Doc. No. 78-1421-18

Router Products Release Notes for Cisco IOS Release 10.0

May 20, 1996

These release notes describe the features, modifications, and caveats for Cisco Internetwork Operating System (Cisco IOS) Release 10.0, up to and including Release 10.0(14). They include all routing and protocol translation features. Refer to the *Router Products Configuration Guide*, *Router Products Command Reference*, *Protocol Translator Configuration Guide and Command Reference*, and *Enhanced IGRP Configuration Guide and Command Reference* publications for complete router and protocol translation documentation for Cisco IOS Release 10.0.

Note Release 10.0(14) is the last maintenance release of Cisco IOS Release 10.0. Release 10.0(14) is available only on Cisco Connection Online (formerly Cisco Information Online). For more details, refer to Product Bulletin no. 455, which can be found on CCO at: `http://cio.cisco.com/warp/customer/732/100/455_pp.htm`.

Introduction

These release notes discuss the following topics:

Platform Support

Release 10.0 supports the following router platforms:

- Cisco 7000 series
- Cisco 4000 series (Cisco 4000 and Cisco 4000-M)
- Cisco 3000 series
- Cisco 2500 series (except Cisco 2520 through Cisco 2523)
- AccessPro PC Card for IBM PC
- AGS+ (with a CSC/4 processor board)
- MGS (with a CSC/4 processor board)

- CGS (with a CSC/4 processor board)
- IGS L/R/TR

Note Release 10.0 is incompatible with the CSC-E card (the older Ethernet card).

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

Table 1 LAN Interfaces Supported by Router Platforms

Feature	Cisco 7000 Series	Cisco 4000 Series	Cisco 3000 Series	Cisco 2500 Series	AccessPro PC Card	AGS+	MGS	CGS	IGS
Ethernet (AUI)	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Ethernet (10BaseT)	No	Yes	No	Yes	Yes	Yes	No	No	No
4-Mbps Token Ring	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
16-Mbps Token Ring	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
FDDI DAS	Yes	Yes	No	No	No	Yes	No	No	No
FDDI SAS	Yes	Yes	No	No	No	Yes	No	No	No
FDDI multimode	Yes	Yes	No	No	No	Yes	No	No	No
FDDI single-mode	Yes	Yes	No	No	No	Yes	No	No	No

Table 2 WAN Data Rates and Interfaces Supported by Router Platforms

Feature	Cisco 7000 Series	Cisco 4000 Series	Cisco 3000 Series	Cisco 2500 Series	AccessPro PC Card	AGS+	MGS	CGS	IGS
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
34/45/52 Mbps	Yes	No	No	No	No	Yes	No	No	No
Interfaces									
EIA/TIA-232 [1]	Yes	Yes	Yes	Yes	Yes	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-530	Yes	Yes	Yes	Yes	Yes	No	No	No	No
EIA-613 (HSSI)	Yes	No	No	No	No	Yes	No	No	No
G.703	Yes	No	No	No	No	Yes	No	No	No
ISDN BRI	No	Yes	Yes	Yes	Yes	No	No	No	No
ATM	Yes	No	No	No	No	No	No	No	No

1. Prior to the acceptance of the EIA/TIA standard by the ANSI committee, EIA/TIA was referred to as recommended standard RS-232.

Cisco IOS Software Feature Sets for the Cisco 2500

Three Cisco IOS software feature sets are provided for the Cisco 2500. Each provides a subset of the full Cisco feature set. Table 3 lists the features provided in each subset image.

Table 3 Cisco 2500 Subset Images

Feature	IP Set	Desktop Set	Enterprise Set
Bridging support	Full bridging features	Full bridging features	Full bridging features
IBM support	Filtering, local acknowledgment, NetBIOS filtering, NetBIOS name caching, proxy explorer, SNA address prioritization	Filtering, local acknowledgment, NetBIOS filtering, NetBIOS name caching, proxy explorer, SNA address prioritization	Full IBM features, including all features in the IP and desktop subsets and other features such as STUN, SDLC Transport, LLC2/SDLC, and SDLLC
LAN protocols	TCP/IP	AppleTalk, DECnet IV, Novell IPX, TCP/IP	Full LAN protocol features, including all features in the desktop subset and other features such as Banyan VINES and XNS
Management and security	Full management and security features	Full management and security features	Full management and security features
Routing protocols	BGP, EGP, IGRP, Enhanced IGRP, OSPF, RIP	BGP, EGP, IGRP, Enhanced IGRP, OSPF, RIP	Full routing protocol features, including all features in the IP and desktop subset images as well as other features
WAN protocols	DDR, Frame Relay, HDLC, ISDN, PPP, X.25	DDR, Frame Relay, HDLC, ISDN, PPP, X.25	Full WAN protocol features, including all features in the IP and desktop subset images as well as other features

Boot ROM Requirements

Boot ROM versions and system images are independent of each other. Table 4 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 5, which lists the available upgrades.

Table 4 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	9.14(7) 10.2(11a)[1] if you order an NP-4B or NP-8B

Platform	Boot ROM Level
Cisco 4500 and 4700	10.3(7)

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

Table 5 Available Boot ROM Upgrades

Platform	Order Number	Current Level
Cisco 2500 series	BOOT-2500=	10.2(8a)
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.

Memory Requirements

Note See the section “Important Notes” later in this document for additional information that pertains to memory.

With Release 10.0, the Cisco software image size exceeds 3 MB and when compressed exceeds 2 MB. Also, the systems now require more than 1 MB of main system memory for data structure tables.

For AGS+, MGS, and CGS routers to take advantage of the Cisco IOS Release 10.0 features, they must have CSC/4 processor cards and 9.1(8)-level (or higher) system ROMs for netbooting.

For the Cisco 2500, Cisco 3000 series, and Cisco 4000 routers to take advantage of the Release 10.0 features, you must upgrade the code or main system memory as listed in Table 6 and Table 7. Some platforms have specific chip or architecture requirements that affect what can be upgraded and in what increments.

Table 6 Release 10.0 Minimum Memory Requirements

Router	Required Code Memory	Required Main Memory	Release 10.0 Runs from ...
Cisco 2500 series/ AccessPro PC Card	4 MB Flash	See Table 7	Flash
Cisco 3101	4 MB Flash	4 MB RAM	Flash
Cisco 3102	4 MB Flash	4 MB RAM	Flash
Cisco 3103	4 MB Flash	4 MB RAM	Flash
Cisco 3104	4 MB Flash	4 MB RAM	Flash
Cisco 3202	2 MB Flash	16 MB RAM	RAM (netboot only)
Cisco 3204	4 MB Flash	4 MB RAM	Flash

Router	Required Code Memory	Required Main Memory	Release 10.0 Runs from ...
Cisco 4000	4 MB Flash	16 MB RAM	RAM
Cisco 4000M	4 MB Flash	8 MB RAM	RAM
IGS L/R/TR	N/A	4 MB RAM	ROM

Note You can use a run-from-RAM image in the Cisco 3000 series; however, main memory requires 8 MB of RAM for the Cisco 3104 and Cisco 3204 and 16 MB of RAM for the Cisco 3101, Cisco 3102, and Cisco 3103. Code memory requirements do not change.

Table 7 Cisco 2500 Series and AccessPro PC Card Main Memory Requirements

Network Size	IP Set	Desktop Set	Enterprise Set
Small	2 MB RAM	2 MB RAM	6 MB RAM
Medium	6 MB RAM	4 MB RAM	6 MB RAM
Large	6 MB RAM	4 MB RAM	AccessPro PC Card: 8 MB RAM Cisco 2500 series: 18 MB RAM

Microcode Software

Table 8 lists the current microcode versions. 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.

Note For Release 10.0 to run on the Cisco 7000 series, all boards must use the 10.0-level microcode that is bundled with the system image.

Table 8 Current Microcode Versions

Processor or Module	Minimum Version Required
AGS+, MGS, and CGS with CCTL2	
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-CCTL2	11.0 [2]
CSC-C2MEC	10.0

Processor or Module	Minimum Version Required
CSC-C2HSCI	10.0
CSC-C2FCI	10.0
CSC-C2FCIT	10.0
CSC-C2CTR	10.0
AGS+, MGS, and CGS with CCTL	
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[3]
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.
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.
3. Minimum level needed to run multiple IPX encapsulations and VINES fast switching.

Processor or Module	Current Bundled Microcode Version	Minimum Version Required
Cisco 7000 Series[1]		
AIP (ATM Interface Processor)	10.8	10.0
EIP (Ethernet Interface Processor)	10.1	10.0
FIP (FDDI Interface Processor)	10.2	10.0
FSIP (Fast Serial Interface Processor)	10.11	10.2
HIP (HSSI Interface Processor)	10.2	10.0
MIP (MultiChannel Interface Processor)	10.4	10.0
SP (Switch Processor)	10.9	10.2
SSP (Silicon Switch Processor, 512 KB)	10.9	10.2
SSP (Silicon Switch Processor, 2 MB)	10.9	10.3
TRIP (Token Ring Interface Processor)	10.2	10.0

1. Pre-FSIP is no longer a supported product, and microcode updates for it are no longer available.

New Features in Release 10.0(14)

There are no new features in Cisco IOS Release 10.0(14).

New Features in Release 10.0(13)

There are no new features in Cisco IOS Release 10.0(13).

New Features in Release 10.0(12)

There are no new features in Cisco IOS Release 10.0(12).

New Features in Release 10.0(11)

There are no new features in Cisco IOS Release 10.0(11).

New Features in Release 10.0(10)

There are no new features in Cisco IOS Release 10.0(10).

New Features in Release 10.0(9)

There are no new features in Cisco IOS Release 10.0(9).

New Features in Release 10.0(8)

There are no new features in Cisco IOS Release 10.0(8).

New Features in Release 10.0(7)

There are no new features in Cisco IOS Release 10.0(7).

New Features in Release 10.0(6)

This section describes new features and enhancements in Cisco IOS Release 10.0(6) of the router products software.

Dual Flash Bank

Dual Flash bank is a software feature available on low-end systems that have at least two banks of Flash memory. It allows you to partition these banks into two separate, logical devices so that each logical device has its own file system. Low-end systems supported are the AccessPro PC card, Cisco 2500 series, Cisco 3000 series, and Cisco 4000 series.

Partitioning has several benefits. It provides a better way to manage files in Flash memory, especially if the Flash size is large. For systems that execute code out of Flash memory, partitioning allows you to download a new image into the file system in one Flash bank while an image is being executed from the file system in the other bank. The download is simple and causes no network disruption or downtime. After the download is complete, you can switch over at a convenient time.

In addition, one system can hold two different images, one image acting as a backup for the other. Therefore, if a downloaded image fails to boot for some reason, the earlier running, good image is still available.

Note Full implementation of dual Flash bank support has meant that certain low-end image names have changed. Specifically, *igs-bfpx* and *igs-bpx* have now been replaced by *igs-bpx-l*. Also, *igs-df* and *igs-if* have been replaced with *igs-d-l* and *igs-i-l*, respectively.

Support for the Cisco 2505 and Cisco 2507

The Cisco 2500 series includes two new routers that have hub functionality for Ethernet interfaces. The hub is a multiport repeater. The configurations are as follows:

- Cisco 2505—8 Ethernet ports
- Cisco 2507—16 Ethernet ports

Refer to the *Update to Router Products for Cisco IOS Release 10.0* for new user interface commands for these configurations.

New Features in Release 10.0(5)

This section describes new features and enhancements in Cisco IOS Release 10.0(5) of the router products software.

Support for the Cisco 2513, Cisco 2514, and Cisco 2515

The Cisco 2500 series has three new configurations, which support dual LANs in one box. These three routers require at least Cisco IOS Release 10.0(5.3) or 10.2(1). At least version 10.0(5.3) ROM monitor and 10.0(5.3) rxboot are required.

The configurations are as follows:

- Cisco 2513—One Token Ring port, two serial ports, and one Ethernet port (1R2T1E)
- Cisco 2514—Two Ethernet ports and two serial ports (2E2T)
- Cisco 2515—Two Token Ring ports and two serial ports (2R2T)

There are no new commands for these configurations.

X.25 DDR

X.25 dial-on-demand routing (DDR) now supports the following features:

- DTR dialing on synchronous serial interfaces. Previously, only in-band V.25bis dialing was supported.
- X.25 encapsulation on interfaces configured for data terminal ready (DTR) dialing, along with Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC) encapsulations.

IGS L/R/TR and Cisco 3202

Support for the IGS/L, IGS/R, IGS/TR, and Cisco 3202 has been added to Release 10.0(5). The Cisco 3202 must be netbooted; you cannot boot it from the router itself.

AccessPro PC Card Token Ring

The AccessPro PC card now supports a Token Ring port. The AccessPro 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 AccessPro PC card consists of an ISA-bus card with an asynchronous serial auxiliary port, a synchronous serial wide-area network (WAN) port, and either an Ethernet 10BaseT port or a Token Ring port for a local-area network (LAN) connection.

Flash Load Helper

Flash load helper is a software feature available to users who want to upgrade their system software on run-from-Flash systems. Flash load helper simplifies the upgrade procedure without requiring additional hardware; however, it does require some brief network downtime.

Flash load helper uses an automated procedure that reloads from the current running image to the ROM-based bootstrap image, downloads to Flash memory, and reboots to the system image in Flash memory. Flash load helper performs checks and validations to maximize the success of a Flash upgrade and minimize the chance of leaving Flash memory in either an erased state or with a nonbootable file.

For Flash load helper to work, both the system image and the boot ROMs must support it. Otherwise, you must perform the Flash upgrade manually.

Flash Enhancements for Cisco 3000 Series and Cisco 4000 Series

In addition to Flash load helper, Release 9.14(8) rxboot adds Flash enhancements that apply to the Cisco 4000 series and the Cisco 3000 series platforms that are not run-from-Flash systems. To have these enhancements, you must update the rxboot ROM to version 9.14(8). These enhancements cover Flash upgrades, automatic booting, and reloads.

New Features in Release 10.0(4)

This section describes new features and enhancements in Cisco IOS Release 10.0(4) of the router products software.

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 wide-area network (WAN) port, and an Ethernet 10BaseT port for a local-area network (LAN) connection.

New Features in Release 10.0(3)

This section describes new features and enhancements in Cisco IOS Release 10.0(3) of the router products software.

Cisco 4000 2R NIM

The Cisco 4000 supports the 2R network interface module (NIM), an interface processor that provides connections to two Token Ring networks.

Cisco 4000 4T NIM

The Cisco 4000 supports the 4T NIM, an interface processor that provides four serial ports in full-duplex or half-duplex mode. The following new software features are supported for the 4T NIM:

- The **invert txc** command is allowed for both DTE and DCE.
- The **show controller** command is enhanced to display the following:
  - Clock rate and cable rate (RS-232, RS-449, V.35, X.21, or EIA-530, DTE, or DCE)
  - Modem signals (handshakes)

Cisco 4000 Protocol Translation

The Cisco 4000 supports protocol translation. The image required is *xx-bpx*.

New Features in Release 10.0(2)

The features in Release 10.0(2) are the same as those in Release 10.0(1).

New Features in Release 10.0(1)

This section describes new features and enhancements in the initial Cisco IOS Release 10.0 of the router products software.

User Interface

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

- Controller configuration mode—This mode allows you to configure channelized T1 interfaces.
- Map-list configuration mode—This mode allows you to configure a map list to support a static mapping scheme. Currently, it is available on Asynchronous Transfer Mode (ATM) interfaces.
- Map-class configuration mode—This mode allows you to specify quality of service (QOS) parameters, which control how much traffic the source router sends over a switched virtual circuit (SVC). Currently, it is available on ATM interfaces.

System Images, Microcode Images, and Configuration Files

The following features have been added to Cisco's image and configuration file software:

- NVRAM file compression—On the Cisco 7000 series and AGS+ routers, which have version 10.0 ROMs and nonvolatile RAM (NVRAM), you can compress configuration files. (The Cisco 4000, Cisco 3000, and Cisco 2500 are currently shipping with version 9.14(6) ROMs and do not support NVRAM.)
- Software configuration boot register for Cisco 7000 series—You can change the configuration register on the Cisco 7000 series routers using software. Previously, you could change the configuration register only on the processor card or with DIP switches located at the back of the router.

Configuring Interfaces

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

- Software compression—Synchronous serial interfaces support point-to-point compression. Our software implements a predictor compressor. Data compression is supported for Link Access Procedure, Balanced (LAPB) or multi-LAPB encapsulation.
- Channelized T1—Support for channelized T1 (also referred to as *fractional T1*) is provided on the Cisco 7000 series by means of a MultiChannel Interface Processor (MIP) and a Cisco Extended Bus (CxBus) channelized T1 adapter (CxCT1). Each CxCT1 can support a maximum of 24 T1 circuits, with each circuit corresponding to one or more timeslots. The MIP can support one or two CxCT1 adapters, providing a maximum of 48 T1 circuits.
- Integrated Services Digital Network (ISDN) caller ID screening—Caller ID screening adds a level of security by allowing you to screen incoming calls. You can verify that the calling line ID is from an expected origin. Caller ID screening requires a local switch that is capable of delivering the caller ID to the router. This feature is available on the Cisco 2500 and Cisco 3000 series routers that have a Basic Rate Interface (BRI).
- Silicon Switch Processor (SSP)—The Silicon Switch Processor is the first implementation of Cisco's silicon switching engine (SSE). SSE switching contributes to very fast packet processing by allowing the SSE to perform switching independently of the route processor. SSE switching is available for IP, IPX, bridging, and IP simple access lists.
- Support for a 64-MB memory option for the route processor in the Cisco 7000 and 7010.

ATM

Cisco IOS Release 10.0 supports native Asynchronous Transfer Mode (ATM) interfaces in Cisco 7000 series routers. ATM is a cell-switching and multiplexing technology designed to combine the benefits of circuit switching (constant transmission delay and guaranteed capacity) with those of packet switching (flexibility and efficiency for intermittent traffic).

Cisco's ATM Interface Processor (AIP) provides a single native ATM network interface for Cisco 7000 series routers. Network interfaces reside on modular interface processors, which provide a direct connection between the high-speed Cisco Extended Bus (CxBus) and the external networks. You can configure the AIP, permanent virtual circuits (PVCs), and switched virtual circuits (SVCs).

X.25 and LAPB

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

- X.25 subinterfaces—X.25 networks provide multiple point-to-point virtual circuits, either permanent (PVCs) or dynamic (SVCs), through a single physical serial interface. If all virtual circuits are present on the same interface, routing protocols that use split horizon to propagate updates are not able to route between the virtual circuits. You can define subinterfaces to assign one or more virtual circuits to separate "virtual" interfaces. This allows routing protocols to route between virtual circuits on separate subinterfaces.
- Software compression—See the description earlier in the "Configuring Interfaces" section.

Frame Relay

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

- Frame Relay Inverse ARP for VINES and DECnet—The software now supports Frame Relay Inverse Address Resolution Protocol (Inverse ARP) for Banyan VINES and DECnet, as well as native hello packets for VINES.

SMDS

The following feature has been added to Cisco's Switched Multimegabit Data Service (SMDS) software:

- 15-digit addressing—You can now enter a 15-digit E.164 address, which is a full 64 bits. You must enter at least 48 bits; SMDS sets any remaining bits to F.

DDR

The following features have been added to Cisco's dial-on-demand routing (DDR) software:

- ISDN caller ID screening—See the discussion earlier in the "Configuring Interfaces" section.
- ISDN subaddress support—You can now specify an optional called-party subaddress number in an outgoing ISDN call. You enter the subaddress number after the called-party number separated with a colon (:) in the **dialer string** or **dialer map** commands.
- For incoming ISDN BRI calls, the software can now verify a called-party number and subaddress number in the incoming setup message if it is delivered by the switch.
- Bandwidth on demand (also referred to as *defining the traffic load threshold*)—You can configure dial backup to activate a secondary line based on the traffic load on the primary line. The software monitors the traffic load and computes a five-minute average. If this average exceeds the value you set for the line, the secondary line is activated and, depending upon how the line is configured, some or all of the traffic will flow onto the secondary dialup line.
- AppleTalk over DDR—You can configure DDR lines so that AppleTalk packets place calls.

AppleTalk

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

- AppleTalk over DDR—You can configure DDR lines so that AppleTalk packets place calls.

Banyan VINES

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

- VINES 5.5—The software supports Banyan VINES Release 5.5.
- Frame Relay Inverse ARP for VINES—See the discussion earlier in the "Frame Relay" section.

DECnet

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

- DECnet Phase IV Prime—This feature supports inherent media access control (MAC) addresses, which allow DECnet nodes to coexist with systems running other protocols that have MAC address restrictions. DECnet Phase IV Prime allows MAC addresses to be assigned globally by IEEE or locally by a system administrator.

IP

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

- Hot Standby Router Protocol—The Hot Standby Router Protocol (HSRP) detects when the designated active router fails, at which point a selected standby router assumes control of the HSRP group's MAC address and IP address. A new standby router is also selected at that time. The HSRP protocol provides high network availability because it routes IP traffic from hosts on Ethernet, FDDI, or Token Ring networks without relying on the availability of any single router.
- DNSIX extended IP Security Option (IPSO) processing enhancements—The two kinds of extended IPSO fields defined by the DNSIX 2.1 specification, Network Level Extended Security Option (NLESO) and Auxiliary Extended Security Option (AESO) fields, are supported by our implementation of extended IPSO. NLESO processing requires that security options be checked against configured allowable information, source, and compartment bit values. It also requires that the router be capable of inserting extended security options in the IP header. AESO is similar to NLESO, except that its contents are not checked and are assumed to be valid if its source is listed in the AESO table.
- DNSIX audit trail facility—The audit trail facility is a User Datagram Protocol (UDP)-based protocol that generates an audit trail of IPSO security violations. This feature allows you to configure organization-specific security information. The system reports security failures on incoming and outgoing packets. The audit trail facility sends DNSIX audit trail messages when a datagram is rejected because of IPSO security violations.
- SSE fast switching for IP—The silicon switching engine (SSE) is on the Silicon Switch Processor (SSP) board in the Cisco 7000 series. SSE switching contributes to very fast packet processing by allowing the SSE to perform switching independently of the system processor.

IP Routing

The following feature has been added to Cisco's IP routing protocol software:

- BGB4—Border Gateway Protocol Version 4 (BGP4) supports classless interdomain routing, which lets you reduce the size of your routing tables by creating aggregate routes, that result in supernets. Classless interdomain routing eliminates the concept of network classes within BGP and supports the advertising of IP prefixes. Classless interdomain routing routes can be carried by OSPF, ISIS-IP, and Enhanced IGRP.

Novell IPX

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

- IPX accounting—IPX accounting allows you to collect information about IPX packets and the number of bytes that are switched through the router. You collect information based on the source and destination IPX address. Accounting tracks only IPX traffic that is routed through the router; it does not track traffic generated by or terminating at the router.

- IPXWAN—Cisco routers support the IPXWAN protocol, as defined in RFC 1362. IPXWAN allows two routers that are running IPX routing to connect via a serial link to another router, possibly from another manufacturer, that is also running IPX routing and using IPXWAN.
- SSE fast switching for IPX—The silicon switching engine (SSE) is on the Silicon Switch Processor (SSP) board in the Cisco 7000. SSE switching contributes to very fast packet processing by allowing the SSE to perform switching independently of the system processor.

XNS

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

- Network masks for extended access lists are supported.

Transparent Bridging

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

- SSE fast switching for transparent bridging—The silicon switching engine (SSE) is on the Silicon Switch Processor (SSP) board in the Cisco 7000. SSE switching contributes to very fast packet processing by allowing the SSE to perform switching independently of the system processor.
- Improved buffer handling increases performance for all autonomous switching.

Source-Route Bridging

The following feature has been added to Cisco's source-route bridging (SRB) software:

- SSE fast switching for source-route bridging—The silicon switching engine (SSE) is on the Silicon Switch Processor (SSP) board in the Cisco 7000. SSE switching contributes to very fast packet processing by allowing the SSE to perform switching independently of the system processor.

IBM Networks

The following features have been added to Cisco's IBM networks software. Note that Cisco IOS Release 10.0 incorporates all the new and enhanced IBM features introduced in Software Releases 9.1(8) and 9.1(9).

- STUN SDLC local acknowledgment and prioritization—SDLC local acknowledgment allows the router adjacent to the SDLC device to terminate the SDLC session, thus eliminating polls and acknowledgments across the WAN. This feature is an enhancement to SDLC Transport, which carries SDLC traffic through our routers using serial tunneling (STUN).
- IBM SDLC half-duplex link support—SDLC half-duplex transmission allows data to travel in both directions on a medium, but in only one direction at a time. Previously, SDLC interfaces could operate only in full-duplex mode.
- SDLLC for Ethernet—This feature allows Ethernet-based devices to communicate with SDLC-based devices over an arbitrary topology using SRB/remote source-route bridging (RSRB) in combination with the source-route translational bridging (SR/TLB) technique. There are no new commands associated with this feature.

- SDLLC serial primary—The serial primary feature allows you to attach a front-end processor to a serial SDLC line while the cluster controller is attached to the LAN media. Starting with Software Release 9.1(9), the front-end processor can be attached to a serial SDLC line while the cluster controller is attached to a Token Ring network or Ethernet LAN. There are no new commands associated with this feature.
- SDLLC local acknowledgment—SDLLC local acknowledgment allows the Cisco router to locally terminate the LLC2 session on the Token Ring side in an SDLLC connection. (The SDLC side is always locally terminated by the conversion process.) This feature provides a great deal of flexibility and allows both SDLC and LLC2 to be locally acknowledged. SDLLC local acknowledgment for Ethernet is not supported.
- LSAP/DSAP prioritization—This feature allows you to use SAP priority lists and filters to specify the priority of one protocol over another across a remote source-route bridging/SDLLC WAN.
- SNA network priority—This feature allows the router to prioritize SNA network priority traffic across an SNA backbone network by enabling the router to read the Format Identification 4 (FID4) frames and extract the SNA network priority information from them.
- Multiple-link transmission group support—Multiple-link SDLC transmission groups can be accommodated across STUN connections between IBM communications controllers, such as IBM 37x5s.
- Custom queuing—This feature allows you to reserve a specified amount of bandwidth for up to 10 queues. Bandwidth can be reserved for a specified protocol, physical port, message size, and LSAP/DSAP.

Enhanced IGRP

Enhanced IGRP is now supported. Call Cisco Customer Engineering (CE) before you enable this feature. A document entitled *EIGRP Deployment Strategies* is available on our Cisco Connection Online (CCO), formerly CIO, system. Refer to this document before deploying Enhanced IGRP.

See “Cisco Connection Online” later in this document for instructions on how to access CCO.

Important Notes

This section describes warnings and cautions about using the Cisco IOS Release 10.0 software. The information in this section supplements that given in the section “Release 10.0(14) Caveats” later in this document.

This section discusses the following topics:

- Upgrading to a New Software Release
- Using ATM Interface Processor (AIP) Cards
- Memory Loss with SNMP on Cisco 2505 and Cisco 2507
- Uploading a File from a Flash Partition
- Controlling IPX Type 20 Packet Propagation
- Odd-Length Novell IPX Packets
- Netbooting or Booting from Flash
- Increased Buffer Allocation
- Forwarding of Locally Sourced AppleTalk Packets

Upgrading to a New Software Release

If you are upgrading to Release 10.0 from an earlier Cisco software release, you should save your current configuration file before configuring your router with the Release 10.0 software.

Using ATM Interface Processor (AIP) Cards

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

Memory Loss with SNMP on Cisco 2505 and Cisco 2507

For the Cisco 2505 and 2507 platforms, performing an SNMP GET or GETNEXT of the objects *rptrAddrTrackLastSourceAddress* and *rptrAddrTrackNewLastSrcAddress* (these objects are defined in RFC 1516) results in the loss of 15 bytes of router system memory. Repeated occurrences of these requests could result in system failure. Note that these two SNMP objects are supported only on the Cisco 2505 and 2507 platforms. An SNMP GET or GETNEXT of these objects on other Cisco platforms does not cause any memory loss.

Uploading a File from a Flash Partition

Systems with the dual Flash bank feature can download a relocatable image from any server into any part of Flash memory and successfully execute the image.

Although routers with dual Flash bank can upload a relocatable image to another router not having dual Flash bank, the latter will not currently be able to execute the image because the image is linked to run from wherever it was stored in Flash memory in the uploading router. This restriction will be eliminated in a future release.

Controlling IPX Type 20 Packet Propagation

In releases before Software 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 Cisco IOS Release 10.0, 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 it will be necessary for you to modify existing configurations if type 20 packet propagation is desired.

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, it was possible to force padding of odd-length IPX packets sent on 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 this situation, it is now necessary to add a new configuration command.

In Software Release 9.21 and Cisco IOS Releases 10.0 and later, the default behavior for 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 following new interface configuration command:

ipx pad-process-switched-packets

Netbooting or Booting from Flash

For the Cisco 3000 and Cisco 4000 series routers, some Release 10.0 images might fail to uncompress after booting across the network or booting from Flash memory because of a problem in some boot ROMs before Release 9.1(8) or 9.14(4). After the ### ... sequence is displayed when the image is uncompressing, the router might reenter the ROM monitor or crash. If this occurs, you have three options or workarounds:

- Do not boot that compressed system image over the network or boot from Flash memory. Switch to a different image.
- Use only an uncompressed version of the system image.
- Upgrade to version 9.14(6)-or-later boot ROMs.

You might also want to upgrade boot ROMs on Cisco 3000 series or Cisco 4000 series routers if you encounter the following problems:

- Flash overerasure—On systems with older boot ROMs, writing to Flash memory with the boot ROM image sometimes causes overerasure of Flash memory. The symptoms are that further Flash memory erase or writes fail after exceeding the permitted number of retries. ROMs based on version 9.1(4), 9.14(1), or later, do not have this problem.
- Serial line goes down while erasing or writing to Flash memory.

Increased Buffer Allocation

On the Cisco 2500, Cisco 3000, and Cisco 4000 running remote source-route bridging (RSRB) applications in some configurations, particularly Token Ring over serial, packets greater than 1524 bytes were dropped because there were no large buffers available to hold the packets for processing. The initial buffer allocation was changed to 15 large permanent buffers and the maximum large buffer to 30 buffers, requiring approximately 45 KB more I/O memory.

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 with 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.

Release 10.0(14) Caveats

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(14). These caveats apply to all 10.0 releases, up to and including 10.0(14). The caveats listed here describe only the serious problems. Additional caveats may be found on Cisco Connection Documentation, Enterprise

Series (formerly UniverCD). You may also view caveats discovered after the release of 10.0(14) by using Bug Navigator. To use Bug Navigator, access CCO (formerly CIO) as described in the section "Cisco Connection Online" at the end of this document.

IBM Connectivity

- In Systems Network Architecture (SNA) sessions, the value for **llc2 local-window** defaults to 8 instead of 7. In NetBIOS sessions, using **llc2 local-window** *x* with *x* equal to 1 or 6, the value will erroneously set to 8. [CSCdi33845]
- 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]
- In rare cases, a router's serial interface driver software will drop Synchronous Data Link Control (SDLC) frames with bit patterns identical to High-Level Data Link Control (HDLC) LAN Emulation Configuration Server (LECS) frames. This problem has been observed on interfaces using serial tunnel (STUN)-basic encapsulation with non-IBM SNA data traffic (for example, COMM10 CNS protocol). Note that there is no indication in the router when this problem occurs. The router does not increment the interface "drop" counter or the STUN "drop" counters. Detection is possible only with a media tracing tool. [CSCdi41558]
- Qualified Logical Link Control (QLLC) connections do not come up if the secondary station is on an X.25 link. [CSCdi43634]
- Logical Link Control, type 2 (LLC2) ping functions do not exist. [CSCdi43876]
- SNA sessions fail to connect to front-end processors when multiple Routing Information Field (RIF) entries are stored for the *tic* address. To work around, issue the **clear rif-cache** command. [CSCdi54449]

Interfaces and Bridging

- Source-route bridging (SRB) frames that are 4494 bytes are not forwarded on Token Ring Interface Processors (TRIPs). Sessions might pause indefinitely if this problem occurs. A workaround is to use smaller frames by performing the **source-bridge largest-frame** command. [CSCdi32548]
- Silicon switching does not work with bridging over Fiber Distributed Data Interface (FDDI). You can verify this behavior by issuing a **show sse summary** command. [CSCdi34326]
- When cBus bridging is configured on interfaces in a bridge group on a Cisco AGS+ router, the Receive Queue Limit (RQL) goes to zero, and remains there. You can verify this behavior by issuing a **show controller cbus** command. [CSCdi35531]
- Ethernet interfaces on a Cisco 7000 might stop passing traffic and generate an error message such as [CSCdi36625]:

```
%CBUS-3-INITERR: Interface 1, Error (8028), idb 00000000 0 rx_setup - cbus_init()
```

Wide-Area Networking

- If ATM signaling timers are changed, erroneous values will be written to nonvolatile RAM (NVRAM). To work around, use the default values, which are sufficient for most networks. [CSCdi32199]

Release 10.0(13) Caveats/Release 10.0(14) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(13). These caveats apply to all 10.0 releases up to and including Release 10.0(13). For additional caveats applicable to Release 10.0(13), see the caveats section for Release 10.0(14), which precedes this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(14).

IBM Connectivity

- One or more Synchronous Data Link Control (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 SDLS 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]
- A LAN net manager 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 show up with bridges that are locally linked to the LAN manager. To work around, first remove and then reconfigure the **source-bridge** command from the Token Ring interface. [CSCdi53954]
- New Systems Network Architecture (SNA) sessions fail to connect to a front-end processor, when duplicate ring numbers are in the Routing Information Field (RIF). To work around, issue the **clear rif-cache** command. [CSCdi55032]

Release 10.0(12) Caveats/Release 10.0(13) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(12). These caveats apply to all 10.0 releases up to and including Release 10.0(12). For additional caveats applicable to Release 10.0(12), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(13).

Basic System Services

- If the **show configuration** and **write memory** commands are issued simultaneously, the system might crash because the Non-Volatile RAM (NVRAM) gets write-protected from the **write memory** operation. This causes continuous reloads. [CSCdi40434]

IBM Connectivity

- If a router receives a source-route bridging (SRB) packet with bit 2 of the routing control field set, the router might send back a bridge path trace report frame to a group address, instead of to the source of the original frame. This can cause congestion. [CSCdi47561]

IP Routing Protocols

- A system running Open Shortest Path First (OSPF) might reload when a user is configuring a controller T1 with a channel-group time slot assignment. [CSCdi43083]
- If an interface receives IP traffic destined for a device located off the same interface, the traffic will be process switched. This will occur even with the **ip route-cache cbus** and **ip route-cache same-interface** commands applied to the interface. This can cause an increase in CPU utilization. [CSCdi43811]
- Attempts to route Internetworking Packet Exchange (IPX) packets by Routing Information Protocol (RIP) or by Extended Interior Gateway Routing Protocol (IGRP) might fail on primary serial interfaces. Failure can occur when the subinterfaces were configured for IPX routing before their primary interface was. [CSCdi44144]
- Enhanced IGRP might announce IP summary routes that have the metric value set too high. This can make the applicable networks unreachable. [CSCdi46290]

Release 10.0(11) Caveats/Release 10.0(12) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(11). These caveats apply to all 10.0 releases up to and including Release 10.0(11). For additional caveats applicable to Release 10.0(11), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section “Cisco Connection Online” at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(12).

AppleTalk

- The system may unexpectedly stop sending AARP Request packets. A possible workaround is to turn on AARP gleaning. [CSCdi41414]

Basic System Services

- On a large AppleTalk network with redundant links, CPU utilization may increase dramatically due to heavy recalculation for each neighbor’s update, as a result of an unbalanced routing table search tree. [CSCdi39372]

IBM Connectivity

- A router configured with remote source-route bridging (RSRB) over Token Ring with Fast-Sequenced Transport (FST) encapsulation may stop forwarding packets to the remote peer if fast switching is enabled. The workaround is to disable fast-switching on the Token Ring interface connected to the remote peer. [CSCdi36686]
- NetBIOS connections occasionally fail to connect through remote source-route bridging (RSRB) when local acknowledgment is enabled. The workaround is to disable local acknowledgment. [CSCdi37525]
- 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 work around this behavior, 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]

IP Routing Protocols

- When the Enhanced IGRP process receives a hello packet from a neighbor (peer), and tries to send an update packet, the update can be suspended by the Enhanced IGRP process. When the Enhanced IGRP process is again scheduled to send the update packet, the neighbor could be dead and all of the internal data structures for that neighbor could have been erased. This confuses the Enhanced IGRP process and results in the generation of erroneous bus addresses which can cause the router to restart. [CSCdi35257]
- In some rare circumstances, the router might unexpectedly stop forwarding packets and stop responding to commands. To recover, power-cycle the router. [CSCdi39471]
- The use of OSPF sometimes creates an intra-area host route that points to itself during route flapping. [CSCdi39623]

ISO CLNS

- The memory for ISO-IGRP is not released until the router runs out of memory completely and has to be rebooted. [CSCdi30219]
- When you are running ISO-IGRP and a Connectionless Network Service (CLNS) route goes into holddown and is deleted, a memory leak of 128 bytes occurs. This might happen often in a normal network. The result is that the ISO-IGRP process uses most of the RAM, the router becomes unreachable and stops functioning. A reboot is the only way to recover. [CSCdi39191]

Release 10.0(10) Caveats/Release 10.0(11) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(10). These caveats apply to all 10.0 releases up to and including Release 10.0(10). For additional caveats applicable to Release 10.0(10), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section “Cisco Connection Online” at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(11).

AppleTalk

- The router invalidates old cache entries. [CSCdi35967]

IBM Connectivity

- Issuing a **show lnm interface token-ring x/x** command will cause indefinite looping when soft errors are present on the Token Ring. [CSCdi33378]

- 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 workaround is to remove the command (use the **no source-bridge proxy-explorer** command) on the Token Ring interfaces. [CSCdi36718]

Interfaces and Bridging

- In high-traffic environments, Fast Serial Interface Processor 8 will get "FCICMDFAIL" messages and may eventually get "8010 fsip_reset" message because of multiple command timeouts. The command timeouts are 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 Routing Information Protocol (RIP) routing process is configured, but no routing update has been sent in the last 24 days (for example, if there are no "line protocol u" interfaces available), then routing updates may be suppressed for up to 24 days before resuming. [CSCdi33918]
- A router acting as an Open Shortest Path First (OSPF) Area Border Router may incorrectly run out of free memory. [CSCdi34206]
- If a serial interface is configured for the same subnet and the subnet falls within the range of the **network** command, the OSPF protocol 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 shortest path first calculations and might incorrectly select that interface 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]
- The system may crash when you issue a **show ip ospf delete-list** command. [CSCdi35275]
- Using Enhanced IGRP-IP, if a default network is known through an interface that is shut down, the **show ip eigrp top act** command shows the default network via the down interface. In these circumstances, CPU utilization for Enhanced IGRP can rise to 40 percent to 50 percent. [CSCdi36032]
- The router does not remove link-state advertisements (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 Routing Information Protocol/Service Advertisement Protocol (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]

VINES

- Fast switching VINES over FDDI can cause void frames to be transmitted onto the FDDI ring. The void frames occur when a new FDDI cache entry is created. [CSCdi34315]

Wide-Area Networking

- When performing bandwidth-on-demand over rotary groups of asynchronous or serial lines, traffic stops while a line is being dialed. [CSCdi34276]
- The 2 MB Silicon Switch Processor (SSP) does not support the ATM Interface Processor (AIP) card. [CSCdi38127]

Release 10.0(9) Caveats/Release 10.0(10) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(9). These caveats apply to all 10.0 releases up to and including Release 10.0(9). For additional caveats applicable to Release 10.0(9), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section “Cisco Connection Online” at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(10).

AppleTalk

- The router sends the first Name Binding Protocol (NBP) FwdRq to the correct DLC next hop address, but sends all FwdRq packets to the multicast address. As a result, a user might not see all entities in a given zone. This problem only occurs when the ARA protocol clients try to send an NBP Broadcast Request to the router. NPB lookups done from the Ethernet port (such as with NBPtest) are not affected. [CSCdi30787]
- Corrected the problem which prevents the router from running in pre-FDDI talk mode. [CSCdi33270]

IBM Connectivity

- Turning on proxy explorers causes the router to pause indefinitely because it puts packets on the same ring more than once. This behavior is a violation of SRB protocol. [CSCdi32284]

IP Routing Protocols

- The **[no] ip summary-address** command can cause the router to reload. [CSCdi23646]

- IP packet are generated with an identification field of zero. Packet fragments arrive at their destination intermixed with fragments from other packets. The receiving end is not able to reassemble the packet correctly because no useful identification is present. [CSCdi30818]

VINES

- The system can halt unexpectedly while processing redirects received on a Token Ring interface. There is no workaround. [CSCdi33132]

Wide-Area Networking

- Packets can be corrupted over BRI interfaces under some conditions. This results in lower throughput than would normally be expected across the BRI connection. [CSCdi25792]
- X.25 interfaces that use priority IP encapsulation (DDN mode) will clear a call if a Call Confirm does not explicitly confirm the requested priority. [CSCdi32872]

Release 10.0(8) Caveats/Release 10.0(9) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(8). These caveats apply to all 10.0 releases up to and including Release 10.0(8). For additional caveats applicable to Release 10.0(8), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section “Cisco Connection Online” at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(9).

Basic System Services

- The router cannot detect a shortage of buffer elements and thus does not create new ones. This causes the router to drop packets even though there are ample packet buffers. The **show buffers** command output shows many buffer element misses. [CSCdi29379]

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]
- You cannot have more than 999 elements in the hold queue. This limit is too low. [CSCdi28903]

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]

IP Routing Protocols

- 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]

VINES

- The VINES address the router retains to assign to clients is not incremented after it is assigned to a client until the router receives an update (RTP or SRTP) from the client. This delay leaves a short window in which duplicate address assignments can occur. [CSCdi29886]
- Metric values in VINES ICP metric notification packets are bit-shifted 4 positions. This causes higher metric values and can cause timeout delays during the retransmission process. [CSCdi30821]

Wide-Area Networking

- DLCI's cannot be reassigned to subinterfaces from a primary interface. [CSCdi28765]

XNS, Novell IPX, and Apollo Domain

- When a new adapter is inserted into the router after it is booted, the interface short name is missing from commands like **show ipx servers** [CSCdi27331]
- The SAP hop count for a server whose internal network number is learned via Enhanced IGRP should be the external hop count +1. (The external hop count is the number following the Enhanced IGRP metric in brackets in the routing table entry.) [CSCdi29455]
- In a network with a mixture of routers running Release 9.1 and 9.21-or-later Cisco images, where one or more of the 9.1 units are using the command **ipx helper-address network.ffff.ffff.ffff** and the network is some network other than –1, IPX NetBIOS filters are not enforced on the helpered packets that are received on the 9.21-or-later units. [CSCdi30101]

Release 10.0(7) Caveats/Release 10.0(8) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(7). These caveats apply to all 10.0 releases up to and including Release 10.0(7). For additional caveats applicable to Release 10.0(7), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(8).

Basic System Services

- When running very large IPX route tables that change frequently, the router can fragment memory to a point where Telnet connections to the router are refused and messages like "Low on memory" and "No memory available" might appear during certain operations. You likely have this problem if the "Free(b)" value is much larger than "Largest(b)" value in the **show memory** output. [CSCdi28549]

EXEC and Configuration Parser

- If you choose the default value for packet rate on a Frame Relay broadcast queue, the broadcast queue will resort to all default values when the router is rebooted. The workaround is to choose a packet rate other than the default, which is 36. [CSCdi27784]

Interfaces and Bridging

- If bridging is enabled on an SSP but SSE bridging is not used, and SSE routing is used for a protocol, then the SSP can route packets that appear on the local LAN but 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 nonbackbone area that points to the wrong direction, 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 not. 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 to the routing table again. The only workaround is to restart the OSPF process on the area border router. [CSCdi27987]

TCP/IP Host-Mode Services

- When the sequence number for a TCP connection grows so large that the right edge of the window rolls over to zero, the usable window size calculation fails to calculate the correct usable window size. [CSCdi27537]

Wide-Area Networking

- In some instances, when a Frame Relay subinterface with an inactive DLCI has been administratively shut down by a user, it might exit the shutdown state and return to the active state even though the DLCI is still in an inactive state. [CSCdi25156]
- When removing dialer maps from a BRI configuration, the router might reload. To work around this problem, shut down the interface before removing a map. [CSCdi28180]

Novell IPX

- The **ipx watchdog-spoof** command is written to nonvolatile memory before the dialer commands are written. Upon a reload, the system complains about DDR not being enabled and will not enable watchdog spoofing. Instead of enforcing watchdog spoofing on dialer-configured interfaces, allow spoofing on all serial or dialer interfaces. [CSCdi27326]

Release 10.0(6) Caveats/Release 10.0(7) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(6). These caveats apply to all 10.0 releases up to and including Release 10.0(6). For additional caveats applicable to Release 10.0(6), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(7).

Interfaces and Bridging

- When TCP/IP routing is enabled along with transparent bridging on the same interface, some SNAP-encapsulated TCP/IP packets with destinations on the same network segment might be bridged to other networks. [CSCdi23944]
- This bug was found in the priority packet path (Eh: keepalives, bpdus, and so on). Holdq_enqueue can fail also due to the lack of available queue elements, in addition to the normal case when the queue becomes full. In such a case, make sure if a tail is present before unqueuing it to accommodate the current priority packet. If there is no tail, just flag failure. The crash occurred because there was no check for the valid tail. [CSCdi26417]

IP Routing Protocols

- 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. There are two workarounds to this problem: run SNAP encapsulation on the Token Ring, or issue the **no ipx route cache** command on the serial interface. [CSCdi26154]

VINES

- The VINES RIF cache becomes corrupted when an end station does an all routes broadcast/nonbroadcast return. The problem is that the router returns a corrupt RIF to the end station. [CSCdi23239]
- Connectivity to remote servers running SRTP might be unexpectedly lost. This 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. You can correct this condition by issuing the command **clear vines neighbor *** on an intervening neighbor router. [CSCdi27374]

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]
- A router might reload itself after you issue the **show frame-relay map** command if the Frame Relay interface has a static map configured and is running Inverse ARP for the same DLCI. [CSCdi25585]

Release 10.0(5) Caveats/Release 10.0(6) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(5). These caveats apply to all 10.0 releases up to and including Release 10.0(5). For additional caveats applicable to Release 10.0(5), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(6).

Basic System Services

- Detection and initialization of the Flash load helper logging buffer is incorrectly handled, possibly causing a "booting loop." During power up, reloading, or exception handling, the presence of the Flash load helper logging buffer is detected by the validation of a Magic value in the buffer header. If the Magic value is present, the buffer is assumed to be present.

  During power cycling, the Magic value can be retained in DRAM even though the contents of the buffer are invalid (and parity has been lost as well). Messages are logged to the buffer during boot-up time, resulting in a parity error. This error, in turn, tries to log a message to the Flash load helper logging buffer, leading to a double bus fault. The system watchdog timer resets the system and the process repeats.

  The following output is seen on the console port:

```
System Bootstrap, Version 4.0(8), RELEASE SOFTWARE
Copyright (c) 1986-1994 by cisco Systems

System Bootstrap, Version 4.0(8), RELEASE SOFTWARE
Copyright (c) 1986-1994 by cisco Systems

System Bootstrap, Version 4.0(8), RELEASE SOFTWARE
Copyright (c) 1986-1994 by cisco Systems

System Bootstrap, Version 4.0(8), RELEASE SOFTWARE
Copyright (c) 1986-1994 by cisco Systems
...
```

  The OK LED might also flash at the rate with which the system reboots.

  If the system showing this symptom is powered off for a minute and then powered on, the system should boot up correctly. [CSCdi24663]

AppleTalk

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

EXEC and Configuration Parser

- Dialer maps for DECnet do not show properly in response to a **write terminal**. [CSCdi23564]
- The interface command **access-expression** [**in**|**out**] *expression* is written to configuration memory as a filter for both inbound and outbound packets. [CSCdi24000]

Interfaces and Bridging

- 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 (from **show interface**) will show *n*+1/*n* packets, where *n* is the size of the input hold-queue. [CSCdi24993]

IP Routing Protocols

- When 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 3 or 4 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 1), 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 in an environment where there are redundant, but not symmetric, interconnections 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]
- Enabling the Hewlett-Packard IP Probe protocol via the **ip probe proxy** command does not correctly enable the protocol. There is no workaround for this behavior. [CSCdi23909]

VINES

- Redundant routers can get into 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 only been seen with the RTP protocol, not with the SRTP protocol. [CSCdi25580]
- When **vines serverless broadcast** is configured in a redundant topology, and all other router interfaces are configured as **vines serverless**, the result is a broadcast storm. [CSCdi25597]
- This fix adds a "pacing" parameter 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. This results in extra broadcast traffic on client-only networks. [CSCdi25642]

Wide-Area Networking

- Dial-on-demand PPP connections to a Wellfleet router (or any router sending an IPCP request with 0.0.0.0) will 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 load (high packet loss rate shown under "output drops"), 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, use priority queueing and assign the heavy load traffic to the low, normal, or medium queue. [CSCdi22420]

- When using IPX over PPP, if the node number is NAK'ed, we continue to ask to negotiate it. [CSCdi24078]
- Serial interfaces are reset every 30 seconds if the link is down. This needs to be configurable as analog modems take more than 30 seconds often to sync up. The new command **serial restart-time** takes a parameter from 1 to 900, which is the time in seconds that this reset should be performed. [CSCdi24868]
- The Frame Relay broadcast queue might exhibit drops under high broadcast volume. There will be an increase in buffer element misses at the same time the drops happen. [CSCdi25707]

Release 10.0(4) Caveats/Release 10.0(5) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(4). These caveats apply to all 10.0 releases up to and including Release 10.0(4). For additional caveats applicable to Release 10.0(4), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section "Cisco Connection Online" at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(5).

AppleTalk

- When system uptime exceeds approximately 24.45 days, AppleTalk interfaces can unexpectedly hang during restarts and never become operational. The only workaround is to reload the system. [CSCdi20052]

Basic System Services

- A crash can happen if the user removes an AIP from one slot, and then plugs another AIP in a different slot and attempts to configure the new AIP or issue the **write terminal** command. This problem is now fixed. [CSCdi22537]

DECnet

- A router that has been configured as a Level 1 router should not send out Level 2 routing updates. [CSCdi20884]

IBM Connectivity

- The **netbios enable-name-cache** command does not work in a topology that has two or more paths to the workstations. The **show rif** command shows both paths, but the **show netbios-cache** command shows only one path. [CSCdi18524]
- When applying NetBIOS access lists with **rsrb remote-peer** access list statements on a system with active SRB traffic, the router may reload due to a bus error. The fix changes the system code so that it handles these conditions in a more graceful manner. [CSCdi18993]

Interfaces and Bridging

- A problem exists with clocking under DCE mode with a multidrop modem. It is fixed by the new board with version 5.1 or above microcode. This fix is a corequisite to the new SCI/HDX board. [CSCdi18325]
- On Cisco 2502 and Cisco 2504 routers, IP and IPX packets of length 920 to 1050 bytes being routed from Token Ring to serial interfaces may be corrupted. The workaround is to disable fast switching on the serial interface. [CSCdi19480]

IP Routing Protocols

- In OSPF, when a neighbor goes down, a host route for that neighbor is incorrectly added. A possible workaround is to trigger the rebuild of OSPF router link state advertisement by changing the interface metric or by rebooting. [CSCdi21103]
- When the router determines that it is isolated from the rest of the network and must send an SRTP REINIT message, it incorrectly resets the next SRTP update time to some multiple of the correct interval. This causes the router to not send updates for some long interval, and thus to time out of its neighbors' routing tables. [CSCdi23534]
- If you are using candidate default routes in IP Enhanced IGRP, be aware that there is a backward-compatibility problem between Cisco versions earlier than Software Release 9.21(4.4), Release 10.0(4.1), Release 10.2(0.6), and later Cisco versions. Upgrade all routers to Release 9.21(4.4), Release 10.0(4.1), or 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]

Wide-Area Networking

- When a BRI interface is used as a backup interface, and the backup is being done based on load, the BRI interface may be taken down prematurely, even though the load is still high. [CSCdi20472]
- When X.25-over-TCP (XOT) sends a call confirm packet that modifies one of the two proposed flow control facilities (window sizes or maximum packet sizes), the values may be set to 0, which is illegal. [CSCdi21602]
- This is a new dial-on-demand routing (DDR) feature: DTR dialing and X.25 encapsulation for DTR dialers. When DTR dialing is configured, DTR signaling is used instead on V.25bis signaling. DTR dialing is available on synchronous serial interfaces only. The configuration command for DTR dialing is [**no**] **dialer dtr**. A DTR dialer interface cannot be called. The interface that receives calls from a DTR dialer must be configured with either in-band dialing, or no dialing. The allowed encapsulations on DTR dialers are HDLC, PPP, and X.25. [CSCdi21822]

- When the system is using Frame Relay maps that were created using Inverse ARP, these maps should be dropped when a DLCI becomes inactive or is deleted. In addition, if the DLCI used by a box at the far end changes, the map entry should be updated. The second scenario might occur when Frame Relay is being accessed using dial-up service and the far end systems makes two calls in rapid succession. [CSCdi21870]
- When the system is using rotary groups, if a call does not complete, the subsequent packets may cause dialing on more than one interface. If a call is already established, these packets might cause the fast idle timer to be set and eventually the disconnection of the call. [CSCdi22717]

Release 10.0(3) Caveats

The caveats in Release 10.0(3) are the same as the caveats in Release 10.0(4).

Release 10.0(2) Caveats/Release 10.0(4) Modifications

This section describes possibly unexpected behavior by Cisco IOS Release 10.0(2). These caveats apply to all 10.0 releases up to and including Release 10.0(2). For additional caveats applicable to Release 10.0(2), see the caveats sections for later 10.0 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, use Cisco Connection Documentation (formerly UniverCD) or access CCO as described in the section “Cisco Connection Online” at the end of this document.

All the caveats listed in this section are resolved in Release 10.0(4).

DECnet

- While converting from DECnet Phase IV to Phase V (and vice versa), the router holds back a converted packet once in a while, and sends it out when some other event (for example, routing update, keepalives) happens. This sporadic delay in packet transmission results in degradation of end-to-end DECnet performance. [CSCdi20151]
- The problem reported here occurs because of incorrect interface MTU negotiation. It is seen on any interface whose default MTU is larger than the Ethernet MTU (for example, FDDI). When the VAX comes up, we end up negotiating a block size that is larger than the maximum value we are willing to process (1524). Consequently, all adjacent routers end up sending larger sized updates, which we reject. This makes all destinations behind the Cisco router unreachable. [CSCdi20225]

EXEC and Configuration Parser

- Starting in Release 9.21, with the new parser, the **ip split-horizon** command is generated before the **encapsulation** command in the configuration file during NVGEN. The **encapsulation** command has a different default for turning on/off the split-horizon feature for different encapsulations. As a result, the [**no**] **ip split-horizon** command might disappear from the configuration after rebooting because it is overridden by the default value of the encapsulation in use. This fix takes care of the problem. It ensures the **ip split-horizon** command will come after the **encapsulation** command in the configuration file of Release 9.21 and later. [CSCdi19006]

IBM Connectivity

- In low-end routers such as the Cisco 4000 and Cisco 3000, the Token Ring interface ignores IP packets that have single-route or all-route broadcast RIF. The correct behavior is to accept the packet and subsequently route it when IP routing is turned on. [CSCdi18131]
- Access lists of the form **rsrb remote-peer** *nnn* **tcp** *ip address* **netbios-output-list host** *access list name* do not function properly. The workaround is to use the same access list applied on the Token Ring interface to achieve the desired result. [CSCdi19198]
- In a local acknowledgment startup phase, the router drops the first I-frame received when the peers are still in pending state. For some end-stations, this causes session startup failures. [CSCdi19999]
- A FEP operating as a secondary SDLC station can now load a remote FEP operating as a primary SDLC station. The opposite has been possible since 9.1(9). Before a FEP is loaded with an NCP Gen, it does not have an SDLC role. The SDLC role is negotiated via XID exchange when the remote FEP is activated. [CSCdi20463]

Interfaces and Bridging

- Systems configured to support the spanning-tree bridging protocol will experience the root bridge BPDUs reappearing at the root bridge in a HSSI environment. [CSCdi18812]
- The **show controllers cbus** command on an AGS platform displays the interface name as a Cisco 7000-style name (/) instead of the correct interface name. This is cosmetic; the bug is in the display routine, so everything else will work fine. [CSCdi20161]

IP Routing Protocols

- OSPF can choose and install nonoptimal interarea and external routes when there are multiple link state advertisements for the same destination advertised by multiple Area Border Routers (or Autonomous System Boundary Routers for external routes). This can cause a routing loop if other neighboring routers still install the shortest path to the destination. This problem will happen only after the system has been up for a period of time. The length of this period depends on how many connectivity changes have occurred. In a fairly busy network, the estimated length of this period is around five to six weeks. [CSCdi20071]

ISO CLNS

- The system might crash and reload itself while it is configured for DECnet convergence or router ISIS L1/L2. The combination of the following conditions will cause this to happen:
  - Need to have a variably subnetted route.
  - Multiple routes must hash into the same subnet table hash bucket.
  - There should be a subnet with netnumber == major_net and mask == major_net_mask.
  - It must have another subnet following it.

  The root cause is the same as CSCdi20345. [CSCdi18659]

Novell IPX

- If a SAP update packet is received with an invalid length, much larger than the data actually contained in the packet, the system may reload. It is also possible, but unlikely, that invalid server entries may appear in the output of the **show ipx server** command. When these packets are received, they should be counted as SAP format errors and the counter seen with the **show ipx traffic** command should increment. [CSCdi19010]

Microcode Revision History

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

ATM Interface Processor (AIP) Microcode Revision Summary

AIP Microcode Version 10.1

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 now supports AAL3/4.

AIP 10.2 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 with Cisco IOS Release 10.0(7).

Modification

AIP 10.3 fixes the problem of the AIP producing invalid PLIM error messages when the AIP was configured with AAL3/4 and SMDS encapsulation. When this occurred, the AIP stopped processing packets.

AIP Microcode Version 10.4

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 with Cisco IOS Release 10.0(9).

Modification

AIP 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 Microcode 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 User Network Interface (UNI) specification requires that it be off by default. [CSCdi32996]

AIP Microcode Version 10.7

Modification

AIP Microcode 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 Microcode Version 10.8 fixes the following:

- Previous versions of the AIP code did not work properly with the 2 MB Silicon Switch Processor (SSP). [CSCdi38127]

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 having the router attempt to initiate a transmission. The packets must be separated by the effective interframe gap time for the router to defer to the burst. The effective interframe gap time is 9.6 microseconds plus whatever transmitter delay is configured. The transmitter delay now configures two parameters: the lower 8 bits are used to compute an effective interframe gap time; the upper 8 bits are the number of bursted packets to defer to before initiating a transmission.

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 may have become suspended.
- The FIP would 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 with Cisco IOS Release 10.0(7).

Modification

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

Fast Serial Interface Processor (FSIP) Microcode Revision Summary

FSIP Microcode Version 10.1

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 after a while 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

Version 10.3 fixes the problem that sometimes caused the fast switching of SAP-encapsulated packets to Frame Relay-encapsulated serial lines to fail.

FSIP Microcode Version 10.4

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

Modification

STUN multipoint link with a 4700 ALA controller drops the connection. We enabled an alternate mark idle pattern in order to coexist with certain types of IBM equipment.

FSIP Microcode Version 10.5

FSIP Microcode Version 10.5 was released with Cisco IOS Release 10.0(7).

Modifications

FSIP Microcode Version 10.5 fixes the following:

- The FSIP would not communicate with certain older equipment that used Mark as the idle code. FSIP now supports a choice of either Mark or Flags as idle code.
- Support for txqlength is added to the FSIP. The field appears in the output of the **show interface** command.

FSIP Microcode Version 10.6

Modification

FSIP 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

Modifications

FSIP Microcode Version 10.7 fixes the following:

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

FSIP Microcode Version 10.8

Modification

FSIP Microcode Version 10.8 fixes the following:

- In high-traffic environments, FSIP8 will get "FCICMDFAIL" messages and may eventually get "8010 fsip_reset" because of multiple command timeouts. The command timeout was caused by a long path in the FSIP firmware during the memd read on transmit. FSIP Microcode Version 10.8 fixes this problem by splitting the memd read on transmit into 32-byte chunks and enabling interrupts between the chunks [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]
- STUN: cannot initial program load a 3725 using FSIP. [CSCdi38317]

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 10.2

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 did not operate properly.
- If you issue a **no shutdown** configuration command for a T1 controller which is already up, it will be taken down and left down. A **show controller t1** command will show it as down, with no alarms being received. A **clear controller** command will fix the problem.

MIP Microcode Version 10.3

MIP Microcode Version 10.3 was released with Cisco IOS Release 10.0(7).

Modifications

MIP Microcode Version 10.3 fixes the following:

- IPX fast switching and IPX autonomous switching did not work with MIP.
- Support was added for txqlength, a field added to the output of the **show interface** command for the MIP.

MIP Microcode Version 10.4

MIP Microcode Version 10.4 was released with Cisco IOS Release 10.0(8).

Modification

MIP Microcode Version 10.4 fixes the problem of the controller remote loopback not working on the first try.

Serial Interface Processor (SIP) Microcode Revision Summary

SIP Microcode Version 1.2

SIP Microcode Version 1.2 was released on May 31, 1994.

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 autonomous source-route bridging SNAP encapsulated frames, the monitor bit was not cleared.
- IPX autonomous switching did not switch packets between Ethernet and Token Ring.
- IP packets on Token Ring were not routed when a RIF was present.
- When autonomous transparent bridging was used, the receive counters displayed may have been incorrect.

SP Microcode Version 10.4

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

Modification

SP Microcode Version 10.4 fixes a bug that prevented fast switching of CLNS packets received from an Ethernet interface.

SP Microcode Version 10.5

SP Microcode Version 10.5 was released with Cisco IOS Release 10.0(7).

Modification

SP Microcode Version 10.5 fixes a bug that caused a Cisco 7000 or Cisco 7010 to possibly experience Multibus timeouts when IPX autonomous switching was enabled.

SP Microcode Version 10.7

Modifications

SP Microcode Version 10.7 adds support for autonomous source-route bridging over FDDI and SAP support for ALL5 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. [CSCSdi26969]
- CLNS over SNAP is not classifying correctly.

SP Microcode Version 10.8

Modifications

SP Microcode Version 10.8 fixes the following bugs:

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

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 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.

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 Version 10.3 fixes the following:

- When autonomous source-route bridging SNAP encapsulated frames, the monitor bit was not cleared.
- IPX autonomous switching did not switch packets between Ethernet and Token Ring.
- IP packets on Token Ring were not routed when a RIF was present.
- When autonomous transparent bridging was used, the receive counters displayed may have been incorrect.

SSP Microcode Version 10.4

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

Modification

SSP Microcode Version 10.4 fixes a bug that prevented fast switching of CLNS packets received from an Ethernet interface.

SSP Microcode Version 10.5

SSP Microcode Version 10.5 was released with Cisco IOS Release 10.0(7).

Modification

SSP Microcode Version 10.5 fixes a bug that caused a Cisco 7000 or Cisco 7010 to possibly experience Multibus timeouts when IPX autonomous switching was enabled.

SSP Microcode Version 10.7

Modifications

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 do not have their time to live (TTL) value decremented if they contain options. [CSCdi26969]

SSP Microcode Version 10.8

Modifications

SSP Microcode Version 10.8 fixes the following bugs:

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

SSP Microcode Version 10.9

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 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.

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:

- Some catastrophic errors would cause a flood of error messages. The number of messages has been reduced.
- This version significantly reduces the load on a queue that at overflow causes the interface to be placed in a reset state (CTRUCHECK).
- The processing of some extremely rare events in noisy networks caused the card to cease operation.
- Token Ring interfaces kept too many buffers locally (very low receive queue limits) if SRB was enabled.

TRIP Microcode Version 10.2

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]

Cisco Connection Online

Cisco Connection Online (CCO), formerly Cisco Information Online (CIO), is Cisco Systems’ primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional content 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, 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, Internet e-mail, and fax download options, and 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`.
- 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 baud rates up to 14.4 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`.

Cisco Connection Documentation CD-ROM

A list of additional caveats against this release is available on Cisco Connection Documentation, Enterprise Series, formerly UniverCD, which is Cisco Systems' CD-ROM library of product information. On CD, access the Cisco IOS Release 10.0 caveats in the Cisco Product Documentation, Cisco IOS Release 10.0 and 10.1 database.

This document is to be used in conjunction with the *Router Products Configuration Guide*, *Router Products Command Reference* publication, *Protocol Translator Configuration Guide and Command Reference* publication, and *Enhanced IGRP Configuration Guide and Command Reference* publication.