).

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, user 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 up to date 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.

This document is to be used in conjunction with the *Router Products Configuration Guide*, *Router Products Command Reference*, and *Protocol Translation Configuration Guide and Command Reference* publications.

978R