Doc. No. 78-1475-20

Router Products Release Notes for Cisco IOS Release 10.2

December 16, 1996

These release notes describe the features, modifications, and caveats for Cisco Internetwork Operating System (Cisco IOS) Release 10.2, up to and including Release 10.2(15). They include all routing and protocol translation features.

Introduction

These release notes discuss the following topics:

Documentation

For printed documentation of Cisco IOS Release 10.2 router software features, refer to the Release 10.2 *Router Products Configuration Guide Addendum* and *Router Products Command Reference Addendum*. These addenda 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 six main parts that match the parts in the Release 10 *Router Products Configuration Guide* and *Router Products Command Reference*.

Electronic documentation of Release 10.2 router software features is available on the Documentation CD-ROM. Refer to the Release 10.2 *Router Products Configuration Guide* and *Router Products Command Reference* publications, which are located in the Cisco IOS Release 10.2 database. (Note that the two addenda are not available on CD, because the information in them has been incorporated into the electronic documents.)

For printed protocol translation documentation, refer to the Release 10 *Protocol Translation Configuration Guide and Command Reference* publication. On CD, refer to the Cisco IOS Release 10.2 *Protocol Translation Configuration Guide and Command Reference* publication in the Cisco IOS Release 10.2 database.

You can also access Cisco technical documentation on the World Wide Web (WWW) URL http://www.cisco.com or http://www-china.cisco.com or http://www-europe.cisco.com.

Platform Support

Release 10.2 is supported on the following platforms:

- Cisco 7000 series
- Cisco 4000 series (Cisco 4000, Cisco 4000-M, Cisco 4500, Cisco 4500-M, Cisco 4700)

- Cisco 3000 series (except the Cisco 3202)
- Cisco 2500 series (Cisco 2501 through Cisco 2516)
- Cisco 1000 series LAN Extender
- AccessPro PC card
- AGS and AGS+ (with a CSC/4 processor board)
- MGS (with a CSC/4 processor board)
- CGS (with a CSC/4 processor board)

Table 1 and Table 2 summarize the features supported on each platform.

Table 1 Interfaces Supported by Router Platforms

Interface	Cisco 7000 Series	Cisco 4000 Series	Cisco 3000 Series[1]	Cisco 2500 Series	Cisco 1000 LAN Extender	AccessPro PC Card	AGS+	MGS	CGS
Ethernet (AUI)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Ethernet (10BaseT)	No	Yes	No	Yes	Yes	Yes	Yes	No	No
4-Mbps Token Ring	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
16-Mbps Token Ring	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
FDDI DAS	Yes	Yes	No	No	No	No	Yes	No	No
FDDI SAS	Yes	Yes	No	No	No	No	Yes	No	No
FDDI multimode	Yes	Yes (DAS/SAS)	No	No	No	No	Yes	No	No
FDDI single-mode	Yes	Yes (DAS)	No	No	No	No	Yes	No	No
ATM	Yes	No	No	No	No	No	No	No	No
ESCON and bus-and-tag	Yes	No	No	No	No	No	No	No	No
Second-generation Channel Interface Processor (CIP2)[2]	Yes	No	No	No	No	No	No	No	No
Channelized T1	Yes	No	No	No	No	No	No	No	No

[1] Except the Cisco 3202.

[2] 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

Feature	Cisco 7000 Series	Cisco 4000 Series	Cisco 3000 Series[1]	Cisco 2500 Series	Cisco 1000 LAN Extender	AccessPro PC Card	AGS+	MGS	CGS
Data Rates									
48/56/64 kbps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
1.544/2.048 Mbps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Feature	Cisco 7000 Series	Cisco 4000 Series	Cisco 3000 Series[1]	Cisco 2500 Series	Cisco 1000 LAN Extender	AccessPro PC Card	AGS+	MGS	CGS
34/45/52 Mbps	Yes	No	No	No	No	No	Yes	No	No
Interfaces									
EIA/TIA-232	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
X.21	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
V.35	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EIA/TIA-449	Yes	Yes	Yes	Yes	No	No	Yes	No	No
EIA/TIA-530	Yes	Yes	Yes	Yes	No	Yes	No	No	No
EIA/TIA-613 (HSSI)	Yes	No	No	No	No	Yes	Yes	No	No
ISDN BRI	No	Yes	Yes	Yes	No	Yes	No	No	No
ISDN PRI	Yes	No	No	No	No	No	No	No	No
G.703	Yes	Yes	No	No	No	Yes	Yes	No	No

[1] Except the Cisco 3202.

Cisco IOS Packaging

Cisco IOS software is available in different packages depending upon the platform. Table 3 lists the feature sets for the Cisco 7000 series, AGS+, MGS, and CGS. Table 4 lists the feature sets for the Cisco 2500 series and AccessPro PC card. Table 5 lists the features sets for the Cisco 4000 series, which includes the Cisco 4000, Cisco 4000-M, Cisco 4500, Cisco 4500-M, and Cisco 4700. Table 6 lists the feature set for the Cisco 3000 series.

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

	Feature Set		
Feature	**Enterprise**	**Enterprise/CIP2**	**SRS**
SNMP	Yes	Yes	Yes
Asynchronous support (SLIP)	Yes	Yes	—
Frame Relay	Yes	Yes	—
SMDS	Yes	Yes	—
X.25	Yes	Yes	—
HDLC	Yes	Yes	—
ISDN	Yes	Yes	—
PPP	Yes	Yes	—
IP	Yes	Yes	Yes (host only)
RIP	Yes	Yes	—
IGRP	Yes	Yes	—
Enhanced IGRP	Yes	Yes	—
OSPF	Yes	Yes	—
EGP	Yes	Yes	—
BGP	Yes	Yes	—

	Feature Set		
Feature	Enterprise	Enterprise/CIP2	SRS
PIM	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	—
IPXWAN	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	—
SDLC	Yes	Yes	—
SDLLC	Yes	Yes	—
STUN	Yes	Yes	—
TG/COS	Yes	Yes	—
QLLC	Yes	Yes	—
AutoInstall	Yes	Yes	—
Telnet	Yes	Yes	—

Table 4 Cisco 2500 Series and AccessPro PC 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	—	—
IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
Enhanced IGRP	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
ES-IS	—	—	—	—	—	—	Yes	—	—
IS-IS	—	—	—	—	—	—	Yes	—	—
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—
Bridging (transparent and translational)	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
IPXWAN	—	—	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	—	—
Source-route bridging	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote source-route bridging	—	Yes	—	Yes	—	Yes	Yes	—	—

	Feature Set								
Feature	IP	IP/IBM Base	IP/IPX	IP/IPX/ IBM Base	Desktop	Desktop/ IBM Base	Enterprise	CFRAD	ISDN
Multiring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	—
SDLC	—	—	—	—	—	—	Yes	Yes	—
SDLLC	—	—	—	—	—	—	Yes	Yes	—
STUN	—	—	—	—	—	—	Yes	Yes	—
TG/COS	—	—	—	—	—	—	Yes	—	—
QLLC	—	—	—	—	—	—	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	—

Table 5 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	—	—	—	—	Yes	Yes	Yes
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
ES-IS	—	—	—	—	—	—	Yes
IS-IS	—	—	—	—	—	—	Yes

	Feature Set						
Feature	**IP**	**IP/IBM Base**	**IP/IPX**	**IP/IPX/ IBM Base**	**Desktop**	**Desktop/ IBM Base**	**Enterprise**
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bridging (transparent and translational)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN extension host	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX	—	—	Yes	Yes	Yes	Yes	Yes
IPXWAN	—	—	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	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote source-route-bridging	—	Yes	—	Yes	—	Yes	Yes
Multiring	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SDLC	—	—	—	—	—	—	Yes
SDLLC	—	—	—	—	—	—	Yes
STUN	—	—	—	—	—	—	Yes
TG/COS	—	—	—	—	—	—	Yes
QLLC	—	—	—	—	—	—	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

Table 6 Cisco 3000 Series Software

	Feature Set
Feature	**Enterprise**
SNMP	Yes
Asynchronous support (SLIP)	Yes
ARA	Yes
Frame Relay (RFC 1490)	Yes

	Feature Set
Feature	Enterprise
SMDS	Yes
X.25	Yes
HDLC	Yes
ISDN	Yes
PPP	Yes
IP	Yes
RIP	Yes
IGRP	Yes
Enhanced IGRP	Yes
OSPF	Yes
EGP	Yes
BGP	Yes
PIM	Yes
ES-IS	Yes
IS-IS	Yes
Snapshot routing	Yes
NTP	Yes
Transparent bridging	Yes
Translational bridging	Yes
LAN extension host	Yes
IPX	Yes
IPXWAN	Yes
AppleTalk Versions 1 and 2	Yes
AURP	Yes
DECnet IV, V	Yes
Apollo Domain	Yes
Banyan VINES	Yes
ISO CLNS	Yes
XNS	Yes
Source-route bridging	Yes
Remote source-route bridging	Yes
SDLLC	Yes
STUN	Yes
TG/COS	Yes
QLLC	Yes
AutoInstall	Yes
Telnet	Yes
Protocol translation	Yes

	Feature Set
Feature	Enterprise
TN3270	Yes
LAT	Yes
XRemote	Yes

Boot ROM Requirements

Boot ROM versions and system images are independent of each other. Table 7 lists the default boot ROM levels that ship with Cisco platforms. These levels contain the latest features and support all current hardware and software features. If you require newer boot ROMs, refer to Table 8, which lists the available upgrades.

Table 7 Default Boot ROM Levels

Platform	Boot ROM Level
AccessPro PC Card	10.2(5)
Cisco 2501 through Cisco 2516	10.2(8a)
Cisco 3000 series	9.14(6)
Cisco 4000 and Cisco 4000-M	10.2(13)
Cisco 4500 and Cisco 4500-M	10.3(7)
Cisco 4700	10.3(10)

Table 8 Available Boot ROM Upgrades

Platform	Order Number	Current Level
Cisco 2500 series	BOOT-2500=	10.2(8a)
Cisco 2509 through Cisco 2512	BOOT-2509/12=	9.14(9b)
Cisco 3000 series	BOOT-3000=	9.14(9b)
Cisco 4000 series	BOOT-4000=	10.2(11a)[1]

[1] 10.2(11a) is an 8 Mb boot ROM that requires the two bottom pins on J8 to be jumpered.

Note For additional information about booting Cisco 4000 routers, see the section “Booting Cisco 4000 Routers” on page 25.

Memory Requirements

With Release 10.2, the Cisco software image size exceeds 4 MB and when compressed exceeds 2 MB. Also, some 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 10.2 features, they must have CSC/4 processor cards and 9.1(8)-level (or higher) system ROMs for booting from a network server.

For the Cisco routers to take advantage of the Release 10.2 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 10.2 Memory Requirements

Router	Required Code Memory	Required Main Memory	Release 10.2 Runs from
Cisco 2500 Series			
IP Set	4 MB Flash	2 MB RAM	Flash
IP/IBM Base Set	4 MB Flash	4 MB RAM	Flash
IP/IPX Set	4 MB Flash	4 MB RAM	Flash
IP/IPX/IBM Base Set	4 MB Flash	4 MB RAM	Flash
Desktop Set	4 MB Flash	4 MB RAM	Flash
Desktop/IBM Base Set	4 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 or 16 MB RAM	RAM
Cisco 3104, Cisco 3204	8 MB Flash	4 MB RAM	Flash
	4 MB Flash	8 or 16 MB RAM	RAM
Cisco 4000			
IP Set	4 MB Flash	16 MB RAM	RAM
IP/IBM Base Set	4 MB Flash	16 MB RAM	RAM
IP/IPX Set	4 MB Flash	16 MB RAM	RAM
IP/IPX/IBM Base Set	4 MB Flash	16 MB RAM	RAM
Desktop Set	4 MB Flash	16 MB RAM	RAM
Desktop/IBM Base 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 Base Set	4 MB Flash	8 MB RAM	RAM
IP/IPX Set	4 MB Flash	8 MB RAM	RAM
IP/IPX/IBM Base Set	4 MB Flash	8 MB RAM	RAM
Desktop Set	4 MB Flash	8 MB RAM	RAM
Desktop/IBM Base Set	4 MB Flash	8 MB RAM	RAM
Enterprise Set	4 MB Flash	8 MB RAM	RAM

Router	Required Code Memory	Required Main Memory	Release 10.2 Runs from
Cisco 4500			
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	32 MB RAM	RAM
Cisco 4500-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[1]	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	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
SRS 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
SRS Set	8 MB Flash	16 MB RAM	RAM
AGS+, MGS, CGS	—	16 MB RAM	RAM

[1] Sixteen MB DRAM is required if you have a CT1, CE1, or MBRI card installed.

Microcode Software

Table 10 and Table 11 list the current 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 10 Current 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[1]
CSC-R16M	3.2[1]
CSC-1R/CSC-2R	1.6[1]
CSC-ENVM	2.2
CSC-CCTL2	11.0 [2]
CSC-C2MEC	10.0
CSC-C2HSCI	10.0
CSC-C2FCI	10.0
CSC-C2FCIT	10.0
CSC-C2CTR	10.0

[1] Minimum level needed to run multiple IPX encapsulations and VINES fast switching.

[2] Minimum level needed to run IPX autonomous switching, multiple IPX encapsulations, autonomous transparent bridging, VINES fast switching, and IP autonomous switching over Frame Relay or PPP.

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[1]
CSC-R16M	3.2[1]
CSC-1R/CSC-2R	1.2[1]
CSC-ENVM	2.2
CSC-CCTL	3.0[1]
CSC-MEC (5.0)	1.1
CSC-MEC (5.1)	2.2
CSC-HSCI	1.0
CSC-FCI	2.0

[1] Minimum level needed to run multiple IPX encapsulations and VINES fast switching.

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)	10.13	10.2
CIP (Channel Interface Processor)[1]	20.8	10.0
CIP2 (second-generation Channel Interface Processor)[1.]	20.8	20.8
EIP (Ethernet Interface Processor)	10.1	10.0
FIP (FDDI Interface Processor)	10.2	10.0
FSIP (Fast Serial Interface Processor)[2]	10.13	10.2
HIP (HSSI Interface Processor)	10.2	10.0
MIP (MultiChannel Interface Processor)	10.4	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)	10.3	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-.”

[2] Release 10.2 does not support the pre-FSIP.

New Features in Release 10.2(13)

This section describes new features and enhancements in Release 10.2(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 boot flash, which is software upgradable (allowing upgrades to the boot microcode without physical replacement of parts)

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

- Router Processor (RP) and Switch Processor (SP) (or Silicon Switch Processor [SSP]) combination
- Cisco 7000 series Route 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 Features in Release 10.2(8)

The following new features have been added in Release 10.2(8):

- Cisco 4700 support. This new member of 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 compatible with the existing network processor modules (NPMs) for the Cisco 4000 series (with the exception of the NP-1E). 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.

- Multivendor Flash single in-line memory module (SIMM) support. Beginning with Release 10.2(8), you can use Flash 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 13 (for Cisco 2500 series and Cisco 4500 platforms) or Table 14 (for the AccessPro PC card and Cisco 2517 router).

  Multivendor Flash memory 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 and Cisco 4000 series platforms do not support the multivendor Flash memory feature.

  Cisco 2500 series routers (non-AccessPro) and the Cisco 4500 router have two slots for Flash SIMMs. Table 13 provides the supported SIMM configurations.

Table 13 Cisco 2500 Series and Cisco 4500 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 10.2(8).

SIMM Size	Vendor	Flash Bank	Considerations
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 10.2(8).
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
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 has one slot for a Flash SIMM. Table 14 provides the supported SIMM configurations.

Table 14 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 Feature in Release 10.2(5)

The following new feature has been added in Release 10.2(5):

- Dual Flash bank Management Information Base (MIB).

Note The first few maintenance releases of each new Cisco IOS software release deliver additional new features. Early maintenance releases of Release 10.2 include several major new features. You should consider the importance they place on maximizing product capability versus maximizing operational stability as you plan to deploy a new release. You should always try an early release of software in a test network before deploying it in a production network.

New Features in Release 10.2(4)

The following new features have been added in Release 10.2(4):

- Source Route Switch—The Cisco 7000 series Source Route Switch 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 four Source Route Switch Token Ring Interface Processors (SRS-TRIPs) that are running the SRS feature set.

  Making hardware connections to SRS-TRIP interface processors is identical to making hardware connections to TRIP interfaces 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 is not interchangeable with the TRIP.

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

- Support for the Cisco 2516—The Cisco 2516 is a router with hub functionality. It has 1 Ethernet interface (14 ports), 2 serial interfaces, and 1 ISDN BRI interface.
- Support for the Cisco Access Server 5100—The Cisco Access Server 5100 is a data communications platform that combines in one chassis the functions of an access server, a router, and analog and digital modems.

New Features in Release 10.2(2)

The following new features have been added in Release 10.2(2):

- Snapshot routing—Snapshot routing, which is available on serial lines, is a method whereby the router learns remote routes dynamically and then keeps the routes available for a period of time while regular routing updates are not being exchanged.
- Dual Flash bank—Dual Flash bank is a software feature that allows you to partition Flash memory into two separate, logical devices so that each logical device has its own file system. This feature is available on the AccessPro PC card, Cisco 2500 series, Cisco 3000 series, and Cisco 4000 series systems.
- Support for the Cisco 2505 and Cisco 2507 routers—These routers have hub functionality for Ethernet interfaces. The hub is a multiport repeater.
- Support for the Cisco 2513, Cisco 2415, and Cisco 2515 routers—These routers support dual LANs in a single chassis.
- Support for the bus-and-tag Parallel Channel Adapter (PCA) in a Cisco 7000 series router.
- AccessPro PC Card for IBM-compatible PC—The AccessPro PC card is a full-featured multiprotocol router card that plugs into an IBM-compatible personal computer (PC) equipped with an Industry Standard Architecture (ISA) bus. The PC accommodates one AccessPro PC card. The AccessPro PC card consists of an ISA-bus card with an asynchronous serial auxiliary port, a synchronous serial WAN port, and an Ethernet 10BaseT port for a LAN connection.
- Cisco 4500 and AGS+ support for LAN extension—The Cisco 4500 and AGS+ routers can now be LAN Extender hosts.
- IP multicast MIB.

- Qualified Logical Link Control (QLLC) MIB.
- Additional software feature sets have been added. These are described in the section “Cisco IOS Packaging” earlier in this document.

Software Features

This section describes new features and enhancements in the initial Release 10.2 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 Release 10.2.

IP Features

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

- IP multicast—This IP protocol supports applications being developed for communicating either between one sender and multiple receivers or between multiple senders and multiple receivers. Cisco’s implementation includes Protocol Independent Multicast (PIM) and the Internet Group Management Protocol (IGMP). PIM allows network administrators to add IP multicast functionality to their existing networks regardless of what routing protocol they are running. PIM works with IGRP, Enhanced IGRP, OSPF, Integrated IS-IS, RIP, and BGP. PIM has two modes: dense mode and sparse mode.
- Local-area mobility—Local-area mobility provides the ability to relocate IP hosts within a limited area without reassigning host IP addresses and without changes to the host software. Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces. It is useful in environments where workers use portable computers and roam to different locations within the corporate network.

Transparent Bridging Features

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

- Deterministic load distribution—This new method distributes bridged traffic more effectively across parallel circuits. It increases bandwidth by using multiple, parallel lines between the same two routers/bridges, an approach Cisco calls “circuit groups.” Traffic is distributed on the parallel lines within the circuit group.

Desktop Protocol Features

This section describes the desktop protocol features that are new in the initial release of Release 10.2.

AppleTalk Features

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

- AppleTalk Update-based Routing Protocol (AURP)—AURP is Apple Computer's new approach to AppleTalk routing. Cisco's implementation of AURP is fully compliant with the mandatory portions of the AURP specification, including the tunneling of AppleTalk packets inside of IP. Macintosh hosts do not implement AURP. Thus, Cisco routers still use RTMP to communicate with hosts and translate (or redistribute) RTMP routing information to and from AURP.
- Fast-switching enhancements—Fast switching of AppleTalk has now been implemented for the following platforms and interfaces:
    - FDDI interface on the Cisco 4000 series
    - Token Ring interfaces on all Cisco 2000, Cisco 3000, and Cisco 4000 series platforms
    - CTR and TRIP Token Ring interfaces on the AGS+ and Cisco 7000 series platforms, respectively
    - Frame Relay and PPP encapsulations on all serial interfaces on all platforms

  With these enhancements, AppleTalk fast switching is now supported on all LAN interfaces on all platforms except for the SBE and STR Token Ring cards on the AGS. Over WANs, Frame Relay, HDLC, and PPP encapsulations are fast-switched on all platforms.
- AppleTalk MIB—A MIB for AppleTalk information has been implemented that complies with RFC 1243. Support is included for the following AppleTalk protocols: AppleTalk Resolution Protocol (ARP), AppleTalk Port Group, AppleTalk Datagram Delivery Protocol (DDP), AppleTalk Routing Table Maintenance Protocol (RTMP), AppleTalk Zone Information Protocol (ZIP), AppleTalk Name Binding Protocol (NBP), and AppleTalk Echo Group.
- ZIP reply filters—ZIP reply filters provide a second means for filtering zone information in an AppleTalk network. These filters allow zone information to be hidden from downstream routers, as configured by the network manager. When a neighbor router queries a router with a ZIP reply filter for the zone list of an advertised network, zones that are denied in the filter are not included in the ZIP reply packet.

Banyan VINES Features

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

- Fast-switching enhancements—Fast switching of Banyan VINES has now been implemented for the PPP, Frame Relay, SMDS, and ATM encapsulations. For ATM, the AAL3/4, AAL5 NLPID, AAL5 LLC/SNAP, and AAL MUX are supported. With these enhancements, VINES fast switching is now supported on all LAN interfaces on all platforms, and for WAN interconnection, on all platforms when HDLC, PPP, Frame Relay, SMDS, or ATM encapsulation is used.
- Banyan VINES-compliant traceroute—A VINES-compliant and interoperable traceroute facility has now been implemented. In addition to VINES network layer addresses, the MAC address of each interface traversed is also recorded.

Novell IPX Features

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

- Fast-switching enhancements—Fast switching of Novell IPX has now been implemented for the Frame Relay and ATM encapsulations. For ATM, the AAL3/4, AAL5 NLPID, AAL5 LLC/SNAP, and AAL MUX are all supported. With these enhancements, IPX fast switching is now supported on all LAN interfaces on all platforms, and for WAN interconnection, on all platforms when HDLC, PPP, Frame Relay, or ATM encapsulation is used.
- IPX-compliant IPX ping—The standard IPX ping function, which was recently specified by Novell, is equivalent to the Cisco-specific ping implemented in previous software releases.
- IPX MIB—A MIB for Novell IPX information has been implemented that is consistent with the variables defined by Novell in their NLSP specification. The MIB supports the Novell IPX, RIP, and SAP MIB portions of the NLSP specification. However, it does not implement the NLSP MIB.

Wide-Area Networking Features

This section describes the wide-area networking features that are new in the initial release of Release 10.2.

ATM Features

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

- AAL 3/4 support—AAL 3/4 is one of the two common ATM Adaptation Layers (AALs) used for bursty data. It is required to support SMDS over ATM. The software already supports AAL 5, the second AAL for bursty data.
- RFC 1490 support—RFC 1490, which is specified for Frame Relay, defines an encapsulation using a Network Layer Protocol Identifier (NLPID) that is used to indicate a protocol type for each packet transferred. RFC 1490 is currently supported over serial interfaces for both Frame Relay and ATM DXI encapsulations.

Frame Relay Features

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

- DE bit support—The Discard Eligibility (DE) bit indicates loss priority. The DE bit of a packet is set by means of an access list. When congestion occurs, packets with the DE bit set are discarded in preference to packets whose DE bit is not set.
- TCP/IP header compression—In RFC 1144, Van Jacobson defines a TCP/IP header compression algorithm that uses the TCP/IP header of a previous packet to predict the TCP/IP header of a subsequent packet. With this algorithm, it is possible to compress 40 octets down to 5 octets. This algorithm is currently supported on serial lines and X.25 networks. With Release 10.2, Frame Relay support is added and header compression can be enabled on a per-DLCI basis.
- Broadcast queue—The Frame Relay broadcast queue is a feature that identifies all broadcast traffic such as routing and SAP updates and places this traffic into a special queue that is managed independently of the normal interface queue. This special queue has its own buffers and a configurable service rate.
- IPXWAN support—IPXWAN is not part of the RFC 1490 specification, but it is necessary for multivendor interoperability for IPX networks. IPXWAN is a link startup and negotiation protocol specified by Novell in RFC 1362.

ISDN/DDR Features

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

- ISDN MBRI—ISDN signaling software is available for the Multiport Basic Rate Interface (MBRI) network processor modules for use with Cisco 4000 series and Cisco 4500 routers. These network processor modules support either 4 or 8 Basic Rate Interfaces, allowing a Cisco router to act as a hub for up to 32 separate remote locations. The complete set of IOS DDR software features is supported, including dial backup, bandwidth on demand, and supplementary bandwidth.
- ISDN PRI—Release 10.2 provides ISDN PRI signaling, which is required to use the Cisco MultiChannel Interface Processor (MIP) card as an ISDN PRI. This card can support either one or two interfaces providing up to 46 ISDN B channels. Initial availability of ISDN PRI will support 4ESS, 5ESS, and DMS-100 signaling for North America.
- Dial-up X.25 using ISDN—Dial-up X.25 can work either via the PSTN, SW56, or ISDN (B channel). The router dials up the network in much the same manner as for dial backup and dial-on-demand routing (DDR). Once the connection to the network is established, the X.25 layers are activated and X.25 calls are placed.
- DDR dialer hold queue—Dial-up services take a finite amount of time to establish a connection to a remote router. This time can vary from a couple of seconds for ISDN up to 30 seconds for an analog modem. During this time, packets destined for the remote router can be discarded because no connection exists. The creation of a dialer hold queue allows packets that would normally be dropped to be held until a connection is established.
- DTR dialing—With Release 10.2, Cisco routers support connections over serial lines connected to non-V.25bis modems using DTR signaling. Cisco already provides support for V.25bis dialing as part of the overall DDR software package.

SMDS Features

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

- Virtual interfaces—This new configuration capability allows each destination E.164 address or a group of addresses to be considered for connection to a separate port (subinterface) on the router. In turn, each virtual interface can be configured with its own addresses, routing protocols, access lists, and routing metrics.
- SMDS over ATM—SMDS is defined by a three-level stack with a Level 3 PDU that contains the variable-length packet and E.164 source and destination addressing. The Level 2 PDUs are defined according to IEEE 802.6 and are similar to ATM cells. Level 2 has been replaced with an ATM Level 2 using AAL 3/4, as defined by ITU-T I.364. Cisco's support of SMDS over ATM complies with I.364 and eliminates the need for a separate CSU/DSU. The stack runs on the AIP. The access class facility normally provided by SMDS is supported by the traffic-shaping capability of the AIP.

X.25 and LAPB Features

The following features have been added to Cisco's X.25 software:

- RFC 1356 support—RFC 1356 supersedes RFC 877, which specified how both IP and OSI could be transported across X.25. RFC 1356 extends RFC 877 in two significant ways:
  - — Multiprotocol interoperability: All protocols are carried in a defined way.
  - — Single virtual circuits: Many protocols can be carried across a single virtual circuit. LLC/SNAP encapsulation of frames is used.

- X.25 payload compression—Payload compression is an extension of link compression in that only the payload of the WAN media is compressed. In the case of X.25, packets can be correctly switched because the headers are not compressed. Cisco’s payload compression uses the STAC algorithm, which is state-of-the-art in both compression ratios and processor efficiency. Compression ratios are data-dependent; they can be greater than 4:1, but are typically around 2:1.
- LAPB enhancements—The following significant LAPB enhancements are included in this release:
    - Modulo 128: This allows a larger window size to be configured on a link.
    - T4 timer: This allows a Receive Ready (RR) to be used as a keepalive to allow rapid link failure detection without relying on higher-layer routing protocols.
    - Hardware outage timer: This allows brief hardware outages to occur without requiring that the protocol be reset.
- IPXWAN on X.25—IPXWAN is not part of the RFC 1356 specification, but it is necessary for multivendor interoperability for IPX networks. IPXWAN is a link startup and negotiation protocol specified by Novell in RFC 1362.
- **encapsulation lapb** command—This command replaces several commands as follows:
    - Instead of **encapsulation lapb-dce**, use the **encapsulation lapb dce** command.
    - Instead of **encapsulation multi-lapb**, use the **encapsulation lapb multi** command.
    - Instead of **encapsulation multi-lapb-dce**, use the **encapsulation lapb dce multi** command.

IBM Functionality Features

This section describes the IBM features that are new in the initial release of Release 10.2:

- Automatic spanning tree—Cisco routers, when acting as source-route bridges, now participate in the spanning-tree protocol to dynamically determine which bridges should be SRB capable.
- Expanded SDLC support: broadcast services—Cisco routers support a feature known as virtual multidrop, which allows multiple SDLC lines to appear as a single virtual multidrop line to a FEP. Cisco is enhancing this feature by adding broadcast services. With SDLC broadcast services, if a Cisco router receives an all-stations broadcast on a virtual multidrop line, the router propagates the broadcast to each SDLC line that is a member of the virtual multidrop line.
- Two-way simultaneous SDLC transmission—This feature allows routers to sequentially poll multiple devices on a multidrop line while concurrently receiving data from another device on the same line.
- QLLC support—Qualified Logical Link Control (QLLC) is the link protocol used by SNA devices when connecting over an X.25 network. This feature provides conversion between QLLC/X.25 and either SDLC or LAN (LLC2). Remote SNA devices can connect to a Cisco router using QLLC/X.25, and the Cisco router converts the frames to Token Ring and forwards them to the appropriate FEP (or AS/400). Cisco’s QLLC support can also be used to convert remote SDLC-attached, Token Ring-attached, or Ethernet-attached devices to QLLC, thus allowing network consolidation of traditional SNA/X.25 networks and LAN internetworks. Cisco's QLLC support applies to remote PU 2.0 devices connected over either permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). Remote Token Ring-attached devices that are converted to local QLLC also support PU_T2.1 devices.

Network Management Features

This section describes the network management features that are new in the initial release of Release 10.2.

- SNMP Version 2—Release 10.2 supports the Simple Network Management Protocol (SNMP) Version 2. Cisco IOS software can communicate with both SNMP Version 1 and SNMP Version 2 network management stations. SNMP is an application-layer protocol designed to facilitate the exchange of management information between network devices. Most of the changes introduced in Version 2 increase SNMP's security capabilities. SNMP Version 2 uses the Message Digest 5 (MD5) algorithm to provide for data integrity and authentication capabilities.
- Access list violation logging—For the IP protocol, access list violation logging tracks source-destination pairs of IP addresses that are generating IP access list violations.

General Features

This section describes the booting features that are new in the initial release of Release 10.2.

- Rsh and rcp—Release 10.2 implements the remote shell (rsh) and remote copy (rcp) protocols. Cisco IOS software can act as a client as well as a server. Rsh allows users to easily execute commands on remote routers without having to continuously initiate or resume Telnet sessions. Rcp has been added as a reliable transport-based mechanism for the **copy** command.

Platform and Interface Features

This section describes the platform and interface features that are new in the initial release of Release 10.2.

- Cisco 1000 series LAN Extender—The Cisco 1000 series of LAN Extender platforms is a two-port chassis that connects a remote Ethernet LAN to a core router at a central site. The LAN Extender is intended for small networks at remote sites consisting of 30 or fewer users. You can use the LAN Extender with Cisco 7000, Cisco 4000, and Cisco 2500 series routers.
- IBM channel attach interface—Support for IBM channel attach is provided on the Cisco 7000 series routers by the Cisco Channel Interface Processor (CIP) and an appropriate interface adapter card. With a CIP and the ESCON Channel Adapter (ECA) or bus-and-tag Parallel Channel Adapter (PCA), a Cisco 7000 series router can be directly connected to a mainframe. This direct connection replaces the function of an IBM 3172 interconnect controller with no loss in LAN-to-channel connectivity, thus enabling mainframe application and peripheral access from LAN-based workstations. Cisco IOS software supports TCP/IP mainframe protocol environments for the IBM MVS and VM operating systems, including the TCP/IP-based applications Telnet, FTP, SMTP, and NFS.
- G.703 interface for FSIP—Release 10.2 supports G.703 interfaces for the Fast Serial Interface Processor (FSIP) board and the 4T NIM (available on Cisco 7000 series and Cisco 4000 routers only).
- SMT 7.3—Release 10.2 supports FDDI Station Management (SMT) 7.3.

Important Notes

This section describes warnings and cautions about using the Release 10.2 software. The information in this section supplements that given in the section "Release 10.2(9) Caveats/Release 10.2(10) Modifications" later in this document.

This section discusses the following topics:

- Upgrading to a New Software Release
- Booting Cisco 4000 Routers
- Tuning Buffers on Cisco 4000 Routers
- Using AIP Cards
- Software Compression Transmission Rates
- IP Multicast and Mrouted
- Forwarding of Locally Sourced AppleTalk Packets
- Configuring AppleTalk over SMDS
- IPX Type 20 Packet Propagation
- Odd-Length Novell IPX Packets
- Cisco 1000 LAN Extender Issues
- Using Source-Route Bridging and Translational Bridging on Cisco 2500, Cisco 4000, and Cisco 4500 Routers
- Assigning DLCIs to Subinterfaces

Note Cisco IOS Release 10.2(3) was never released.

Upgrading to a New Software Release

If you are upgrading to Release 10.2 from an earlier Cisco software release, you should save your current configuration file before configuring your router with the Release 10.2 software.

Booting Cisco 4000 Routers

You must use the Release 9.14 rxboot image for Cisco 4000 routers because the Release 10.2 rxboot image is too large to fit in the ROMs. (Note that this is not a problem for Cisco 4500 or 4700 routers.) The Release 9.14 rxboot image does not recognize new network processor modules, such as the Multiport Basic Rate Interface (MBRI) network processor module. Having to use the 9.14 rxboot image causes two problems:

- You cannot boot from a network server over BRI lines. Instead, 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
```

Tuning Buffers on Cisco 4000 Routers

You should modify the buffer allocation for Cisco 4000 and Cisco 4500 routers with MBRI interfaces because the default buffer allocation is inadequate. The number and type of buffers you need depend on the number of BRI interfaces that are enabled, the maximum transmission unit (MTU) size configured for the BRI interfaces, and the amount of available I/O memory. The discussion in this section provides guidelines for determining how many buffers you need to allocate.

To determine the MTU size that is configured for each BRI interface, use the **show interfaces** EXEC command.

To determine if you have enough buffers in your free list for the affected buffer pool, use the **show buffers** EXEC command. The affected buffer pool depends on the MTU of the interface. By default, all BRI MTUs default to 1500 bytes, which fall into the big buffers pool (buffers of 1524 bytes). The following example shows output from the **show buffers** command on a router with eight active BRI interfaces:

```
Router# show buffers

Buffer elements:
     430 in free list (500 max allowed)
     144 hits, 0 misses, 0 created
Small buffers, 104 bytes (total 60, permanent 60):
     60 in free list (20 min, 150 max allowed)
     16 hits, 0 misses, 0 trims, 0 created
Middle buffers, 600 bytes (total 27, permanent 25):
     27 in free list (10 min, 75 max allowed)
     51 hits, 1 misses, 0 trims, 2 created
Big buffers, 1524 bytes (total 325, permanent 325, need -36):
     45 in free list (5 min, 40 max allowed)
     719 hits, 0 misses, 0 trims, 0 created
Large buffers, 5024 bytes (total 0, permanent 0):
     0 in free list (0 min, 10 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
Huge buffers, 18024 bytes (total 41, permanent 20, need 40):
     21 in free list (20 min, 100 max allowed)
     44 hits, 2 misses, 0 trims, 21 created
     4 max cached, 4 in cache free list
2 failures (0 no memory)
```

This example shows that the big buffers pool has 45 buffers in the free list. This is not enough buffers for eight active BRI interfaces.

Another factor to consider when tuning buffers is the amount of I/O memory. You need to monitor this value to ensure that you do not exhaust the memory when you increase the number of buffers in the free pool. Use the **show memory** command to display I/O memory. For example:

```
Router# show memory

             Head  FreeList    Total(b)     Used(b)     Free(b)  Largest(b)
Processor   4813EC    3EFE5C    12053524      863664    11189860    11167048
      I/O  6000000    3F6504     4194304     2147884     2046420     2008828
     SRAM     1000    3F5788       65536       64892         644         512
```

Because this router has 2 MB of free I/O memory out of a total of 4 MB, it contains enough free I/O memory to tune the big buffers pool.

The following example shows the global configuration commands you might issue to tune the big buffers pool. These commands allocate 500 permanent big buffers, with a minimum of 50 and a maximum of 600 free buffers. The last command allocates 50 temporary buffers when the router is reloaded.

```
buffers big permanent 500
buffers big max-free 600
buffers big min-free 50
buffers big initial 50
```

After you tune the number of free buffers, use the **show buffers** and **show memory** commands again to verify the results. In the following example, the **show buffers** command shows many more buffers in the free list, and the **show memory** command shows 1.5 MB of free I/O memory, which is sufficient for the router to operate at a good performance level:

```
Router# show buffers

Buffer elements:
     430 in free list (500 max allowed)
     146 hits, 0 misses, 0 created
Small buffers, 104 bytes (total 60, permanent 60):
     60 in free list (20 min, 150 max allowed)
     20 hits, 0 misses, 0 trims, 0 created
Middle buffers, 600 bytes (total 27, permanent 25):
     27 in free list (10 min, 75 max allowed)
     25 hits, 1 misses, 0 trims, 2 created
Big buffers, 1524 bytes (total 550, permanent 500):
     270 in free list (50 min, 600 max allowed)
     719 hits, 0 misses, 0 trims, 50 created
Large buffers, 5024 bytes (total 0, permanent 0):
     0 in free list (0 min, 10 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
Huge buffers, 18024 bytes (total 82, permanent 60):
     62 in free list (20 min, 100 max allowed)
     45 hits, 1 misses, 0 trims, 22 created
     4 max cached, 4 in cache free list
1 failures (0 no memory)

Router# show memory

               Head  FreeList    Total(b)     Used(b)     Free(b)  Largest(b)
Processor    4813EC    3EFE5C    12053524      951924    11101600    11091096
      I/O   6000000    3F6504     4194304     2601348     1592956     1586056
     SRAM      1000    3F5788       65536       64892         644         512
```

Using AIP Cards

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

Software Compression Transmission Rates

The rate of transmitting compressed data is about the same on all Cisco routers. Currently, there is no speed advantage in running compression on a Cisco 4500, which has a faster CPU than the other routers.

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.

Forwarding of Locally Sourced AppleTalk Packets

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

Configuring AppleTalk over SMDS

When configuring AppleTalk interfaces, there are two network options: nonextended networks and extended networks. (Non-extended is not Phase 1, unless it is used on Ethernet.) All AppleTalk routers in the Switched Multimegabit Data Service (SMDS) cloud need to agree that the network is either nonextended or extended.

Non-extended AppleTalk is recommended if any devices on the cloud are running Cisco IOS Release 10.0, Release 10.2(6) or earlier, or Release 10.3(3) or earlier.

Extended AppleTalk is recommended for interoperability with non-Cisco IOS devices. In this case, all devices using Cisco IOS software must be running Cisco IOS Release 10.2(7) or later, Release 10.3(4) or later, or 11.0. This will allow dynamic AARPs on the SMDS Multicast channel and eliminate the need for static maps.

IPX Type 20 Packet Propagation

In releases prior to Release 9.21, IPX type 20 packet propagation was controlled by the **ipx helper-address** interface configuration command. This is no longer the case. In Releases 9.21, 10.0, and later, type 20 packet propagation is disabled by default on all interfaces. To enable it, use the following interface configuration command:

ipx type-20-propagation

Note that you must modify existing configurations to use type 20 packet propagation.

When enabled, type 20 packet handling now conforms to the behavior specified in the Novell *IPX Router Specification*. Type 20 packets continue to be subject to any restrictions that may be specified by the **ipx helper-list** command.

Odd-Length Novell IPX Packets

In releases prior to Release 9.21, you could force padding of odd-length IPX packets sent on Fiber Distributed Data Interface (FDDI) and serial interfaces by simply disabling fast switching on an interface. This action corrected packet length problems in certain topologies running older software releases.

In Releases 9.21, 10.0, and later, the default behavior when process switching is identical to fast switching: odd-length IPX packets are always padded on Ethernet interfaces and never padded on FDDI, serial, or Token Ring interfaces. To force padding of odd-length packets on FDDI, serial, or Token Ring interfaces, you must disable fast switching and issue the new **ipx pad-process-switched-packets** interface configuration command.

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 data terminal equipment (DTE) devices only, they require the data communications equipment (DCE) to provide both a transmit and receive clock. A digital service unit/channel service unit (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 directly connected directly to a Cisco 1000 with a DCE cable. To work around this problem, either use a different serial card or install a modem eliminator in the line that supplies both the transmit and receive bit clocks.

Using Source-Route Bridging and Translational Bridging on Cisco 2500, Cisco 4000, and Cisco 4500 Routers

On Cisco 2500, Cisco 4000, and Cisco 4500 routers, you cannot use source-route bridging and translational bridging simultaneously. This is because Texas Instruments has stopped production of the TMS380C16 and has switched to the TMS380C26 Token Ring chip. The new chip disables the source router accelerator chip (SRA) when the TMS380C26 chip is in promiscuous mode. Whenever transparent bridging is turned on, the source route bridging ceases to function. This problem is being tracked as caveat CSCdi22815.

Assigning DLCIs to Subinterfaces

When you use the **frame-relay inverse arp** command to assign a data-link connection identifier (DLCI) to a subinterface, the system does not retain the configuration and the **write terminal** command does not display the configuration. See the documentation for the **frame-relay interface-dlci** command for information about assigning subinterfaces.

Release 10.2(15) Caveats

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(15). These caveats apply to all 10.2 releases, up to and including Release 10.2(15). The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Documentation CD-ROM or access Cisco Connection Online as described at the end of this document.

FDDI

- If you upgrade a Synoptics 3800 series router to Cisco IOS Release 10.2(13) or a later release, all routers connected via FDDI will reboot with the bus error message, “System restarted by bus error at PC 0x1340C2, address 0xAE010004.” This reboot will occur intermittently, about once a week. [CSCdi70585]

IP Routing Protocols

- IP packets might be accepted on an interface that is not configured for IP if an IP directed broadcast is input on that interface. [CSCdi72982]

- Packets routed using RIP with a time to live (TTL) value set to zero might be ignored by router. [CSCdi46442]

ISO IGRP

- After removing a static CLNS route, ISO-IGRP prefix routes might count to infinity around a looped topology. The workaround is to use **clns router iso-igrp** DOMAIN to break the loops in the CLNS topology untill the routes age out. [CSCdi78048]

SRB

- If you define a ring group to support remote source-route bridging (RSRB) or to support more than two source-route bridging interfaces, all packets will be process-switched. [CSCdi69100]

Wide-Area Networking

- Combining a synchronous serial interface in a rotary dialer with Basic Rate Interfaces (BRIs) does not follow the bandwidth-on-demand load-sharing model. [CSCdi37048]
- 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]

Release 10.2(14) Caveats/Release 10.2(15) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(14). These caveats apply to all 10.2 releases up to and including Release 10.2(14). For additional caveats applicable to Release 10.2(14), see the caveats section for Release 10.2(15), 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-ROM or access Cisco Connection Online as described at the end of this document.

The caveats listed in this section are resolved in Release 10.2(15).

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]

Basic System Services

- The system might reload if the **show version** EXEC command is performed. The syslog system error message “ALIGN-3-CORRECT” might display before the reload. [CSCdi34937]

IBM Connectivity

- Sometimes when remote source-route bridging (RSRB) peers appear to be in an open or opening state, no traffic can pass through. Once the remote peer statements are removed and reconfigured, the peers will become operational. [CSCdi36072]
- Source-route bridging from Token Ring to Fiber Distributed Data Interface (FDDI) environments causes a corrupt frame to be generated on the FDDI ring when an explorer frame is bridged from the Token Ring. The resulting FDDI explorer frame has its MAC address length bit set to indicate 2-byte addressing when, in fact, the frame has a 6-byte address. These frames are misread by other stations on the FDDI ring. [CSCdi39289]
- Qualified Logical Link Control (QLLC) devices that are connected through a router using QLLC/Logical Link Control, type 2 (LLC2) conversion might occasionally experience poor response time. [CSCdi44923]
- 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]

Interfaces and Bridging

- A system reload occurs with autonomous cBus bridging enabled on a Cisco 7000 router running Switch Processor (SP) microcode version 10.9. To work around, run fast cBus bridging or upgrade to a version of Release 10.2 that includes SP microcode version 10.12. [CSCdi36643]
- The router takes a large number of drops on a serial card. [CSCdi37512]
- When an access list is loaded via the **config net** command, large blocks of memory might be consumed by the silicon switching engine (SSE) manager process, requiring the router to be rebooted. [CSCdi39419]
- If a router configured for X.21 and acting as a data terminal equipment (DTE) device sets Control = OFF for any reason (such as interface resets) and frames exist on the Transmit circuit, the data communications equipment (DCE) device might go into a loop 2 or loop 3 condition. When X.21 is configured, the DTE device should not send any data if Control = OFF. [CSCdi45512]

IP Routing Protocols

- The system might fail to send a proxy Address Resolution Protocol (ARP) response upon receipt of an ARP request through an interface where the **ip mobile arp** command has been configured. This problem occurs when the source IP address of the ARP request is part of the directly connected network of the system's interface on which the ARP request is received.

  The system should not suppress a proxy ARP response in the above situation if it can generate such a response without interfering with potential mobile IP addresses. Specifically, the system should not suppress such responses if it can determine the source of the ARP request to be a mobile host, or the destination of the ARP request to not be a mobile host. The **ip mobile arp access-group** command must be used to enable the system to make such determinations in this situation. [CSCdi36709]

- 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 cBus or Switch Processor (SP) complex. [CSCdi39274]

Wide-Area Networking

- 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)
```

Release 10.2(13) Caveats/Release 10.2(14) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(13). The caveat listed in this section applies to all 10.2 releases up to and including Release 10.2(13). For additional caveats applicable to Release 10.2(13), see the caveats sections for later 10.2 releases, which precede this section.

Only the serious problems are listed in this section. For a complete list of caveats against this release, use the Documentation CD-ROM or access Cisco Connection Online as described at the end of this document.

The caveat listed in this section is resolved in Release 10.2(14).

IP Routing Protocols

- Deconfiguring an IP output access group on a subinterface causes the IP output access-list checks to be disabled for other subinterfaces of the same hardware interface. [CSCdi60685]

Release 10.2(12) Caveats/Release 10.2(13) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(12). These caveats apply to all 10.2 releases up to and including Release 10.2(12). For additional caveats applicable to Release 10.2(12), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(13).

Basic System Services

- 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]

IBM Connectivity

- The router might crash if you remove remote source-route bridging (RSRB) peers. [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 you configure a router for RSRB via direct encapsulation, the router will continually reboot while the remote router sends keepalives. The router will only come up if the connection between the two routers breaks, or if the remote router determines the link to be dead. [CSCdi45949]
- 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]
- Low-end platforms will cache invalid Routing Information Field (RIF) entries when using any form of the **multiring** command. You can see these invalid entries in the data-link switching (DLSw) reachability cache. You might also observe loops within the LAN Network Manager (LNM). [CSCdi50344]
- When the command **fst** is used with RSRB, the router might suffer performance degradation and display the console message: [CSCdi50997]

  ```
  SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=xxxxxx, count=0 -Traceback=xxxxxx
  xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
  ```

- One or more SDLC-attached devices might fail to be polled. This failure will occur if an interface is defined for SDLC encapsulation and you add an SDLC address that is a lower value than any other SDLC address already defined on the interface. A workaround is to reload the router or to remove all SDLC address definitions and re-add them in ascending order. [CSCdi53646]
- 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]
- An 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 this problem, first remove and then reconfigure the **source-bridge** command from the Token Ring interface. [CSCdi53954]
- New Systems Network Architecture (SNA) sessions fail to connect to a front-end processor, when duplicate ring numbers are in the RIF. To work around this problem, issue the **clear rif-cache** command. [CSCdi55032]
- Issuing a **no source-bridge remote-peer** command might sometimes cause the bus error “address 0xd0d0d0d0” and a router reload. [CSCdi55919]
- The **lnm resync** command does not work with 10.3(10.2) on Cisco 7000 series routers if the router is configured for IBM automatic spanning tree (AST) support. [CSCdi59890]

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]

- 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]
- Cisco 4500 routers cannot bridge IPX unicast packets between Ethernet and Fiber Distributed Data Interface (FDDI) environments. [CSCdi53363]
- SABME (for Netbios) messages are not correctly bridged from FDDI to serial lines if you are using High-Level Data Link Control (HDLC) encapsulation. However, bridging of SABME messages between FDDI and Ethernet works correctly. [CSCdi58733]

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]
- Packet corruption might occur when fast-switching IP packets from ATM interfaces to Token Ring interfaces configured with the **multiring** command. [CSCdi49734]
- If you use regular expressions longer than 59 characters in the **ip as-path access-list** configuration command, the router will reload. [CSCdi53503]

ISO CLNS

- When using RFC1490 encapsulation for Open System Interconnection (OSI) protocols, the system inserts an extra byte into the header. When communication is between two Cisco devices, Cisco encapsulation can be used to work around this problem. [CSCdi40775]
- Issuing a Connectionless Network Service (CLNS) ping to one of the router’s own addresses will cause the router to reload if **debug clns packet** is on. The workaround is to not have this particular debug on if you need to ping to one of the router’s own addresses. [CSCdi50789]

Wide-Area Networking

- A Cisco 4000 series router with Integrated Services Digital Network (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]
- 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]

Release 10.2(11) Caveats/Release 10.2(12) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(11). These caveats apply to all 10.2 releases up to and including Release 10.2(11). For additional caveats applicable to Release 10.2(11), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(12).

AppleTalk

- AppleTalk Transaction Protocol (ATP) packets might be incorrectly sent to a multicast address instead of a unicast address. This can cause problems such as the inability to login to an AppleTalk server. [CSCdi44145]

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

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

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]

EXEC and Configuration Parser

- If you configure a nondefault Fiber Distributed Data Interface (FDDI) transmission time and save the **fddi valid-transmission-time** to nonvolatile random-access memory (NVRAM), the system will reload when the boot monitor reads the command from NVRAM at boot time. If a nondefault time is required, the workaround is to boot that portion of the configuration using the **boot host** command. [CSCdi37664]

IBM Connectivity

- Remote source-route bridging (RSRB) remote peers configured for direct and TCP encapsulation exhibit a memory leak in a dead state. It takes an hour for the dead peer to consume the entire memory. The workaround is to manaully remove the dead peers. [CSCdi32752]
- 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 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 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]
- Applying a **source-bridge output-lsap-list** to a Token Ring interface when **source-bridge explorer-fastswitch** is enabled might cause packets permitted by the output-lsap-list to be dropped. The workaround is to issue the **no source-bridge explorer-fastswitch** command. [CSCdi51754]

Interfaces and Bridging

- On a Cisco 4500 router, if you issue the **no shutdown** command on a Fiber Distributed Data Interface (FDDI), the router will reboot. [CSCdi42429]
- A Cisco 7000 series router configured with a Silicon Switch Processor (SSP) might sporadically reload when main memory is low. [CSCdi43446]
- When a Cisco 2500 runs X.25 over the B channel of a Basic Rate Interface (BRI), it sends the idle character 0xFF (mark) instead of the idle character 0x7E (flag). X.25 requires flags, not marks, for the idle character. [CSCdi44262]
- When bridging is configured on interfaces not capable of silicon switching engine (SSE) bridging, then SSE bridging for all interfaces on the router is disabled. The workaround is to use cBus bridging. [CSCdi45124]

IP Routing Protocols

- In a Cisco 7000 series router, when Open Shortest Path First (OSPF) is configured, an interface cost is not automatically assigned to the CIP interface. To work around this problem, configure the subinterface command **ip ospf cost** *cost* to statically assign a cost to the interface. [CSCdi42163]
- A system running 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 (Enhanced IGRP) might fail on primary serial interfaces. Failure can occur when the subinterfaces were configured for IPX routing before their primary interface was. [CSCdi44144]
- Enhanced IGRP might announce IP summary routes that have the metric value set too high. This can make the applicable networks unreachable. [CSCdi46290]

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]
- ISO–IGRP sometimes fails to install parallel routes into the Connectionless Network Service (CLNS) prefix table. [CSCdi50714]
- If two Cisco 4500 routers are connected and one router is running DECnet and CLNS, and the other router is running DECnet, IPX, and CLNS, both routers will display the following message:

  ```
  ALIGN-3-SPURIOUS: Spurious memory access made at 0x60144260 reading 0x0
  ```

  Each router will reload shortly after the other displays this message. [CSCdi52421]

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]
- When an Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) route is advertised back into Routing Information Protocol (RIP), the delay within the Enhanced IGRP cloud is not properly taken into account 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]
- If IPX Enhanced IGRP is running, the following command sequence might cause the router to reload: [CSCdi49577]

  interface serial

  no ipx network

  no ipx routing

TCP/IP Host-Mode Services

- 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
  ```

VINES

- VINES servers located downstream might unexpectedly lose routes that were learned via Sequenced Routing Update Protocol (SRTP). This behavior results from improper handling of network sequence 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 sets the IPC length in each IPC message to the total number of bytes of all IPC messages. [CSCdi47766]

- 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 an "abnormal end of Vines SRTP." A workaround is to turn off Vines redirects on the serverless segment interface. [CSCdi50536]

Wide-Area Networking

- When a Cisco 4500 receives a compressed TCP packet over X.25, it might reset the virtual circuit. [CSCdi36886]
- 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]
- Basic Rate Interface (BRI) interfaces might stop placing calls after a period of normal operation. To re-enable the interface, you must 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 **encap lapb** or **encap X25** configured, sometimes the command **lapb N1 xxx** disappears from the working configuration and N-1 falls back to the default. This problem is most likely to occur after an interface reset or a reload. [CSCdi44422]
- When a Cisco 4000 with a BRI interface 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]
- Issuing a **no dialer-list** command followed by a **dialer-list** command causes the router to reboot. [CSCdi45951]

Release 10.2(10) Caveats/Release 10.2(11) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(10). These caveats apply to all 10.2 releases up to and including Release 10.2(10). For additional caveats applicable to Release 10.2(10), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(11).

AppleTalk

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

IBM Connectivity

- When an SDLLC or QLLC virtual ring is configured, explorers may be incorrectly forwarded to the interface corresponding to the third ring in the routing information field (RIF). [CSCdi43378]

- On low-end systems for a DTE router interface, after a router reload, SDLC packets are identified as HDLC packets by the serial driver until a **shut/no shut** command is performed for the interface. This causes packets to drop occasionally without any trace, if the byte pattern happens to match that of other protocols. This can also cause serious performance problems. [CSCdi43686]
- Using the source-route bridging (SRB) proxy-explorer feature with SRB autonomous switching on FDDI might cause incoming packets to be dropped by the FDDI interface. The workaround is to disable the SRB proxy-explorer feature, or to disable SRB autonomous switching on the FDDI interface. [CSCdi44095]
- SRB bridged packets may be dropped when the router is configured for RSRB direct, and priority/custom queueing is enabled on the output serial interface. A work-around is to disable priority/custom queueing on the serial interface. [CSCdi44430]

Interfaces and Bridging

- The serial interface on Cisco 2500 series routers will enter a looped state if it is configured as a backup DTE interface, and if the cable is disconnected and reconnected a few times. A **clear interface** command fixes the problem. [CSCdi32528]
- With two routers on a FDDI ring, Open Shortest Path First (OSPF) neighbors disappear after a few hours because the IP process does not receive the multicast packet for OSPF hellos. [CSCdi38185]
- On a Cisco 4500 router bridging DECnet, certain stations might be unable to establish connectivity over transparent bridging, because some DLC frames are not forwarded when they should be. [CSCdi42690]
- Enabling SSE for IP might cause the system to crash. The workaround is to perform the **no ip route-cache sse** command. [CSCdi44414]

VINES

- 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]
- 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" message. If the router runs out of call control blocks, severe errors will likely occur. [CSCdi42123]
- Under unusual circumstances, configuring an interface for Link Access Procedure, Balanced (LAPB) or X.25 might cause the router to become unresponsive, requiring it to be reloaded. [CSCdi42803]
- Hardware flow control may be inadvertently disabled on the Cisco 2509, 2510, 2511 and 2512 routers’ asynchronous ports after a **configure network** or a **copy tftp running-config** command is issued. To restore flow control, issue the line configuration command **flowcontrol hardware** on all lines. [CSCdi43306]

Release 10.2(9) Caveats/Release 10.2(10) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(9). These caveats apply to all 10.2 releases up to and including Release 10.2(9). For additional caveats applicable to Release 10.2(9), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(10).

Basic System Services

- Memory might become corrupted when servicing MacIP AppleTalk Translation Protocol (ATP) packets, causing a system reload. [CSCdi41076]

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]
- In very rare circumstances the router may reload after a **show lnm station** command is entered and part of the output has been displayed. This might happen if the router is attached to Token Ring(s) that are in great distress and experiencing serious error conditions at the time the command is entered. [CSCdi39483]
- The Cisco 4500 router might reload if a TEST(F) or NULL XID(F) is received while the X.25 SVC for the QLLC connection is down. [CSCdi40851]
- In rare cases, the router's serial interface driver software will drop SDLC frames with bit patterns identical to HDLC LEX frames. This problem has been observed on interfaces using STUN-basic encapsulation with non-IBM SNA data traffic (for example, COMM10 CNS protocol). 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]
- Fast Sequenced Transport (FST) performs poorly when running over serial lines. [CSCdi41846]
- The Find Name NetBIOS broadcast is sent from all the Token Ring interfaces even though the proxy-explorer and NetBIOS name caches are configured on the interface. To workaround, run backlevel software. [CSCdi41972]
- After configuring a LAN Network Manager (LNM) PC with a bridge definition that contains the target interface MAC addresses on the router, you might notice the following behavior. If a **no source-bridge** *local-ring bridge-number target-ring* command is subsequently entered for one of the interfaces previously configured on the LNM PC, and a **link bridge** command is then entered on the LNM PC, the router will halt with a bus error indication. The only workaround is to ensure that **no source-bridge** *local-ring bridge-number target-ring* commands are not executed on the router after the target LNM server bridge is defined on the LNM PC. [CSCdi41997]

Interfaces and Bridging

- For a given bridge table entry, bridging may fail to forward packets sourced from that address destined for a particular device but not for others. This behavior is present when a **show bridge** *nnnn.nnnn.nnnn* shows the TX count incrementing, but the RX count staying constant. The workaround is to issue a **clear bridge** command. [CSCdi42445]

IP Routing Protocols

- Enhanced IGRP displays incorrect redistributed routes in the topology table. [CSCdi40200]
- OSPF is not able to flood huge router link-state advertisements (LSAs) correctly (bigger than 1456 bytes). The huge router LSAs are generated when there are more than a hundred OSPF interfaces or more than a hundred secondary addresses defined on the OSPF interfaces. This huge LSA can cause the router to crash. Note that the fix for this problem requires all routers in the OSPF area that need to process huge LSAs to be upgraded with the Cisco IOS version containing the fix; routers running older versions could crash upon receiving the huge LSA. [CSCdi41883]

ISO CLNS

- When you run ISO-IGRP and a Connectionless Network Service (CLNS) route goes in holddown and is deleted, a memory leak of 128 bytes will occur. This behavior can happen very frequently in a normal network. The final result will be that the ISO-IGRP process will use most of the RAM memory, and the router will become unreachable and will stop functioning. A reboot is the only way to get the router going again. [CSCdi39191]

Novell IPX, XNS, and Apollo Domain

- When **ipx route-cache cbus** and **ipx encapsulation arpa** commands are configured for a router interface, autonomous switched packets are dropped by the router. The only workaround is to use fast-switching only. [CSCdi40585]

Wide-Area Networking

- When you are using data terminal ready (DTR) dialing and Point-to-Point (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 behavior 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 get sent out to the network. [CSCdi39627]
- When using multiple BRIs into a rotary group, the router may dial extra B channels in a very short period of time, even though the load on some of these B channels is less than the configured threshold. [CSCdi39713]
- In rare circumstances, an SDLLC connection failure can cause the router to reload. [CSCdi39832]
- 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. Entering a **clear line x** command, or changing to the line parameters will cause the line to start accepting input again. [CSCdi40994]
- ISDN routers with a Primary Rate Interface (PRI) or BRI interface may crash when receiving a Layer 3 Status Enquiry message with a “Display IE” in the message. [CSCdi42382]

Release 10.2(8) Caveats/Release 10.2(9) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(8). These caveats apply to all 10.2 releases up to and including Release 10.2(8). For additional caveats applicable to Release 10.2(8), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(9).

AppleTalk

- The system may halt unexpectedly when the **show appletalk route** command detail is given. [CSCdi36007]

IBM Connectivity

- NetBIOS connections occasionally fail to connect through RSRB when local acknowledgment is enabled. The workaround is to disable local acknowledgment. [CSCdi37525]
- The following three problems have been observed when source-route bridging from Token Ring to FDDI is enabled on a router:
    - — A corrupt frame is generated on the FDDI when a explorer frame is bridged from the Token Ring. The resulting FDDI explorer frame has its MAC address length bit set to indicate 2-byte addressing when in actuality the frame has a 6-byte address. These frames are misread by other stations on the FDDI ring.
    - — If source-route bridging from Token Ring to FDDI is configured to use a ring group while remote source-route bridging (RSRB) is also configured, the router will erroneously attempt to forward FDDI frames over RSRB links. Source-route bridging from FDDI to Token Ring over RSRB is not supported.
    - — If the router receives a FDDI frame with a duplicate ring number in the routing information field (for example, a RIF loop), it will erroneously forward the frame. The correct behavior is to drop frames that contain RIF loops. [CSCdi39293]

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]
- The Cisco 4500 router with an FDDI interface module may reload with an error. The interface should reset first instead of reload. A temporary workaround is to shut down the FDDI interface. [CSCdi35936]
- On the Brut partner product (a Cisco 3000 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 Enhanced IGRP (EIGRP) process receives a hello packet from a neighbor, it tries to send an update packet, but the process of sending an update packet can be suspended by the EIGRP process. When the EIGRP process is again scheduled to send the update packet, the neighbor could 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]

- 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]
- Static routes are not being redistributed into EIGRP after a **clear ip route *** command is issued. A workaround is to kick-start the redistribution process by either removing one static route and reinstalling it, or by removing and reinstalling the **redistribute static** command under the **router eigrp** *xx* command. [CSCdi38766]

ISO CLNS

- When issuing a **clear clns is-neighbors** command the maximum number of entries in the ISIS route table can be reduced to 130. Any additional entries that may have existed could be lost. The only workaround is not to issue this command. [CSCdi36854]
- Route redistribution from ISIS into another IP routing protocol does not function. One symptom is that ISIS routes that are redistributed into RIP are advertised with metric 16 (infinity) after the first periodic ISIS SPF run. [CSCdi40353]

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]

Wide-Area Networking

- When a serial PPP link from a Cisco 7000 router to a LEX box goes protocol down, the LEX continues to forward frames out the serial interface. [CSCdi39882]

Release 10.2(7) Caveats/Release 10.2(8) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(7). These caveats apply to all 10.2 releases up to and including Release 10.2(7). For additional caveats applicable to Release 10.2(7), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(8).

Basic System Services

- A TTY line configured for software flow control on a Cisco 2509 through Cisco 2512 access server will occasionally garble data when connecting to a remote host using the telnet protocol. [CSCdi35487]

DECnet

- When a DECnet MOP remote console connection is attempted from a VAX to a Cisco router, a connection is made, and a password prompt is issued. Shortly thereafter, the connection breaks. [CSCdi36500]

IBM Connectivity

- When bridging from Ethernet to Token Ring using an FDDI backbone on a Cisco 4500 router, the MAC layer address is not bit-flipped correctly for transparently bridged frames received on the FDDI interface that are then translated to source-route bridged frames via source-route translational bridging (SR/TLB) and sent out that same FDDI interface. [CSCdi34328]
- The following error messages may result in a router reload or loss of session when using local-ack: [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.
```

- If RSRB is configured on more than two Token Ring interfaces in a router with a CBUS/SP controller (AGS+ and Cisco 7000 series), then some of the Token Ring interfaces will stop accepting packets after a number of explorers arrive at the interface. FDDI interfaces may also stop accepting packets. See CSCdi34101. [CSCdi36539]
- Source-route bridging from Token Ring to FDDI causes a corrupt frame to be generated on the FDDI when an all-routes explorer frame is bridged from the Token Ring. The resulting FDDI explorer frame has its MAC address length bit set to indicate 2. [CSCdi36678]
- In some networks, when direct source-route bridging from Token Ring to FDDI is enabled on a wrapped FDDI ring, the router fails to strip frames from the FDDI ring properly. When this condition occurs, the FDDI ring utilization approaches 100% and the router appears to pause. [CSCdi36717]
- 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 Logical Link Control (LLC) explorer frames and the router console does not accept keyboard input. Recovery is achieved by reloading. The work around is to remove the command (use the **no source-bridge proxy-explorer** command) on the Token Ring interfaces. [CSCdi36718]

Interfaces and Bridging

- When encapsulation bridging on FDDI is used on a Cisco 4500 router, swapping from a canonical to a non-canonical MAC address is not performed for packets sent on the FDDI interface. [CSCdi37188]

IP Routing Protocols

- 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]

Novell IPX, XNS, and Apollo Domain

- Large **ipx output-sap-delay** and **ipx output-rip-delay** settings may keep normal updates from running.

  Four new Novell IPX commands are added:

  — **ipx default-output-rip-delay**

  — **ipx default-output-sap-delay**

  — **ipx triggered-rip-delay**

  — **ipx triggered-sap-delay**

  The **ipx default-output** commands set global defaults for all interfaces.

  The **ipx triggered** commands set per-interface values for the interpacket gap in Flash and poison RIP/SAP updates. Values override the **ipx output-rip-delay** and **ipx output-sap-delay** settings and are recommended to be a small values, if a large normal interpacket gap is configured. [CSCdi34411]

Wide-Area Networking

- Under unknown conditions, some X.25 data packets may incorrectly have the D bit set, which causes a connection to be reset. [CSCdi35036]
- The 2 MB SSP does not support the AIP card. [CSCdi38127]

Release 10.2(6) Caveats/Release 10.2(7) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(6). These caveats apply to all 10.2 releases up to and including Release 10.2(6). For additional caveats applicable to Release 10.2(6), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(7).

AppleTalk

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

Basic System Services

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

DECnet

- When DECnet IV/V conversion is enabled on a router configured for L2, the router ceases to send L2 hellos to the Phase IV+ (all L2 routers) multicast. As a result, other vendors' routers that explicitly listen to L2 hellos on this multicast will not create an L2 adjacency.

  In an all-Cisco environment, there is no problem, since Cisco routers will listen for L2 hellos on the "old" ("all routers") multicast. [CSCdi34275]

IBM Connectivity

- 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]
- In some rare cases a router configured for STUN with local acknowledgment will stop forwarding all packets and will continuously print the following messages on the console: "%SYS-2-INTSCHED: event dismiss at level 5 -Process= "IP Input", ipl=5, pid=7". [CSCdi33993]

Interfaces and Bridging

- In high-traffic environments, FSIP8 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 Microcode Version 10.8 fixes this problem by splitting the memd read on transmit into 32-byte chunks and enabling interrupts between the chunks. [CSCdi27451]

IP Routing Protocols

- If an IGRP or RIP routing process is configured but no routing update has been sent in the last 24 days so that no "line protocol up" interfaces are available, then routing updates may be suppressed for up to 24 days before resuming. [CSCdi33918]
- If a serial interface is configured for the same subnet and the subnet falls within the range of the **network** command, OSPF might not recognize that one or more serial interfaces are nonfunctional (shut down). In this situation, OSPF might include one of these nonfunctional interfaces as an output interface in SPF calculations and might incorrectly select it for routing to another border area router. If a nonfunctional interface is selected for routing, the **show ip ospf border-router** command will display incorrect information, and summary and external routes will not be installed in the IP routing table. [CSCdi35182]

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]

TCP/IP Host-Mode Services

- Serial interfaces with Frame Relay encapsulation will drop the very small incoming frames that are sometimes produced by TCP/IP header compression. This results in excessive retransmits which cause TCP to become very slow. The work around is to disable TCP/IP header compression on interfaces configured with Frame Relay encapsulation. [CSCdi34470]

VINES

- Bridge access lists 200 don’t work when used in a dialer-list because the extracted packet ethertype is off by 4 bytes. To work around the problem use the **dialer-list 1 protocol bridge permit** command. [CSCdi27037]
- A 32 bit cell that is used to store timer values wraps every 49 days and 17 hours. This results in incorrect time values being shown in various displays. [CSCdi29908]
- If the system is running Novell IPX over a Frame Relay link and the maximum path value is greater than 1, the system will not function. [CSCdi31042]
- The system can halt unexpectedly while processing redirects received on a Token Ring interface. There is no workaround. [CSCdi33132]
- AppleTalk users running in Extended mode with Dynamic AppleTalk address resolution enabled are affected by the following: AARP frames sent to an SMDS interface are sent with a type 4(HW_SMDS) SMDS address. The SMDSTalk specification specifies that SMDS AARP entries use a type 14(HW_SMDSTALK) address. This behavior is incompatible with other vendor implementations.

  Caution This fix creates an incompatibility with the existing AppleTalk/SMDS base when you are using AARP in Extended mode. Users *must* upgrade all routers to the newer Cisco IOS versions to interoperate.

  The workaround until all routers are running Cisco IOS with this fix is to run AppleTalk on SMDS with a nonextended configuration.

  See CCO (formerly CIO), under Technical Tips and AppleTalk References for sample configurations. [CSCdi33586]
- 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]
- When you are using the bandwidth-on-demand feature over rotary groups of asynchronous or serial lines, traffic stops while a line is being dialed. [CSCdi34276]
- Some asynchronous line scripts incorrectly hang up the line. These include the line activation script, the network connection script and, in some cases the user command script. [CSCdi35773]

Release 10.2(5) Caveats/Release 10.2(6) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(5). These caveats apply to all 10.2 releases up to and including Release 10.2(5). For additional caveats applicable to Release 10.2(5), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(6).

AppleTalk

- The following error messages and trace back are displayed on the console of router configured 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 and include the text and the traceback of this message and the information from the **show version** command. [CSCdi29127]

- A slow memory leak occurs when AppleTalk Enhanced IGRP is enabled. [CSCdi30641]
- When ARA is shut down, all ARA context queues and one MNP4 context queue are not emptied. [CSCdi31592]
- CSCdi31098 identified the following error: Some AppleTalk Enhanced IGRP update packets from neighboring AppleTalk Enhanced IGRP routers are dropped with an indication that they were received with an incorrect DDP checksum. Although the update packets are, in fact, not being generated with an incorrect checksum, the error in question causes the packets to be dropped regardless. The easiest workaround is to disable DDP checksums on the router that is running AppleTalk Enhanced IGRP, dropping update packets, and indicating checksum errors. [CSCdi31812]

Basic System Services

- A Cisco 4500 may crash occasionally when executing multiple **write memory** or **write network** commands. [CSCdi29920]
- SLARP can cause routers with dual Flash bank to reload. [CSCdi30588]

IBM Connectivity

- The system may reload when using an IBM LAN Manager to change the ring number of the Token Ring interface. [CSCdi30096]
- Enabling proxy explorers causes the router to crash. It puts packets on the same ring more than once, which is a violation of source-route bridging protocol. [CSCdi32284]
- The router drops TEST/XID frames. [CSCdi32976]

Interfaces and Bridging

- When the ISDN image (igs-g-f) is run on a Cisco 2500 with two serial ports attached, the image causes the system to disable the two serial ports and reload. When the two serial ports are removed, the system functions properly. [CSCdi27578]
- In Bufferin FSIP code, custom and priority queueing do not work properly on an overdriven (high-traffic) serial link. [CSCdi28181]
- 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 can be alleviated somewhat by increasing the initial, minimum, and maximum numbers of huge buffers. [CSCdi31501]

IP Routing Protocols

- Issuing the [**no**] **ip summary-address** can cause the router to reload. [CSCdi23646]
- If an interface is configured with an IP secondary address and the **ip access-group in** command, the router will not respond to pings or Telnets directed to the interface secondary address if the ping or Telnet comes into the router on an interface other than the interface configured with the **ip access-group in** command. [CSCdi30011]

- Routes are not distributed between different IP and Enhanced IGRP processes. This problem occurs only when you enter certain commands, such as **clear ip route ***, **ip address**, **transmit-interface**, and **mtu interface**. The workaround is either to retype the redistribute router commands or to reload the configuration file either from NVRAM or over the network, depending on the location of the configuration file. [CSCdi30575]

Novell IPX, XNS, and Apollo Domain

- Apollo traffic over FDDI is not forwarded to the next-hop gateway. Instead, it is dropped by the router because the router computes the data offset incorrectly. [CSCdi32395]

Protocol Translation

- Telnet negotiation on a PAD-to-TCP translation session can fail, resulting in an opened Telnet session with no login prompt from the host. A workaround is to configure a terminal type on the VTYs used for translation. [CSCdi31420]

VINES

- Metric values in VINES ICP metric notification packets are bit-shifted four positions. This causes higher metric values and can cause time-out delays during the retransmission process. [CSCdi30821]
- Source-route information contained in SRTP Redirect packets might not be placed in the router's RIF cache with multiring configured on the interface. This error causes the router to lose connectivity with the client workstation across the source-route bridge on the Token Ring. [CSCdi30962]
- The system may halt unexpectedly following the display of **show vines ipc** output. A workaround is to issue the **terminal length 0** command prior to the VINES **show** command. [CSCdi31900]
- The system may halt unexpectedly when processing a Server Service Format Time RPC call from a client. A workaround is to have the client use another routing server that does not exhibit the problem. If the client is on a serverless net, there is no workaround. [CSCdi33030]

Wide-Area Networking

- PVCs do not work over an X.25 remote switching (XOT) connection. [CSCdi27337]
- For the **x25 route** command, allow an option **xot-source** that 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]
- If an asynchronous line is configured with the **script reset** command, the chat process that runs the script can continue indefinitely without terminating. [CSCdi29975]
- The X.25 default protocol command—**x25 default** {**ip** | **pad**}—does not work. [CSCdi30318]
- DDN and 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 ignores incoming calls with the High-Layer Compatibility (HLC) element. This causes problems for routers calling from Norway, using basic-nwnet3, because the HLC must be used in calls. Incoming calls with HLC are accepted by all the net3 switch versions. [CSCdi31517]
- Routers with multiple BRI interfaces (Cisco 4000 and Cisco 4500) can crash and have spurious memory alignment problems. This can occur if interfaces are defined and configured but not connected to a BRI interface. We recommend that unused interfaces be shut down to prevent the software from attempting to activate the interface. [CSCdi32565]

Release 10.2(4) Caveats/Release 10.2(5) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(4). These caveats apply to all 10.2 releases up to and including Release 10.2(4). For additional caveats applicable to Release 10.2(4), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(5).

AppleTalk

- When used on serial interfaces, the **no appletalk send-rtmp** command may have the unintended side effect of causing the router to never fully enable AppleTalk routing on the serial interface. The workaround is not to use this command on serial interfaces. [CSCdi29674]

Basic System Services

- The router cannot detect a shortage of buffer elements and thus does not create new ones. This situation causes the router to drop packets even though ample packet buffers exist. 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 behavior 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]
- If a system is set to be an NTP master, eventually other systems will refuse to synchronize to it. There is no workaround. [CSCdi30293]

DECnet

- A router receiving a MOP connection request through its serial port for one of its LAN port addresses responds with the LAN port’s burnt-in address instead of the actual hardware address. If the requesting host uses the DECnet-style MAC address of the router in the request packet, the host will not recognize the response packet sent by the router because it sees a different address in the “source” field. This behavior causes the requesting host to time out on the connect request. [CSCdi26991]

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 prioritization is used 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

- When you use Flash load helper to copy a new image into Flash memory, the system might return to the system image without carrying out the copy request. This behavior occurs when the length of the source and destination filenames causes a buffer to overflew. The buffer can hold only 56 characters, not including null terminators, and it can hold only 54 characters when Flash memory is partitioned into multiple partitions. You can detect the failure with the **show flh-log** command. If the copy fails, the **show flh-log** command output shows that a new image was not copied to Flash memory. This output can vary because the effects of buffer overflow are unpredictable. To prevent this problem from occurring, make sure that source and destination filenames each contain fewer than 28 ASCII characters, or 26 ASCII characters if your Flash memory is partitioned. [CSCdi26920]
- On an MCI/ciscoBus interface to a Multibus Token Ring interface that is configured for transparent bridging and fast switching, two or eight bytes of data starting from the LSAP are dropped. [CSCdi28616]
- On high-end routers, transparent bridging in FDDI encapsulation mode does not work at the process level. [CSCdi28839]
- In some cases, frames received on Token Ring interfaces may be fast-switched when they should be silicon-switched. [CSCdi29733]

IP Routing Protocols

- If a virtual link is configured, the router can place external LSAs into the retransmission list of virtual neighbors but then never send the LSAs out. When these external LSAs become invalid by reaching their maximum age, the router cannot remove them because the LSAs are still in some neighbor retransmission lists. As a result, these external LSAs remain forever in the link-state database. You will see external LSAs with arbitrarily high ages in the link-state database. [CSCdi27964]
- An IP packet that is destined for the address 0.0.0.0 is accidently routed instead of being treated as a broadcast packet if the system has a route to 0.0.0.0 in the routing table. The workaround is to use 255.255.255.255 as the broadcast address. [CSCdi28929]

Novell IPX, XNS, and Apollo Domain

- The SAP hop count for a server whose internal network number is learned via Enhanced IGRP should be the external hop count plus 1. (The external hop count is the number following the Enhanced IGRP metric in brackets in the routing table entry.) [CSCdi29455]

TCP/IP Host-Mode Services

- Certain failures during incoming rsh connections can cause the software to reload. There is no workaround. [CSCdi30148]

VINES

- The VINES address that the router retains to assign to clients is not incremented after each assignment until the router receives an RTP or SRTP update from the client. During this brief window, duplicate address assignments can occur. [CSCdi29886]

Wide-Area Networking

- When you are bridging over DDR using the **dialer map bridge** command, spanning-tree BPDUs are not transmitted over the DDR link. To work around this problem, use the **dialer string** command. [CSCdi27419]
- When dialer maps are removed from a BRI configuration, the router may reload. To work around this problem, shut down the interface before removing a map. [CSCdi28180]
- When LQM is used with PPP on a Cisco 7000 or other system that supports autonomous switching, the link may go down if the PPP quality is set too high and if significant amounts of the traffic are autonomously switched. When you reboot the router, a race condition can sometimes prevent the Cisco 7000 from starting PPP. [CSCdi28655]
- DTR dialing does not work with PPP encapsulation. Even though the console shows the line going up and down, no traffic goes through, and the serial interface is still spoofing. To work around this problem, use HDLC or X.25 encapsulation. [CSCdi29249]
- When remote source-route bridging is used over a DDR connection configured for direct encapsulation, a LINK-3-BADMACREG message is displayed. [CSCdi29352]
- A BRI interface used as the interface in a backup interface command cannot be placed in standby mode after a reload. [CSCdi29603]
- When reverse Telnet is used in certain traffic-loading conditions on asynchronous lines—generally, an asynchronous line with receive and transmit looped—garbage characters may be output on the line. [CSCdi29696]
- 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. The hardware fix for this problem was implemented on cards shipped after February 22, 1995. The hardware fix requires Cisco IOS Release 10.0(9), 10.2(5), 10.3(1), or later. [CSCdi29885]
- If you are using PPP LQM and the far side of the connection stops replying, the router does not detect that the link has failed. The workaround is not to use PPP LQM by not issuing the **ppp quality** command. [CSCdi30042]
- When a dialer string is used on a BRI or PRI interface, the router reloads. To work around this problem, use dialer maps. [CSCdi30442]
- A router with a BRI interface can run out of call control blocks (CCBs). Layer 2 can also become wedged in a state waiting for a TEI to be assigned by the switch. This condition can cause incoming or outgoing calls on the BRI interface to fail. [CSCdi30501]

Release 10.2(3) Caveats/Release 10.2(4) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(3). These caveats apply to all 10.2 releases up to and including Release 10.2(3). For additional caveats applicable to Release 10.2(3), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(4).

Basic System Services

- The router crashes due to a race condition in rsh. For example, this race condition might occur when the system is clearing the VTY line on which the rsh request arrived. [CSCdi28361]

IBM Connectivity

- A segV exception crash might occur when you are configuring source-route bridging. [CSCdi28269]

Release 10.2(2) Caveats/Release 10.2(3) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(2). These caveats apply to all 10.2 releases up to and including Release 10.2(2). For additional caveats applicable to Release 10.2(2), see the caveats sections for newer 10.2 releases, which precede this section.

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

All the caveats listed in this section are resolved in Release 10.2(3).

Basic System Services

- If a Telnet connection to the router is dropped while Flash memory is being erased, the router might crash while waiting for a response from the user. [CSCdi27218]
- Ethernet hosts using only SNAP encapsulation for IP can be excluded from the ARP table. [CSCdi27984]

IBM Connectivity

- Setting the **llc2 ack-max** parameter to a value *n* actually causes the router to acknowledge every *n* + 1 packets. Because this value cannot be set to zero, you cannot tell the router to acknowledge every packet. [CSCdi27034]

Interfaces and Bridging

- If bridging is enabled on an SSP, SSE bridging is not used, and SSE routing is used for a protocol, the SSP can route packets that appear on the local LAN even though they were not intended to be routed by the router. [CSCdi26048]

IP Routing Protocols

- For an OSPF nonbackbone area that has multiple connections to the backbone, if a serial link within the nonbackbone area goes down and then comes back up, a race condition might occur. This condition can create a host route within the no-backbone area that points to the wrong direction, thus resulting in a routing loop. This host route, an interarea route created from one of the summary LSAs, should be removed already, but it is no. The host route is then advertised by one of the area border routers. Issuing the **clear ip route** command does not correct the situation, because the summary LSA causes the host route to be inserted into the routing table again. The only workaround is to restart the OSPF process on the area border router. [CSCdi27987]

Novell IPX, XNS, and Apollo Domain

- The **ipx watchdog-spoof** command is written to nonvolatile memory before the dialer commands are written. When the system reloads, it does not enable DDR or watchdog spoofing. [CSCdi27326]

VINES

- Connectivity to remote servers running SRTP might be unexpectedly lost. This condition occurs when the router is rebooted and comes up after the remote server has marked the route to the router as bad but before the remote server has completely flushed the route out of its network table. To correct this condition, issue the **clear vines neighbor *** command on an intervening neighbor router. [CSCdi27374]

Wide-Area Networking

- The negotiation time of PPP-encapsulated ISDN call setups over the BRI interface has been improved. [CSCdi21126]

Release 10.2(1) Caveats/Release 10.2(2) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(1). These caveats apply to all 10.2 releases up to and including Release 10.2(1). For additional caveats applicable to Release 10.2(1), see the caveats sections for later 10.2 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-ROM or access Cisco Connection Online as described at the end of this document.

All the caveats listed in this section are resolved in Release 10.2(2).

AppleTalk

- AppleTalk ports can get stuck in the restart state when system uptime is greater than 24.85 days. There is no workaround; you must reload the system. [CSCdi25482]

EXEC and Configuration Parser

- Dialer maps for DECnet do not display properly when you issue a **write terminal** command. [CSCdi23564]

Interfaces and Bridging

- Bridging is not supported on lex interfaces. [CSCdi23852]
- When receiving DECnet control packets of an unidentifiable type (usually illegal), the interface can saturate its input buffer space and become unable to receive additional packets. The input queue (displayed with the **show interface** command) will show *n*+1/*n* packets, where *n* is the size of the input hold queue. [CSCdi24993]

IP Routing Protocols

- When you are load-balancing IP traffic over multiple equal-cost paths, the system's routing table might reach an inconsistent state, leading to a system reload. Before the inconsistent state is reached, the system must have three or four equal-cost paths for a particular route. A routing update must then be received that causes the system to replace those paths with fewer (but still more than one), better metric paths. This route must then become used for further locally generated traffic. This problem is most likely to be seen after an interface flap (that is, after an interface's line state goes from up to down to up again) in an environment where redundant, but not symmetric, interconnections exist between routers. The problem also seems more likely in FDDI environments, where interfaces flap before fully coming up. These flaps can result in multiple back-to-back routing table changes. [CSCdi20674]
- If you are using candidate default routes in IP Enhanced IGRP, be aware that a backwards compatibility problem exists between Cisco software versions earlier than Release 9.21(4.4), Release 10.0(4.1), Release 10.2(0.6) and later versions. Upgrade all routers to Release 9.21(4.4), Release 10.0(4.1), and Release 10.2(0.6) 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 10.0(4.7), 10.2(0.11), and 9.21(5.1). Routers running a version older than those versions will still be unable to mark Enhanced IGRP internal routes as candidate default routes. [CSCdi23758]
- Pings to secondary addresses fail if the secondary address is configured on an interface different from the one on which the packets arrive. In this case, the secondary address is mistakenly added to the IP route cache, which causes the problem. The workaround is to use the **no ip route-cache** command to disable fast switching on the interface that has the secondary address configured. [CSCdi26022]
- Packets with a time-to-live (TTL) value of 128 or greater whose TTL values are checked on systems with 68000 processors are rejected with the message "ICMP Time Exceeded." The cases that are not affected are SSE switching, autonomous switching, and most high-end fast switching (TTL checked by microcode). The case that is affected is switching on low-end routers. Notably, our ping and Telnet implementations send packets with a TTL of 255. Normal hosts generally use a smaller TTL. [CSCdi26799]

Novell IPX

- The IPX Enhanced IGRP **distribute-list** command allows standard access lists only (access lists whose numbers are 800 through 899). It should also allow extended access lists (numbers from 900 through 999). [CSCdi25895]
- IPX SAP/ISO encapsulation frames over Token Ring on a CTR or Cisco 7000 that are being sent to an FSIP or HSSI interface are corrupted if the Token Ring frames contain a Routing Information field. To work around this problem, either run SNAP encapsulation on the Token Ring, or issue the **no ipx route cache** command on the serial interface. [CSCdi26154]

Protocol Translation

- In LAT-to-PAD (X.25) translated sessions, a CTRL-S followed by the entry of any character can sometimes create a continuous stream of empty LAT messages, causing a session disconnect. [CSCdi24491]

VINES

- The VINES RIF cache becomes corrupted when an end station does an all-routes broadcast/nonbroadcast return. The router returns a corrupt RIF to the end station. [CSCdi23239]
- The router loses packets if it receives an SRTP update while there are packets on the SRTP reassembly queue from a different SRTP update. [CSCdi25280]
- Redundant routers can enter a deadlock state where they continuously exchange unicast RTP messages. This state can last up to three minutes or until broken by information from a third router. This problem has been seen with the RTP protocol only, not with the SRTP protocol. [CSCdi25580]
- When the **vines serverless broadcast** command is configured in a redundant topology and all other router interfaces are configured with the **vines serverless** command, a broadcast storm results. [CSCdi25597]
- A “pacing” parameter has been added to the VINES **ping** command. This parameter allows pings to be limited to a specified rate—for example, one per second—instead of being transmitted as fast as possible. [CSCdi25598]
- The router does not honor the “server nets only” bit in the broadcast class field, which results in extra broadcast traffic on client-only networks. [CSCdi25642]

Wide-Area Networking

- The X.25 software typically does not encode address or facility information in a Call Accepted/Call Connected packet, which some X.25 equipment rejects with a “packet too short” diagnostic (38). [CSCdi21201]
- Dial-on-demand PPP connections to any router sending an IPCP request with an IP address of 0.0.0.0 do not work. The workaround is to have the non-Cisco router propose a valid IP address in its IPCP packet. [CSCdi22160]
- Under very high traffic loads (indicated by a high packet loss rate shown in the “output drops” field), PPP Echo Reply packets are not transmitted, and the remote router declares the line down. In the case of DDR connections, the call is taken down. To work around this problem, use priority queueing and assign the heavy load traffic to the low, normal, or medium queue. [CSCdi22420]

- The system declares the AIP as operational even though the PLIM type is INVALID. As a temporary fix, the AIP interface has been disabled until the PLIM problem is corrected. [CSCdi23947]
- X.25 calls with a null destination address that are directed to the router are denied with cause 0, diag 67. [CSCdi23975]
- When IPX is used over PPP, if the node number is negatively acknowledged, the software continues to ask to negotiate it. [CSCdi24078]
- The Frame Relay broadcast queue might exhibit drops under high broadcast volume. “Buffer element” misses increase at the same time the drops happen. [CSCdi25707]

Microcode Revision History

The following sections describe each revision of microcode for the Cisco 7000 series switch and interface processors.

ATM Interface Processor (AIP) Microcode Revision Summary

AIP Microcode Version 10.1

AIP Microcode Version 10.1 was not released.

AIP Microcode Version 10.2

AIP Microcode Version 10.2 was released on September 12, 1994.

Modifications

AIP Microcode Version 10.2 adds support for AAL3/4 and fixes the following:

- IP fast-switching counters were incorrect. If fast switching was enabled, any fast-switched packets were shown as being process-switched.
- If an EOM PDU required padding bytes, the last four bytes were not set to zero.
- If the size of the CPCS-PDU was a multiple of 44, an extra cell was transmitted with an LI field of zero.
- In STM-1 mode, the SS bits were incorrectly set to 00. They are now set to 10.

AIP Microcode Version 10.3

AIP Microcode Version 10.3 was released on December 12, 1994.

Modification

AIP Microcode Version 10.3 fixes the following:

- An AIP configured with AAL3/4 and SMDS encapsulation might produce invalid PLIM error messages. When this occurs, the AIP stops processing packets. [CSCdi26813]

AIP Microcode Version 10.4

AIP Microcode Version 10.4 was released on January 19, 1995.

Modification

- AIP Microcode Version 10.4 adds support for the Route Switch Processor (RSP).

AIP Microcode Version 10.5

AIP Microcode Version 10.5 was released on March 3, 1995.

Modification

AIP Microcode Version 10.5 fixes the following:

- 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 10.6

AIP Microcode Version 10.6 was released on May 15, 1995.

Modifications

AIP Version 10.6 fixes the following:

- The **atm framing g804** command works on DS3 PLIM interfaces when it should not. It should work only on E3 PLIM interfaces. [CSCdi31226]
- Issuing the **atm txbuff0** command causes the following CxBus/800E errors: [CSCdi31438]

  ```
  %DBUS-3-CXBUSERR: Slot 1, CxBus Error
  %CBUS-3-OUTHUNG: ATM1/0: tx0 output hung (800E - queue full), interface
  ```

- DS3 cell scrambling is on by default. The ATM UNI specification requires that it be off by default. [CSCdi32996]

AIP Microcode Version 10.7

Modification

AIP Version 10.7 fixes the following:

- 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:

- Previous versions of the AIP code did not work properly with the 2MB SSP. [CSCdi38127]

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. To work around, use the **no ip route-cache** command to turn off fast switching 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:

- If sub-interfaces are defined on ATM interfaces (AIP), and if for each sub-interface *aal-encap* is set to **aal5mux ip** via the **atm pvc** command, the interface will fail to establish Permanent Virtual Circuits (PVCs) after reload until a **config memory** command is performed. [CSCdi43387]

AIP Microcode Version 10.13

Modification

AIP Microcode Version 10.13 fixes the following bug:

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

Channel Interface Processor (CIP) Microcode Revision Summary

CIP Microcode Version 10.0

CIP Microcode Version 10.0 was released on October 4, 1994.

CIP Microcode Version 10.1

CIP Microcode Version 10.1 was released on December 12, 1994.

Modifications

CIP Microcode Version 10.1 fixes the following bugs:

- CIP now drops packets for CLAW connections that are not established. Formerly, when you connected to multiple hosts and sent packets to hosts that are not up, buffers were used but not transmitted, thereby preventing other connections from transmitting data. Now if buffers are received for hosts that are not connected, they are dropped. [CSCdi25021]
- Sometimes the statistics reported to the RP by the CIP and displayed by the **show extended channel statistics** command are incorrect. [CSCdi25024]
- The optical wrap test runs once and quits; it should loop forever. With CIP Version 10.1, it loops forever if there is no other active adapter, possibly resulting in an error message if the wrap plug is removed. [CSCdi25151]
- If you issue the **shutdown** and **no shutdown** commands in rapid succession, the CIP may be up but the RP assumes it is down. [CSCdi25153]
- If an ESCON fiber that carries an active connection is repeatedly disconnected and reconnected in a very short time, the CIP might crash. [CSCdi25914]
- If the timing is just right on the mainframe, the TCP/IP software modifies a ReadFF CCW to a TIC and the channel fetches it before the opcode is updated but after the length is updated. This condition results in a ReadFF of length 0, which puts the CIP firmware into a loop. [CSCdi26124]
- A CIP interface that is shut down and has its configuration changed cannot find the new configuration file when it is brought back up. With CIP Version 10.1, the CIP deletes its configuration file during a shutdown and reads it again after the **no shutdown** command is issued, thereby making sure its configuration file is always in sync with that of the RP. [CSCdi26306]
- When a channel program check occurs, the CIP attempts to reestablish the CLAW connection incorrectly using link ID 0. As a result, the host performs a disconnect for link ID 0 and displayed the message “Link 0 being freed is out of range.” [CSCdi26438]
- Buffers are not freed properly. As a result, the software runs out of memory. [CSCdi26485] [CSCdi26539]
- When a resetting event occurs, setting “resetting event” in the flag field code of the status flag field causes VM to take the attached device offline. [CSCdi26690]

CIP Microcode Version 10.3

CIP Microcode Version 10.3 was released on February 6, 1995.

CIP Microcode Version 10.4

CIP Microcode Version 10.4 was released on March 27, 1995.

Modifications

CIP Microcode Version 10.4 provides the following enhancements and fixes the following bugs:

- A halt on one CLAW device does not queue a halt to other CLAW devices. [CSCdi26456]
- Some stack sizes are too small. [CSCdi28585]
- The CIP clean-up test and utility routines have been enhanced. [CSCdi28735]
- GDB support has been added for CIP. [CSCdi28738]
- The pca.dis file is not copied to the release directory. [CSCdi28963]
- The CIP console has been modified to support dynamically added test commands. [CSCdi28749]
- The CIP PCA fails when it is heavily loaded. [CSCdi28755]
- The CIP PCA is missing a selection after a CHPID comes online. [CSCdi28818]
- The PCA tag timeout must request a reset. [CSCdi28823]
- The debugger task needs a bigger stack. [CSCdi29084]
- The CIP PCA is causing “bus in” parity errors after a reset. [CSCdi29198]
- CIP console help does not list the “quit” option. [CSCdi29253]
- Support is needed to dynamically enable and disable GDB. [CSCdi29357]
- There is a timing problem with the CIP PCA wrap diagnostics. [CSCdi29479]
- The ESCON microcode does not handle receiving an RLP. [CSCdi29994]
- The CIP PCA timeout for diagnostics is too short. [CSCdi30400]
- Revision 2 of the ORION chip requires changes to the CIP microcode. [CSCdi30459]
- GDB support causes online insertion and removal not to work properly. [CSCdi30460]
- The dbus handler does not deal properly with old WCS commands. [CSCdi30469]
- The CIP software does not boot properly. [CSCdi30487]
- The LED startup sequence does not match that shown in the manuals. [CSCdi30530]

CIP Microcode Version 10.6

CIP Microcode Version 10.6 was released on May 15, 1995.

Modifications

CIP Microcode Version 10.6 fixes the following bugs:

- On the parallel channel, a duplicate packet might be sent to the host and the intended packet lost. [CSCdi31205]
- The CIP reaches a breakpoint and displays the message “SCB chain out of sequence” on a parallel channel interface if the adapter receives a host reset request while it is 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 does not fix it. The next time the CPU reads the memory location with the bad parity, it takes a cache error exception, which in turn leads to another microcode reload. The workaround is to either reload the 7000 or, as a less drastic measure, to 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 erroneously incremented. When OP OUT is down and the PCA is configured and running, it presents 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. Do not run wrap diagnostics without a wrap plug installed. [CSCdi33716]
- On a bus/tag channel, if a device has been configured and is active on the channel, a system reset might 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 you are using RIP (ROUTED) to provide a redundant IP datagram mode Common Link Access for Workstations (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 in to the CIP console via the Route Processor’s (RP’s) serial ports and modem, and then disconnecting while still in the CIP console mode, 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 from 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 that 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 the following:

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

  To verify that a crash was caused by this problem, provide the entire crash dump output (roughly 180 lines) to Cisco Technical Assistance Center (TAC). [CSCdi40754]
- If a CIP in a Cisco 7500 Route/Switch Processor (RSP) crashes, it displays only 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 Cisco IOS 10.2(8.4), 10.3.(6.1), or 11.0(1.1), a microcode reload or a system reload could prevent the static route for the **claw** or **offload** commands from being added. This omission happens only on a Parallel Channel Adapter (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 with no error condition indicated on the host or router console. This is due to the CiscoBus FIFOs erroneously resetting prior to each direct memory access (DMA) transfer. [CSCdi43981]
- VPLD Version 4.32 is too slow for old Altera parts. [CSCdi44782]

CIP Microcode Version 20.6

Modification

CIP Microcode Version 20.6 fixes the following bug:

- CIP IPC requires at least one interface to be completely up before allowing access to MEMD. [CSCdi48381]

CIP Microcode Version 20.8

Modifications

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]

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

CIP2 Microcode Version 20.8

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

Ethernet Interface Processor (EIP) Microcode Revision Summary

EIP Microcode Version 10.0

EIP Microcode Version 10.0 was released on May 31, 1994.

EIP Microcode Version 10.1

Modification

EIP Microcode Version 10.1 fixes the following:

- 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 9.6usec 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.

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

FIP Microcode Version 10.0

FIP Microcode Version 10.0 was released on May 31, 1994.

FIP Microcode Version 10.1

FIP Microcode Version 10.1 was released on August 22, 1994.

Modifications

FIP Microcode Version 10.1 fixes the following:

- Under heavy load, the FIP output might be suspended.
- The FIP does not allow a connection topology of router Phy B to Phy A, and router Phy A to Phy B. [CSCdi21521]

FIP Microcode Version 10.2

FIP Microcode Version 10.2 was released on December 12, 1994.

Modification

FIP Microcode Version 10.2 fixes the following:

- The FIP might enter TRACE mode when a neighboring station is rebooted.

Fast Serial Interface Processor (FSIP) Microcode Revision Summary

FSIP Microcode Version 10.1

FSIP Microcode Version 10.1 was released on May 31, 1994.

FSIP Microcode Version 10.2

FSIP Microcode Version 10.2 was released on July 11, 1994.

Modification

FSIP Microcode Version 10.2 fixes the following:

- Multiple LAPB serial lines running at 64 KB each with compression eventually lose some of their IP routes. They also lose the route to the connected serial line; all the pings across the line will not work. This was a problem only for 10.0, because compression is a 10.0 feature.

FSIP Microcode Version 10.3

FSIP Microcode Version 10.3 was released on August 22, 1994.

Modification

FSIP Microcode Version 10.3 fixes the following:

- Fast switching SAP-encapsulated packets to Frame Relay-encapsulated serial lines sometimes fails.

FSIP Microcode Version 10.4

FSIP Microcode Version 10.4 was released on October 10, 1994.

Modification

FSIP Microcode Version 10.4 fixes the following:

- A STUN multipoint link with a 4700 ALA controller drops the connection. To fix this, an alternate mark idle pattern was enabled.

FSIP Microcode Version 10.5

FSIP Microcode Version 10.5 was released on December 12, 1994.

Modifications

FIP Microcode Version 10.5 fixes the following:

- Support for the txqlength field has been added to the output of the **show interface** command for the FSIP. [CSCdi198410]
- Formerly, the FSIP did not communicate with certain older equipment that used "mark" as the idle code. The FSIP now supports either "mark" or "flags" as the idle code. [CSCdi20511]

FSIP Microcode Version 10.6

FSIP Microcode Version 10.6 was released on February 6, 1995.

Modification

FIP Microcode Version 10.6 fixes the following:

- When cabled as a DTE, the FSIP with the default port adapter (PA-7KF-SPA) does not go into loopback mode. [CSCdi27351]

FSIP Microcode Version 10.7

FSIP Microcode Version 10.7 was released on May 15, 1995.

Modifications

FSIP Microcode Version 10.7 fixes the following:

- Priority queuing on a Cisco 7000 serves the low, normal, and 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 large number of abnormal terminations. [CSCdi28278]

FSIP Microcode Version 10.8

Modification

FSIP Microcode Version 10.8 fixes the following:

- In high-traffic environments, FSIP8 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 Microcode Version 10.8 fixes this problem by splitting the memd read on transmit into 32-byte chunks and enabling interrupts between the chunks [CSCdi27451].

FSIP Microcode Version 10.9

Modification

FSIP Microcode Version 10.9 fixes the following:

- Under high traffic conditions, the FSIP can fail with the following error, “%CBUS-3-INITERR: Interface x, error(D104).” This error causes all cBus boards to be reset. The affected interface is reset, and a frame error is counted on the interface. [CSCdi33079]

FSIP Microcode Version 10.10

Modifications

FSIP Microcode Version 10.10 fixes the following:

- Data carrier detect signals are not ignored on high-end Cisco platforms as needed for SDLC Multidrops. [CSCdi32813]
- A Cisco 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 Cisco 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]

HSSI Interface Processor (HIP) Microcode Revision Summary

HIP Microcode Version 10.0

HIP Microcode Version 10.0 was released on May 31, 1994.

HIP Microcode Version 10.1

HIP Microcode Version 10.1 was released on February 6, 1995.

Modifications

HIP Microcode Version 10.1 fixes the following:

- In CRC32 mode, frames that are the size of the MTU or one less than the size of the MTU are not longer treated as “giants.”
- There was an error in giant handling that could result in error conditions such as buffer starvation.

HIP Microcode Version 10.2

HIP Microcode Version 10.2 was released on March 27, 1995.

Modification

HIP Microcode Version 10.2 fixes the following:

- 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 10.0

MIP Microcode Version 10.0 was released on May 31, 1994.

MIP Microcode Version 10.1

MIP Microcode Version 10.1 was released on July 11, 1994.

Modifications

MIP Microcode Version 10.1 fixes the following:

- The **remote loop** command does not operate properly.
- If you issue a **no shutdown** configuration command for a T1 controller that is already up, the controller is taken down and left down. A **show controller t1** command shows it as down, but no alarms are issued. Issue a **clear controller** command to correct the problem.

MIP Microcode Version 10.3

MIP Microcode Version 10.3 was released on December 12, 1994.

Modifications

MIP Microcode Version 10.3 fixes the following:

- Support for the txqlength field has been added to the output of the **show interface** command for the MIP. [CSCdi198410]
- IPX fast switching and IPX autonomous switching does not work with the MIP. [CSCdi25536]

MIP Microcode Version 10.4

MIP Microcode Version 10.4 was released on March 1, 1995.

Modification

MIP Microcode Version 10.4 fixes the following:

- There are problems with remote controller loopback.

Switch Processor (SP) Microcode Revision Summary

SP Microcode Version 10.2

SP Microcode Version 10.2 was released on May 31, 1994.

SP Microcode Version 10.3

SP Microcode Version 10.3 was released on July 11, 1994.

Modifications

SP Microcode Version 10.3 fixes the following:

- When SNAP-encapsulated frames are autonomously source-route bridged, the monitor bit is not cleared.
- IPX autonomous switching does not switch packets between Ethernet and Token Ring.
- IP packets on Token Ring are not routed when a RIF is present.
- When autonomous transparent bridging is used, the receive counters displayed can be incorrect.

SP Microcode Version 10.4

SP Microcode Version 10.4 was released on August 22, 1994.

Modification

SP Microcode Version 10.4 fixes the following:

- CLNS packets received from an Ethernet interface cannot be fast-switched.

SP Microcode Version 10.5

SP Microcode Version 10.5 was released on December 12, 1994.

SP Microcode Version 10.7

SP Microcode Version 10.7 was released on January 12, 1995.

Modifications

SP Microcode Version 10.7 adds support for autonomously source-route bridging over FDDI and SAP support for AAL5 SNAP, and fixes the following bugs:

- The classification of IP packets with options was changed to RXTYPE_UNKNOWN instead of DODIP on serial and AIP interfaces. [CSCdi26969]
- CLNS over SNAP is not classifying correctly.

SP Microcode Version 10.8

SP Microcode Version 10.8 was released on March 27, 1995.

Modifications

SP Microcode Version 10.8 fixes the following bugs:

- 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

SP Microcode Version 10.9 was released on May 15, 1995.

Modifications

SP Microcode Version 10.9 fixes the following:

- Flooding through FDDI has been fixed (part of CSCdi23977).
- The problem of intermittent (that is, random) MEMA corruption during flooding has been fixed.
- A Multibus timeout 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:

- 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:

- Maximum transmission unit (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:

- 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:

- IP packets sent to the HSRP virtual MAC address fail to be 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:

- IPX packets might be corrupted if autonomously 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 10.2

SSP Microcode Version 10.2 was released on May 31, 1994.

SSP Microcode Version 10.3

SSP Microcode Version 10.3 was released on July 11, 1994.

Modifications

SSP Microcode 10.3 fixes the following:

- When SNAP-encapsulated frames are autonomously source-route bridged, the monitor bit is not cleared.
- IPX autonomous switching does not switch packets between Ethernet and Token Ring.
- IP packets on Token Ring are not routed when a RIF is present.
- When autonomous transparent bridging is used, the receive counters displayed can be incorrect.

SSP Microcode Version 10.4

SSP Microcode Version 10.4 was released on August 22, 1994.

Modification

SSP Microcode Version 10.4 fixes the following:

- CLNS packets received from an Ethernet interface cannot be fast-switched.

SSP Microcode Version 10.5

SSP Microcode Version 10.5 was released on December 12, 1994.

Modification

SSP Microcode Version 10.5 fixes the following:

- When IPX autonomous switching is enabled, a Cisco 7000 series router might experience Multibus timeouts. [CSCdi26663]

SSP Microcode Version 10.7

SSP Microcode Version 10.7 was released on February 6, 1995.

Modification

SSP Microcode Version 10.7 adds support for source-route bridging over FDDI. It also fixes the following:

- On a Cisco 7000, IP packets that are received on ATM or HSSI interfaces will not have their TTL decremented if they contain options. [CSCdi26969]

SSP Microcode Version 10.8

SSP Microcode Version 10.8 was released on March 27, 1995.

Modifications

SSP Microcode Version 10.8 fixes the following bugs:

- 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

SSP Microcode Version 10.9 was released on May 15, 1995.

Modifications

SSP Microcode Version 10.9 fixes the following bugs:

- Flooding through FDDI has been fixed (part of CSCdi23977).

- The problem of intermittent (that is, random) MEMA corruption during flooding has been fixed.
- A Multibus timeout 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:

- 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:

- Maximum transmission unit (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:

- 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:

- IP packets sent to the HSRP virtual MAC address fail to be received if the packet is SNAP-encapsulated and the receiving interface is part of the cBus or SP complex. [CSCdi39274]
- ISL classification support for FEIP was added.

SSP Microcode Version 10.14

Modifications

SSP Microcode Version 10.14 fixes the following:

- IPX packets might be corrupted if autonomously 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 10.0

TRIP Microcode Version 10.0 was released on May 31, 1994.

TRIP Microcode Version 10.1

TRIP Microcode Version 10.1 was released on August 22, 1994.

Modifications

TRIP Microcode Version 10.1 fixes the following problems:

- Formerly, some catastrophic errors caused a flood of error messages. The number of messages has been reduced.
- The load on a queue when it overflows and causes the interface to be placed in a reset state (CTRUCHECK) has been significantly reduced.
- The processing of some extremely rare events in noisy networks causes the card to cease operation.
- Token Ring interfaces keep too many buffers locally (very low receive queue limits) if source-route bridging is enabled.

TRIP Microcode Version 10.2

TRIP Microcode Version 10.2 was released on May 15, 1995.

Modifications

TRIP Microcode Version 10.2 fixes the following problems:

- Token Ring interfaces can cease transmitting and log the message “800E output hung” or “800E tx queue full.” These errors require that the interface be reinitialized. [CSCdi31121]
- Extremely rarely, a CTRUCHECK error occurs as a result of a command queue overflow. [CSCdi31131]

TRIP Microcode Version 10.3

Modifications

TRIP Microcode Version 10.3 fixes the following problems:

- The direct memory access (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 is set).
- A SpyGlass problem causes Adapter Checks.

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*, *Router Products Configuration Guide Addendum*, *Router Products Command Reference Addendum*, and *Enhanced IGRP Configuration Guide and Command Reference* publications.

9611R