Doc. No. 78-1476-15

Access and Communication Servers Release Notes for Cisco IOS Release 10.2

December 16, 1996

These release notes describe the features, modifications, and caveats for Cisco Internetwork Operating System (Cisco IOS) Release 10.2, up to and including Release 10.2(15). These release notes include all routing, access server, and protocol translation features. Refer to the *Access and Communication Servers Configuration Guide* and *Access and Communication Servers Command Reference* publications for complete access server and communication server documentation for Release 10.2.

Introduction

These release notes discuss the following topics:

If you have upgraded your hardware to the Cisco 2500 series access servers, note that the booting process differs from that on the ASM-CS and 500-CS platforms.

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

Platform Support

Release 10.2 is supported on the following access and communication server platforms:

- Cisco 2500 series access servers (Cisco 2509 through Cisco 2512)
- 500-CS communication servers—508-CS and 516-CS
- ASM/4-CS communication servers
- Cisco AS5100

Table 1 summarizes the interfaces supported on each platform. Table 2 summarizes the WAN data rates and interfaces supported on the Cisco 2500 series and Cisco AS5100.

Table 1 Interfaces Supported

Interface	ASM-CS	500-CS	Cisco 2500 Series	Cisco AS5100
Synchronous Serial	Yes	No	Yes	Yes
Ethernet (AUI)	Yes	Yes	Yes	Yes
4-Mbps Token Ring	Yes	No	Yes	No
16-Mbps Token Ring	Yes	No	Yes	No

Table 2 WAN Data Rates and Interfaces Supported

	Cisco 2500 Series	Cisco AS5100
Data Rate		
48/56/64 kbps	Yes	Yes
1.544/2.048 Mbps	Yes	Yes
34/45/52 Mbps	No	No
Interface		
EIA/TIA-232	Yes	Yes
X.21	Yes	Yes
V.35	Yes	Yes
EIA/TIA-449	Yes	Yes
EIA-530	Yes	Yes
EIA/TIA-613 (HSSI)	No	No
ISDN BRI	Yes	No
ISDN PRI	No	No
G.703/G.704	No	No

Cisco IOS Packaging for the Cisco 2500 Series

Table 2 lists the Cisco IOS feature sets available for the Cisco 2500 series and the Cisco AS5100 and the features provided in each set.

Table 3 Cisco 2500 Series and Cisco AS5100 Software Feature Sets

	Feature Set							
Feature	**IP**	**IP/IBM Base**	**IP/IPX**	**IP/IPX/ IBM Base**	**Desktop**	**Remote Access Server**	**Desktop/ IBM Base**	**Enterprise**
SNMP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Asynchronous support (SLIP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARA	—	—	—	—	Yes	Yes	Yes	Yes
Frame Relay (RFC 1490)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SMDS	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes
X.25	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes
PPP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HDLC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 3 Cisco 2500 Series and Cisco AS5100 Software Feature Sets (Continued)

	Feature Set							
Feature	**IP**	**IP/IBM Base**	**IP/IPX**	**IP/IPX/ IBM Base**	**Desktop**	**Remote Access Server**	**Desktop/ IBM Base**	**Enterprise**
OSPF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ES-IS	—	—	—	—	—	—	—	Yes
IS-IS	—	—	—	—	—	—	—	Yes
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bridging (transparent and translational)	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes
LAN extension host	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes
IPX	—	—	Yes	Yes	Yes	Yes	Yes	Yes
IPXWAN	—	—	Yes	Yes	Yes	Yes	Yes	Yes
AppleTalk Versions 1 and 2	—	—	—	—	Yes	Yes	Yes	Yes
AURP	—	—	—	—	Yes	Yes	Yes	Yes
DECnet IV	—	—	—	—	Yes	Yes	Yes	Yes
DECnet V	—	—	—	—	—	—	—	Yes
Apollo Domain	—	—	—	—	—	—	—	Yes
Banyan VINES	—	—	—	—	—	—	—	Yes
ISO CLNS	—	—	—	—	—	—	—	Yes
XNS	—	—	—	—	—	—	—	Yes
Source-route bridging	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes
Remote source-route bridging	—	Yes	—	Yes	—	—	Yes	Yes
Multiring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SDLC	—	—	—	—	—	—	—	Yes
SDLLC	—	—	—	—	—	—	—	Yes
STUN	—	—	—	—	—	—	—	Yes
TG/COS	—	—	—	—	—	—	—	Yes
QLLC	—	—	—	—	—	—	—	Yes
Protocol translation	—	—	—	—	—	Yes	—	Yes
TN3270	—	—	—	—	—	Yes	—	Yes
LAT	—	—	—	—	—	Yes	—	Yes
XRemote	—	—	—	—	—	Yes	—	Yes
Telnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AutoInstall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Memory Requirements

To take advantage of the Cisco IOS Release 10.2 features, you must upgrade the code or main system memory as listed in Table 4. Some platforms have specific chip or architecture requirements that affect what can be upgraded and in what increments.

Table 4 Cisco IOS Release 10.2 Memory Requirements

Router	Required Code Memory	Required Main Memory	Cisco IOS Release 10.2 Runs from
Cisco 2500 Series			
IP Set	4 MB Flash	4 MB RAM	Flash
IP/IBM Base Set	4 MB Flash	4 MB RAM	Flash
IP/IPX Set	4 MB Flash	4 MB RAM	Flash
IP/IPX/IBM Base Set	4 MB Flash	4 MB RAM	Flash
Desktop Set	4 MB Flash	4 MB RAM	Flash
Remote Access Server	4 MB Flash	4 MB RAM	Flash
Desktop/IBM Base Set	4 MB Flash	4 MB RAM	Flash
Enterprise Set	8 MB Flash	6 MB RAM	Flash
ASM-CS	—	16 MB RAM	RAM
500-CS	—	10 MB RAM	RAM
Cisco AS5100			
IP Set	4 MB Flash per AS51-16A-E card	2 MB RAM per AS51-16A-E card	Flash
IP/IPX Set	4 MB Flash per AS51-16A-E card	6 MB RAM per AS51-16A-E card	Flash
Desktop Set	4 MB Flash per AS51-16A-E card	6 MB RAM per AS51-16A-E card	Flash
Enterprise Set	8 MB Flash per AS51-16A-E card	6 MB RAM per AS51-16A-E card	Flash
Remote Access Server	4 MB Flash per AS51-16A-E card	6 MB RAM per AS51-16A-E card	Flash

New Feature in Release 10.2(13)

The **enable secret** command has been added, which brings an additional layer of security.

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

New Feature in Release 10.2(8)

Multivendo Flash SIMM is a new feature in Release 10.2(8):

Multivendor Flash SIMM Support.

Beginning with Release 10.2(8), you can use Flash SIMMs from multiple vendors, as long as the total size of each SIMM is equal (if both slots are used, where available) and the SIMMs are installed in one of the combinations shown in Table 4.

Multivendor Flash support is restricted to platforms that use Rxboot Version 10.2(7a) or later, and Cisco IOS Release 10.2(8) or later.

Cisco 2500 series access servers have two slots for Flash SIMMs. Table 4 provides the supported SIMM configurations.

Table 5 Cisco 2500 Series Flash SIMM Support

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

Table 5 Cisco 2500 Series Flash SIMM Support (Continued)

SIMM Size	Vendor	Flash Bank	Considerations
8 MB	AMD (2 Mb x8)	Single	This configuration requires Version Rxboot 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(11) or later • 10.2(7) or later • 10.3(4) or later
8 MB/8 MB	AMD/AMD (2 Mb x 8)	Dual	This configuration requires Version Rxboot 10.2(7a) or later. It also requires one of the following Cisco IOS Releases: • 10.0(11) or later • 10.2(7) or later • 10.3(4) or later

New Feature in Release 10.2(7)

Support for the Cisco AS5100 has been added in Release 10.2(7):

Cisco Access Server AS5100

The Cisco AS5100 is a versatile data communications platform that combines in one chassis the functions of a Cisco access server with analog and digital modems, CSUs, and T1 channel banks.

The Cisco AS5100 provides the greatest benefit for organizations that need to centralize processing capabilities for remote offices and LANs. It enables them to aggregate their modem traffic onto analog or digital telephone lines and route it through the Public Switched Telephone Network (PSTN).

New Feature in Release 10.2(5)

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

- Dual Flash bank MIB

New Features in Release 10.2(2)

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

- Snapshot routing—Snapshot routing, which is available on dial-on-demand routing (DDR) lines/interfaces, Asynchronous/synchronous, and ISDN lines, is a method of learning remote routes dynamically and then keeping the routes available for a period of time while regular routing updates are not being exchanged.
- Dual Flash bank—Dual Flash bank is a software feature that allows you to partition the two banks of Flash memory into two separate, logical devices so that each logical device has its own file system. This feature is available on Cisco 2500 series systems that have at least two banks of Flash memory. These systems must have at least two banks of Flash; one bank is a set of four chips.

- IP multicast MIB.
- Additional software feature sets have been added. These are described in the section "Cisco IOS Packaging for the Cisco 2500 Series" earlier in this document.

Software Features

This section describes new features and enhancements in the initial Release 10.2 of the access server and communication server products software.

Access Server Functionality

This section describes the access server and communication server features that are new in the initial release of Release 10.2.

- Chat script enhancements—Chat scripts are scripts written in the access server for specific user configurations, such as helping to manage modem connections. Chat scripts have been enhanced to run automatically when certain events occur. To support this enhancement, chat scripts allow you to define the following events: activation, connection, dialer, reset, and startup.
- ARA Version 2.0—Support for the AppleTalk Remote Access (ARA) protocol Version 2.0 permits users to authenticate via external security application programming interfaces (APIs) including TACACS (Terminal Access Controller Access System). Authentication via a TACACS server no longer requires a special ARAP modem connection control language (CCL) script.
- User menu terminal services—This feature allows novice users to connect to network systems by viewing and selecting a menu list. Instead of entering the name of a host to connect to, the user sees a numbered list and selects the host name by entering the associated number.
- CHAP support—PPP single-client users can now use the Challenge Handshake Authentication Protocol (CHAP) to authenticate to a TACACS server when they connect to a remote LAN. This allows you to perform CHAP authentication in the client window. The access server can then take the CHAP information, send it to the TACACS server, and authenticate the user. As a result, you no longer have to use a script for authentication.
- Asynchronous setup—You can use the **setup** command facility to configure the asynchronous lines when you start the access server or communication server for the first time.

Backbone Protocol Routing Features

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

IP Features

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

- IP multicast—This IP protocol supports applications being developed for communicating either between one sender and multiple receivers or between multiple senders and multiple receivers. Cisco's implementation includes Protocol Independent Multicast (PIM) and the Internet Group Management Protocol (IGMP). PIM allows network administrators to add IP multicast functionality to their existing networks regardless of what routing protocol they are running. PIM works with IGRP, Enhanced IGRP, OSPF, Integrated IS-IS, RIP, and BGP. PIM has two modes: dense mode and sparse mode.

- Local-area mobility—Local-area mobility provides the ability to relocate IP hosts within a limited area without reassigning host IP addresses and without changes to the host software. Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces. It is useful in environments where workers use portable computers and roam to different locations within the corporate network.

Desktop Protocol Features

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

AppleTalk Features

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

- AppleTalk Update-based Routing Protocol (AURP)—AURP is Apple Computer's new networking protocol, tuned for WANS. Cisco's implementation of AURP is fully compliant with the mandatory portions of the AURP specification, including the tunneling of AppleTalk packets inside of IP. Macintosh hosts require RTMP. Thus, Cisco routers still use RTMP to communicate with hosts and translate (or redistribute) RTMP routing information to and from AURP.
- Fast-switching enhancements—Fast switching of AppleTalk has now been implemented for Frame Relay and PPP encapsulations on all serial interfaces on all platforms. With these enhancements, AppleTalk fast switching is now supported on all LAN interfaces on all platforms. Over WANs, Frame Relay, HDLC, and PPP encapsulations are fast-switched on all platforms.
- AppleTalk MIB—A MIB for AppleTalk information has been implemented to comply with RFC 1243. Support is included for the following AppleTalk protocols: AppleTalk Address Resolution Protocol (AARP), AppleTalk Port group, AppleTalk Datagram Delivery Protocol (DDP), AppleTalk Routing Table Maintenance Protocol (RTMP), AppleTalk Zone Information Protocol (ZIP), AppleTalk Name Binding Protocol (NBP), and AppleTalk Echo Group. (Note that an AppleTalk Port represents a logical connection to a network over which AppleTalk packets can be transmitted. The AppleTalk Port group allows you to manage the configuration of these AppleTalk ports.)
- ZIP reply filters—ZIP reply filters provide one effective means for filtering zone information in an AppleTalk network. These filters allow zones to be hidden from downstream routers, as configured by the network manager. When a neighbor router queries a router with a ZIP reply filter for the zone list of an advertised network, zones that are denied in the filter are not included in the ZIP reply packet.

Novell IPX Features

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

- Fast-switching enhancements—Fast switching of Novell IPX has now been implemented for the Frame Relay and ATM encapsulations. For ATM, the AAL3/4, AAL5 NLPID, AAL5 LLC/SNAP, and AAL MUX are all supported. With these enhancements, IPX fast switching is now supported on all LAN interfaces on all platforms, and for WAN interconnection, on all platforms when HDLC, PPP, Frame Relay, or ATM encapsulation is used.
- IPX-compliant IPX ping—The standard IPX ping function, which was recently specified by Novell, is equivalent to the Cisco-specific ping implemented in previous software releases.

- IPX MIB—A MIB for Novell IPX information has been implemented that is consistent with the variables defined by Novell in their NLSP specification. The MIB supports the Novell IPX, RIP, and SAP MIB portions of the NLSP specification. However, it does not implement the NLSP MIB.

Wide-Area Networking Features

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

Frame Relay Features

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

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

DDR Features

The following features have been added to the Cisco DDR software:

- DDR dialer hold queue—Dialup services take a finite amount of time to establish a connection to a remote router. This time can vary from a couple of seconds for ISDN up to 30 seconds for an analog modem. During this time, packets destined for the remote router can be discarded because no connection exists. The creation of a dialer hold queue allows packets that would normally be dropped to be held until a connection is established.
- DTR dialing—With Release 10.2, Cisco routers support connections over serial lines connected to non-V.25bis modems using DTR signaling. Cisco already provides support for V.25bis dialing as part of the overall DDR software package.

SMDS Features

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

- Virtual interfaces—This new configuration capability allows each destination E.164 address or a group of addresses to be considered for connection to a separate port (subinterface) on the router. In turn, each virtual interface can be configured with its own addresses, routing protocols, access lists, and routing metrics.

X.25 Features

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

- RFC 1356 support—RFC 1356 supersedes RFC 877, which specified how both IP and OSI could be transported across X.25. RFC 1356 extends RFC 877 in two significant ways:
  - Multiprotocol interoperability: All protocols are carried in a defined way.
  - Single virtual circuits: Many protocols can be carried across a single virtual circuit. LLC/SNAP encapsulation of frames is used.
- X.25 payload compression—Payload compression is an extension of link compression in that only the payload of the WAN media is compressed. In the case of X.25, packets can be correctly switched because the headers are not compressed. Cisco's payload compression uses the STAC algorithm, which is state-of-the-art in both compression ratios and processor efficiency. Compression ratios are data-dependent; they can be greater than 4:1, but are typically around 2:1.
- LAPB enhancements—The following significant LAPB enhancements are included in this release:
  - Modulo 128: This allows a larger window size to be configured on a link.
  - T4 timer: This allows a Receive Ready (RR) to be used as a keepalive to allow rapid link failure detection without relying on higher-layer routing protocols.
  - Hardware outage timer: This allows brief hardware outages to occur without requiring that the protocol be reset.
- IPXWAN on X.25—IPXWAN is not part of the RFC 1356 specification, but it is necessary for multivendor interoperability for IPX networks. IPXWAN is a link startup and negotiation protocol specified by Novell in RFC 1362.

Network Management Features

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

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

General Features

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

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

Important Notes

Warnings and cautions about using the Release 10.2 software are described in the following sections:

- Image Name Change
- Booting Cisco 2500 Series Access Servers
- Cisco 500-CS Jumpers
- IP Multicast and Mrouted
- Forwarding of Locally Sourced AppleTalk Packets
- Assigning DLCIs to Subinterfaces

Image Name Change

The name of the RAS+ feature set image has changed to *igs-c-l*. In previous releases, it was named *igs-cd-l*.

Booting Cisco 2500 Series Access Servers

Note that the booting process in the Cisco 2500 series access servers differs from the booting process on the ASM-CS and 500-CS platforms. On the ASM-CS and 500-CS platforms, you boot either from ROM or from a TFTP server. On the Cisco 2500 series platforms, you boot images from Flash memory or from a TFTP server.

To enable booting from Flash, enter configuration mode, specify a boot file name, and set the configuration register so that the system boots from Flash and the Break key is ignored:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
boot system flash [filename]
config-reg 0x2102
^Z
Router#
```

To copy a new image into Flash, you must first reboot from ROM and then copy the new image into Flash. You cannot copy a new image into Flash while the system is running from Flash.

The following commands set the system to reboot from ROM (note that the default gateways use boot ROMs and do not support IP routing):

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
config-reg 0x2101
IP default-gateway 131.108.2.1
^Z
Router#
```

The following example illustrates the sequence that occurs when you reboot the system from ROM:

```
Router# reload
%SYS-5-RELOAD: Reload requested
.
. The ROM image is booted here.
.
Press RETURN to get started!
Router(boot)> enable
Router(boot)# copy tftp flash
System flash directory:
File  name/status
```

```
  0   xxx/igs-bfpx.102-0.15
  [92836/4194304 bytes free/total]
IP address or name of remote host [255.255.255.255]? 131.108.1.111
Name of file to copy? igs-j-1.102-7
Copy igs-bfpx.102-current from 131.108.1.1 into Flash address space ?  [confirm] <Return>
92772 bytes available for writing without erasure.
Erase Flash address space before writing? [confirm] <Return>
Flash: verify/erasing bank 0 .. 00/01/02/03/04/05/06/07/08/09/10/11/12/13/14/15/
Loading from 131.108.1.111: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK -
 2697053/4194240 bytes]
Verify checksum...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
Verification successful: Length = 2697053, checksum = 0x74D0
```

The following commands modify the configuration register to set the system to reboot from Flash and cause the Break key to be ignored:

```
Router(boot)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
config-reg 0x2102
^Z
```

The following example illustrates the sequence that occurs when you reboot the system from Flash:

```
Router(boot)# reload
%SYS-5-RELOAD: Reload requested
.
. The Flash image is booted here
.
Press RETURN to get started!
```

Cisco 500-CS Jumpers

When you upgrade the EEPROMs to the *cs500-kr* image for Releases 9.21(1), 10.0(1), 10.2(1), or later, you need to install or move jumpers on the Cisco 500-CS system card. Table 6 indicates the locations of the jumpers for a system with four 4-MB PROMs and 10 MB of RAM. For more information, refer to the *Cisco 500-CS Memory and Software Upgrade Instructions* document.

Table 6 J3 and J4 Jumper Settings

Jumper	Place Jumpers on ...
J3 (selects 10-MB RAM)	Pins 1 and 2
J4 (selects 4-MB PROMs)	Pins 7 and 8 Pins 9 and 10 Pins 13 and 14

IP Multicast and Mrouted

Version 3.3 of mrouted, which was announced on August 26, 1994, has a multicast traceroute facility that does not work through Cisco routers. Cisco routers do have multicast tracing utilities that can be used to manage multicast internetworks.

Forwarding of Locally Sourced AppleTalk Packets

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

Assigning DLCIs to Subinterfaces

When using the **frame-relay inverse arp** command to assign a DLCI to a subinterface, the system does not retain the configuration and the **write terminal command** does not display the configuration. See the documentation for the **frame-relay interface-dlci** command for information about assigning multipoint subinterfaces.

Release 10.2(15) Caveats

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

ISO IGRP

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

SRB

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

Wide-Area Networking

- Combining a synchronous serial interface in a rotary dialer with Basic Rate Interfaces (BRIs) does not follow the bandwidth-on-demand load-sharing model. [CSCdi37048]
- If a serial interface is set to loopback via a hardware signal, the interface will remain in loopback until the hardware signal is dropped and a **no loopback interface** configuration command is issued. [CSCdi47768]

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

This section describes possibly unexpected behavior by Cisco IOS Release 10.2(14). These caveats apply to all 10.2 releases up to and including Release 10.2(14). For additional caveats applicable to Release 10.2(14), see the caveats section for Release 10.2(15), which precedes this section.

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

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

AppleTalk

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

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

Basic System Services

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

IBM Connectivity

- Sometimes when remote source-route bridging (RSRB) peers appear to be in an open or opening state, no traffic can pass through. Once the remote peer statements are removed and reconfigured, the peers will become operational. [CSCdi36072]
- Qualified Logical Link Control (QLLC) devices that are connected through a router using QLLC/Logical Link Control, type 2 (LLC2) conversion might occasionally experience poor response time. [CSCdi44923]

Interfaces and Bridging

- If a router configured for X.21 and acting as a data terminal equipment (DTE) device sets Control = OFF for any reason (such as interface resets) and frames exist on the Transmit circuit, the data communications equipment (DCE) device might go into a loop 2 or loop 3 condition. When X.21 is configured, the DTE device should not send any data if Control = OFF. [CSCdi45512]

IP Routing Protocols

- IP packets sent to the Hot Standby Router Protocol (HSRP) virtual MAC address are not received if the packet is Subnetwork Access Protocol (SNAP)-encapsulated and the receiving interface is part of the cBus or Switch Processor (SP) complex. [CSCdi39274]

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

This section describes possibly unexpected behavior by Release 10.2(13). Unless otherwise noted, these caveats apply to all 10.2 releases up to and including 10.2(13). For additional caveats applicable to Release 10.2(13), see the caveats sections for newer 10.2 releases. The caveats for newer releases precede this section.

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

IP Routing Protocols

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

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

This section describes possibly unexpected behavior by Release 10.2(12). Unless otherwise noted, these caveats apply to all 10.2 releases up to and including 10.2(12). For additional caveats applicable to Release 10.2(12), see the caveats sections for newer 10.2 releases. The caveats for newer releases precede this section.

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

IBM Connectivity

- When a Synchronous Data Link Control (SDLC) device is reloaded, the connection is not automatically reestablished. To reestablish the connection, issue the configuration commands **shut** and **no shut**. [CSCdi42369]
- If you configure a router for RSRB via direct encapsulation, the router will continually reboot while the remote router sends keepalives. The router will only come up if the connection between the two routers breaks, or if the remote router determines the link to be dead. [CSCdi45949]
- An incorrect timer reference causes explorer frames to be flushed on interfaces, even when the maximum data rate for explorers on the interface is not exceeded. [CSCdi47456]
- Low-end platforms will cache invalid Routing Information Field (RIF) entries when using any form of the **multiring** command. You can see these invalid entries in the data-link switching (DLSw) reachability cache. You might also observe loops within the LAN Network Manager (LNM). [CSCdi50344]
- When the command **fst** is used with RSRB, the router might suffer performance degradation and display the console message: [CSCdi50997]

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

- One or more SDLC-attached devices might fail to be polled. This failure will occur if an interface is defined for SDLC encapsulation and you add an SDLC address that is a lower value than any other SDLC address already defined on the interface. A workaround is to reload the router or to remove all SDLC address definitions and re-add them in ascending order. [CSCdi53646]
- In certain mixed-vendor bridge environments, the automatic spanning tree (AST) never becomes active if a Cisco device is the root bridge. Bridge protocol data units (BPDUs) are constantly exchanged, but the spanning tree topology never develops or becomes active. [CSCdi53651]

IP Routing Protocols

- A small delay occurs between the time Open Shortest Path First (OSPF) marks a link-state advertisement (LSA) as deleted and the time the LSA is actually removed. Within this small window, if OSPF receives an old copy of the LSA with a higher sequence number, OSPF cannot resolve the conflict and is unable to remove the LSA. The old LSA copy is most likely received from some new neighbors through database exchange. You will observe a self-originated LSA stuck in the database. [CSCdi48102]
- Packet corruption might occur when fast-switching IP packets from ATM interfaces to Token Ring interfaces configured with the **multiring** command. [CSCdi49734]
- If you use regular expressions longer than 59 characters in the **ip as-path access-list** configuration command, the router will reload. [CSCdi53503]

ISO CLNS

- Issuing a Connectionless Network Service (CLNS) ping to one of the router's own addresses will cause the router to reload if **debug clns packet** is on. The workaround is to not have this particular debug on if you need to ping to one of the router's own addresses. [CSCdi50789]

Wide-Area Networking

- If chat script operations fail over asynchronous interfaces, a reload might occur during later operations because data was left in an inconsistent state. [CSCdi47460]
- Groups of 4 ports on a Cisco 2511 might have data set ready (DSR) behaving in unison to a single stimulus. Reloading the router is the only workaround. [CSCdi49127]

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

This section describes possibly unexpected behavior by Release 10.2(11). Unless otherwise noted, these caveats apply to all 10.2 releases up to and including 10.2(11). For additional caveats applicable to Release 10.2(11), see the caveats sections for newer 10.2 releases. The caveats for newer releases precede this section.

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

AppleTalk

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

Basic System Services

- Available memory will slowly decrease on a router that is bridging IP and that has more than one interface with the same IP address. [CSCdi44023]

DECnet

- DECnet Phase IV-to-Phase V conversion might introduce incorrect area routes into the ISO Interior Gateway Routing Protocol (IGRP), if there are DECnet L2 routes on the DECnet side. These area routes show up as "AA00" and are propagated to other routers. [CSCdi47315]

IBM Connectivity

- When source-route transparent (SRT) bridging is configured on the router, calls to management functions that are related to source-route bridging (SRB) might not work correctly. [CSCdi42298]
- When a front-end processor (FEP) initiates a Qualified Logical Link Control (QLLC) connection, a virtual circuit is established, but the exchange identification (XID) negotiation never proceeds to completion. The router sends XID responses as commands, rather than as responses. [CSCdi44435]

- A router might crash if running QLLC and using remote source-route bridging (RSRB) over a serial line to provide the Logical Link Control, type 2 (LLC2) connection from QLLC to an end station or host. The crash only occurs if multiple changes are made to the encapsulation type on the RSRB serial line. [CSCdi45231]
- If a router receives a 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 OSPF might reload when configuring a controller T1 with a channel-group time-slot assignment. [CSCdi43083]
- Attempts to route Internetwork Packet Exchange (IPX) packets by Routing Information Protocol (RIP) or by Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) might fail on primary serial interfaces. Failure can occur when the subinterfaces were configured for IPX routing before their primary interface was. [CSCdi44144]
- Enhanced IGRP might announce IP summary routes that have the metric value set too high. This can make the applicable networks unreachable. [CSCdi46290]

Novell IPX, XNS, and Apollo Domain

- If **ipx sap-incremental** is configured, a router may end up with fewer service access point (SAP) entries than actually exist if the interface goes down and then comes back up. This problem occurs more often when there are many SAP entries in the network environment. [CSCdi46224]
- When an enhanced IGRP route is advertised back into Routing Information Protocol (RIP) the delay within the enhanced IGRP cloud is not properly taken into account in the tics value of the route when it is redistributed into RIP. The RIP-advertised route appear to be closer than it really is. [CSCdi49360]
- If IPX Enhanced IGRP is running, the command sequence **interface serial** / **no ipx network** / **no ipx routing** may cause the router to reload. [CSCdi49577]

VINES

- VINES servers located downstream might unexpectedly lose routes that were learned via Sequenced Routing Update Protocol (SRTP). This behavior results from improper handing of network sequence numbers by the system. Issuing a **clear vines neighbor** or disabling SRTP are suggested workarounds. [CSCdi45774]
- Vines SRTP on serverless segements with 10.3(8) IOS is not sending the redirect to the correct network number (layer 3) address. Workaround is to shut off Vines redirects on the serverless segment interface. Sniffer trace of this packet will show an "abnormal end of Vines SRTP." [CSCdi50536]

Wide-Area Networking

- When routing an X.25 call request packet containing a Calling/Called Address Extension facility, sometimes the Calling/Called Address Extension facility is inadvertently modified. [CSCdi41580]

- With **encap lapb** or **encap X25** configured, sometimes the command **lapb N1 xxx** disappears from the working configuration and N-1 falls back to the default. This problem is most likely to occur after an interface reset or a reload. [CSCdi44422]
- Doing a **no dialer-list** followed by a **dialer-list** will cause the router to crash and reboot. [CSCdi45951]

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

This section describes possibly unexpected behavior by Release 10.2(10). Unless otherwise noted, these caveats apply to all 10.2 releases up to and including 10.2(10). For additional caveats applicable to Release 10.2(10), see the caveats sections for newer 10.2 releases. The caveats for newer releases precede this section.

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

AppleTalk

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

IBM Connectivity

- When an SDLLC or QLLC virtual ring is configured, explorers may be incorrectly forwarded to the interface corresponding to the 3rd ring in the routing information field (RIF). [CSCdi43378]
- On low-end systems for a DTE router interface, after a router reload, SDLC packets are identified as HDLC packets by the serial driver until a **shut/no shut** command is performed for the interface. This causes occassional packet drops without any trace, if the byte pattern happens to match that of other protocols. This can also cause serious performance problems. [CSCdi43686]
- SRB bridged packets might be dropped when the router is configured for RSRB direct, and priority/custom queueing is enabled on the output Serial interface. A workaround is to disable priority/custom queueing on the Serial interface. [CSCdi44430]

Interfaces and Bridging

- The serial interface on Cisco 2500 series routers will enter a looped state if it is configured as a backup DTE interface, and if the cable is disconnected and reconnected a few times. A **clear interface** command fixes the problem. [CSCdi32528]

VINES

- A Sequenced Routing Update Protocol (SRTP) update sent in response to a client request for specific networks will omit the last network specified in the request. [CSCdi44517]
- Under unusual circumstances, configuring an interface for LAPB or X.25 might cause the router to become unresponsive, requiring it to be reloaded. [CSCdi42803]
- Hardware flow control may be inadvertently disabled on the Cisco 2509, 2510, 2511 and 2512 routers' asynchronous ports after issuing a **configure network** or a **copy tftp running-config** command. To restore flow control, issue the line configuration command **flowcontrol hardware** on all lines. [CSCdi43306]

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

This section describes possibly unexpected behavior by Release 10.2(9). Unless otherwise noted, these caveats apply to all 10.2 releases up to and including 10.2(9). For additional caveats applicable to Release 10.2(9), see the caveats sections for newer 10.2 releases. The caveats for newer releases precede this section.

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

Basic System Services

- Memory may become corrupted when servicing MacIP ATP packets, causing a system reload. [CSCdi41076]

IBM Connectivity

- The SNA packet is lost during fragmentation if no buffer is available to store the fragmented packet. The SNA application will recover and resend the packet without disconnecting the session. [CSCdi27730]
- Fast Sequenced Transport (FST) performs poorly when running over serial lines. [CSCdi41846]
- After configuring an LNM PC with a bridge definition that contains the target interface MAC addresses on the router, 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 defining the target LNM server bridge on the LNM PC. [CSCdi41997]
- In very rare circumstances the router may reload after a **show lnm station** command is entered and part of the output has been displayed. This might happen if the router is attached to Token Ring(s) that are in great distress and experiencing serious error conditions at the time the command is entered. [CSCdi39483]
- In rare cases, the router's serial interface driver software will drop SDLC frames with bit patterns identical to HDLC LEX frames. This problem has been observed on interfaces using STUN-basic encapsulation with non-IBM SNA data traffic (for example, COMM10 CNS protocol). There is no indication in the router when this problem occurs. The router does not increment the interface "drop" counter or the STUN "drop" counters. Detection is only possible with a media tracing tool. [CSCdi41558]
- The Find Name NetBIOS broadcast is sent from all the Token Ring interfaces even though the proxy-explorer and NetBIOS name caches are configured on the interface. To workaround, run backlevel software. [CSCdi41972]

Interfaces and Bridging

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

IP Routing Protocols

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

ISO CLNS

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

Wide-Area Networking

- Cisco 2509 through Cisco 2512 routers' asynchronous lines stop accepting input under certain conditions. One of these conditions occurs when a user connected to a LAT host types a Control-C character. A **clear line x** or a change to the line parameters will cause the line to start accepting input again. [CSCdi40994]
- When using DTR dialing and PPP encapsulation, DTR does not stay "low" after the call is disconnected. [CSCdi39576]
- In rare circumstances, an SDLLC connection failure can cause the router to reload. [CSCdi39832]

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

This section describes possibly unexpected behavior by Release 10.2(8). Unless otherwise noted, these caveats apply to all 10.2 releases up to and including 10.2(8). For additional caveats applicable to Release 10.2(8), see the caveats sections for newer 10.2 releases. The caveats for newer releases precede this section.

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

AppleTalk

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

IBM Connectivity

- NetBIOS connections occasionally fail to connect through remote source-route bridging when local acknowledgment is enabled. The workaround is to disable local acknowledgment. [CSCdi37525]

Interfaces and Bridging

- On the BRUT partner product (a Cisco 2500 variant developed with DEC), when an Ethernet interface goes down, the output of a **show interface** command still shows the interface as being up. The SNMP replies are also incorrect. [CSCdi37135]

IP Routing Protocols

- When the Enhanced IGRP process receives a hello packet from a neighbor, it tries to send an update packet, but this process of sending an update packet can be suspended by the EIGRP process. When the 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 peer (neighbor) could have been erased, which confuses the Enhanced IGRP process and results in the generation of wrong bus address. [CSCdi35257]
- In a misconfigured or malfunctioning Token Ring bridging environment, pinging the Hot Standby Router Protocol (HSRP) virtual IP address can cause the ICMP echo request packets to be massively replicated. [CSCdi38170]
- Static routes are not being redistributed into Enhanced IGRP after a **clear ip route *** command is issued. A workaround is to kick-start the redistribution process by either removing one static route and reinstalling it, or by removing and reinstalling the **redistribute static** command under the **router eigrp** *xx* command. [CSCdi38766]

TCP/IP Host-Mode Services

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

VINES

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

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

This section describes possibly unexpected behavior by Release 10.2(7). Unless otherwise noted, these caveats apply to all 10.2 releases up to and including 10.2(7). For additional caveats applicable to Release 10.2(7), see the caveats sections for newer 10.2 releases. The caveats for newer releases precede this section.

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

Basic System Services

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

IBM Connectivity

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]

- The following error messages my result in a router reload or loss of session when using local-ack:

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

  [CSCdi34930]

DECnet

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

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**

  These commands set values for the interpacket gap in Flash and poison RIP/SAP updates for each interface. Values override the **ipx output-rip-delay** and **ipx output-sap-delay** settings. If a large normal interpacket gap is configured, the setting should be small values. [CSCdi34411]

VINES

- Occasionally, some X.25 data packets might have the D bit set incorrectly, causing a connection to be reset. [CSCdi35036]

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

This section describes possibly unexpected behavior by Release 10.2(6). The caveats listed here describe only the serious problems. For the most current list of caveats against this release, access CIO 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 10.2(7).

AppleTalk

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

Basic System Services

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

IP Routing Protocols

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

Protocol Translation

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

TCP/IP Host-Mode Services

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

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

This section describes possibly unexpected behavior by Release 10.2(5). The caveats listed here describe only the serious problems. For the most current list of caveats against this release, use the documentation CD-ROM or access CCO as described in the section "Cisco Connection Online" later in this document.

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

AppleTalk

- The following error messages and trace back are displayed on the console of a router configured with AppleTalk over SMD:

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

  If this message is displayed, contact Cisco Systems and include the text and the traceback of this message and the information from the **show version** command. As a workaround solution, you can try using non-extended addressing on SMDS [CSCdi29127]

- A slow memory leak occurs when AppleTalk Enhanced IGRP is enabled. [CSCdi30641]

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

Basic System Services

- SLARP can cause routers with dual Flash bank to reload. [CSCdi30588]

IP Routing Protocols

- Issuing the [**no**] **ip summary-address** can cause the router to reload. [CSCdi23646]
- If an interface is configured with an IP secondary address and the **ip access-group in** command, the router will not respond to pings or Telnets directed to the interface secondary address if the ping or Telnet comes into the router on an interface other than the interface configured with the **ip access-group in** command. [CSCdi30011]
- Routes are not distributed between different IP and Enhanced IGRP processes. This problem occurs only when you enter certain commands, such as **clear ip route ***, **ip address**, **transmit-interface**, and **mtu interface**. The workaround is either to retype the redistribute router commands or to reload the configuration file either from NVRAM or over the network, depending on the location of the configuration file.[CSCdi30575]

Protocol Translation

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

Wide-Area Networking

- PVCs do not work over an X.25 remote switching (XOT) connection. [CSCdi27337]
- The **x25 route** command requires that an option **xot-source** takes an interface name as a parameter. This causes XOT TCP connections to use the IP address' specified interface as the source address of the TCP connection, which allows the connection to move to a backup interface without terminating the TCP session. [CSCdi28892]
- If an asynchronous line is configured with the **script reset** command, the chat process that runs the script can continue indefinitely without terminating. [CSCdi29975]
- The X.25 default protocol command—**x25 default** {**ip** | **pad**}—does not work. [CSCdi30318]
- DDN and BFE modes do not encode the needed local facilities when originating a call. [CSCdi31252]

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

This section describes possibly unexpected behavior by Release 10.2(4). The caveats listed here describe only the serious problems. For the most current list of caveats against this release, use UniverCD or access CIO as described in the section "Cisco Connection Online" later in this document.

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

AppleTalk

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

Basic System Services

- The router cannot detect a shortage of buffer elements and thus does not create new ones. This situation causes the router to drop packets even though an ample packet buffers exist. The **show buffers** command output shows many buffer element misses. [CSCdi29379]
- If a system is set to be an NTP master, eventually other systems will refuse to synchronize to it. There is no workaround. [CSCdi30293]

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]

Interfaces and Bridging

- When you use Flash load helper to copy a new image into Flash memory, the system might return to the system image without carrying out the copy request. This behavior occurs when the length of the source and destination filenames causes a buffer to overflew. The buffer can hold only 56 characters, not including null terminators, and it can hold only 54 characters when Flash memory is partitioned into multiple partitions. You can detect the failure with the **show flh-log** command. If the copy fails, the **show flh-log** command output shows that a new image was not copied to Flash memory. This output can vary because the effects of buffer overflow are unpredictable. To prevent this problem from occurring, make sure that source and destination filenames each contain fewer than 28 ASCII characters, or 26 ASCII characters if your Flash memory is partitioned. [CSCdi26920]

IP Routing Protocols

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

Novell IPX, XNS, and Apollo Domain

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

TCP/IP Host-Mode Services

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

Wide-Area Networking

- DTR dialing does not work with PPP encapsulation. Even though the console shows the line going up and down, no traffic goes through, and the serial interface is still spoofing. To work around this problem, use HDLC or X.25 encapsulation. [CSCdi29249]
- When reverse Telnet is used in certain traffic-loading conditions on asynchronous lines—generally, an asynchronous line with receive and transmit looped—garbage characters may be output on the line. [CSCdi29696]
- If you are using PPP LQM and the far side of the connection stops replying, the router does not detect that the link has failed. The workaround is not to use PPP LQM by not issuing the **ppp quality** command. [CSCdi30042]
- If an ASM asynchronous interface is configured with the **flowcontrol hardware in** command, the CTS line does not honor the flow control request. To provide correct operation, issue the **flowcontrol hardware** command. [CSCdi30054]

Release 10.2(2) Caveats/Release 10.2(4) Modifications

This section describes possibly unexpected behavior by Release 10.2(2). The caveats listed here describe only the serious problems. For the most current list of caveats against this release, use UniverCD or access CIO as described in the section “Cisco Connection Online” later in this document.

Note that for the access and communication servers, Release 10.2(3) was skipped.

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

Basic System Services

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

Communication Server

- Under rare circumstances, a 500-CS line configured for hardware flow control might become locked. This condition can prevent the next user of the line from seeing any response from the Cisco 500. [CSCdi27906]

TCP/IP Host-Mode Services

- The source IP address validation performed by the rsh server can fail when the IP address name specified via the **ip host** command is not in DNS. A side effect is that the static host mapping is deleted. [CSCdi28424]

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

This section describes possibly unexpected behavior by Release 10.2(1). The caveats listed here describe only the serious problems. For the most current list of caveats against this release, use UniverCD or access CIO as described in the section "Cisco Connection Online" later in this document.

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

AppleTalk

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

Access Server

- A router or communication server can spontaneously reload while attempting to hang up a line configured with the **autohangup** command once the last network connection on the line is closed. This crash happens only if the last connection was resumed with the **resume** EXEC command. [CSCdi24025]
- The communication server leaks memory if the **nohangup** keyword of the **username** global configuration command is used to define special username entries. [CSCdi25520]
- On the Cisco 2509, Cisco 2510, Cisco 2511, and Cisco 2512 routers, asynchronous lines set with BREAK as the escape character require an additional character to be sent before a prompt is displayed. [CSCdi25768]

EXEC and Configuration Parser

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

IP Routing Protocols

- When you are load-balancing IP traffic over multiple equal-cost paths, the system's routing table might reach an inconsistent state, leading to a system reload. Before the inconsistent state is reached, the system must have three or four equal-cost paths for a particular route. A routing update must then be received that causes the system to replace those paths with fewer (but still more than one), better metric paths. This route must then become used for further locally generated traffic. This problem is most likely to be seen after an interface flap (that is, after an interface's line state goes from up to down to up again) in an environment where redundant, but not symmetric, interconnections exist between routers. The problem also seems more likely in FDDI environments, where interfaces flap before fully coming up. These flaps can result in multiple back-to-back routing table changes. [CSCdi20674]

- If you are using candidate default routes in IP Enhanced IGRP, be aware that a backwards compatibility problem exists between Cisco software versions earlier than Release 9.21(4.4), Release 10.0(4.1), Release 10.2(0.6) and later versions. Upgrade all routers to Release 9.21(4.4), Release 10.0(4.1), and Release 10.2(0.6) or later.

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

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

  A complete fix to the backwards compatibility problem is available as of Releases 10.0(4.7), 10.2(0.11), and 9.21(5.1). Routers running a version older than those versions will still be unable to mark Enhanced IGRP internal routes as candidate default routes. [CSCdi23758]

- Pings to secondary addresses fail if the secondary address is configured on an interface different from the one on which the packets arrive. In this case, the secondary address is mistakenly added to the IP route cache, which causes the problem. The workaround is to use the **no ip route-cache** command to disable fast switching on the interface that has the secondary address configured. [CSCdi26022]

- Packets with a time-to-live (TTL) value of 128 or greater whose TTL values are checked on systems with 68000 processors are rejected with the message “ICMP Time Exceeded.” The cases that are not affected are SSE switching, autonomous switching, and most high-end fast switching (TTL checked by microcode). The case that is affected is switching on low-end routers. Notably, our ping and Telnet implementations send packets with a TTL of 255. Normal hosts generally use a smaller TTL. [CSCdi26799]

Novell IPX

- The IPX Enhanced IGRP **distribute-list** command allows standard access lists only (access lists whose numbers are 800 through 899). It should also allow extended access lists (numbers from 900 through 999). [CSCdi25895]

- IPX SAP/ISO encapsulation frames over Token Ring on a CTR or Cisco 7000 that are being sent to an FSIP or HSSI interface are corrupted if the Token Ring frames contain a Routing Information field. To work around this problem, either run SNAP encapsulation on the Token Ring, or issue the **no ipx route cache** command on the serial interface. [CSCdi26154]

Protocol Translation

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

Wide-Area Networking

- The X.25 software typically does not encode the address or facility information in a Call Accepted/Call Connected packet, some X.25 equipment rejects with a “packet too short” diagnostic (38). [CSCdi21201]

- Dial-on-demand PPP connections to any router sending an IPCP request with an IP address of 0.0.0.0 do not work. The workaround is to have the non-Cisco router propose a valid IP address in its IPCP packet. [CSCdi22160]
- Under very high traffic loads (indicated by a high packet loss rate shown in the "output drops" field), PPP Echo Reply packets are not transmitted, and the remote router declares the line down. In the case of DDR connections, the call is taken down. To work around this problem, use priority queueing and assign the heavy load traffic to the low, normal, or medium queue. [CSCdi22420]
- X.25 calls with a null destination address that are directed to the router are denied with cause 0, diag 67. [CSCdi23975]
- When IPX is used over PPP, if the node number is negatively acknowledged, the software continues to ask to negotiate it. [CSCdi24078]
- The Frame Relay broadcast queue might exhibit drops under high broadcast volume. "Buffer element" misses increase at the same time the drops happen. [CSCdi25707]

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

CD-ROM Documentation

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

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

9611R