CISCO SYSTEMS

Doc. No. 78-1817-17

Access and Communication Servers Release Notes for Cisco IOS Release 10.3

September 23, 1996

These release notes describe the *new* features, modifications, and caveats for Cisco Internetwork Operating System (Cisco IOS) Release 10.3, up to and including Release 10.3(15). They include all access and communication server features and protocol translation features.

Cisco IOS Release 10.3(15) and all subsequent 10.3 releases are deemed “Generally Deployable.” Cisco believes Release 10.3 is suitable for deployment anywhere in the network where the features and functionality of the release are required.

Introduction

These release notes discuss the following topics:

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

Documentation

For printed documentation of Cisco IOS Release 10.3 access and communication server software features, refer to the Cisco IOS Release 10.3 *Access and Communication Servers Configuration Guide Addendum* and *Access and Communication Servers Command Reference Addendum*. These addenda include Release 10.3 features and supplement the information in the following manuals:

- Release 10 *Access and Communication Servers Configuration Guide*
- Release 10 *Access and Communication Servers Command Reference*

The configuration guide and command reference addenda are divided into eight main parts. Seven parts match the parts in the Release 10 *Access and Communication Servers Configuration Guide* and *Access and Communication Servers Command Reference*. The eighth part contains chapters covering new technology areas.

Electronic documentation of Release 10.3 access server software features, is available on Cisco Connection Documentation, Enterprise Series CD-ROM, formerly UniverCD. Refer to the Cisco IOS Release 10.3 *Access and Communication Servers Configuration Guide* and *Access and Communication Servers Command Reference* publications, which are located in the Cisco IOS Release 10.3 database. (Note that the two addenda are not separate documents on the CD, because the information in them has been incorporated into the electronic documents.)

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

You can also access Cisco technical documentation on Cisco Connection Online (CCO), formerly Cisco Information Online (CIO), as described at the end of this document. CCO can be found on the World Wide Web (www) at URL http://www.cisco.com.

Platform Support

Cisco IOS Release 10.3 supports the following access and communication server platforms:

- ASM-CS
- 500-CS
- Cisco 2500 series (Cisco 2509, Cisco 2510, Cisco 2511, and Cisco 2512)
- Cisco AS5100 access server

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

Table 1 Interfaces Supported

Interface	ASM-CS	500-CS	Cisco 2500 Series	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	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	No	No
ISDN PRI	No	No
G.703/G.704	No	No

Cisco IOS Software Feature Sets

The Cisco IOS software is available in different feature sets depending upon the platform. Table 3 lists the feature sets for the Cisco 2500 series and the Cisco AS5100.

Table 3 Cisco 2500 Series and AS5100 Software Feature Sets

	Feature Set							
Feature	**IP**	**IP/IBM Base**	**IP/IPX**	**IP/IPX/ IBM Base**	**Desktop**	**Desktop/ IBM Base**	**Enterprise**	**Remote Access Server**
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
IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NHRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ES-IS	—	—	—	—	—	—	Yes	—
IS-IS	—	—	—	—	—	—	Yes	—
Snapshot routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transparent and translational bridging	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—
Multiring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN extension host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—
IPX	—	—	Yes	Yes	Yes	Yes	Yes	Yes
NLSP	—	—	Yes	Yes	Yes	Yes	Yes	—
IPXWAN 2.0	—	—	Yes	Yes	Yes	Yes	Yes	Yes
AppleTalk Versions 1 and 2	—	—	—	—	Yes	Yes	Yes	Yes
AURP	—	—	—	—	Yes	Yes	Yes	Yes
DECnet IV	—	—	—	—	Yes	Yes	Yes	Yes
DECnet V	—	—	—	—	—	—	Yes	—

	Feature Set							
Feature	IP	IP/IBM Base	IP/IPX	IP/IPX/ IBM Base	Desktop	Desktop/ IBM Base	Enterprise	Remote Access Server
Apollo Domain	—	—	—	—	—	—	Yes	—
Banyan VINES	—	—	—	—	—	—	Yes	—
ISO CLNS	—	—	—	—	—	—	Yes	—
XNS	—	—	—	—	—	—	Yes	—
Source-route bridging (SRB) and remote source-route bridging (RSRB)	—	Yes	—	Yes	—	Yes	Yes	—
DLSw+	—	Yes	—	Yes	—	Yes	Yes	—
SDLC	—	Yes	—	Yes	—	Yes	Yes	—
SDLLC	—	Yes	—	Yes	—	Yes	Yes	—
STUN	—	Yes	—	Yes	—	Yes	Yes	—
TG/COS	—	—	—	—	—	—	Yes	—
DSPU	—	—	—	—	—	—	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
DHCP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Boot ROM Requirements

Boot ROM versions and system images are independent of each other. Table 4 lists the default boot ROM level that ships with the Cisco 2500 platform. This level contains the latest features and supports all current hardware and software features. If you require a newer boot ROM, refer to Table 5, which lists the available upgrades.

Table 4 Default Boot ROM Level

Platform	Boot ROM Level
Cisco 2509 through Cisco 2512	10.2(8a)

Table 5 Available Boot ROM Upgrade

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

Memory Requirements

Beginning with Cisco IOS Release 10.3, the Cisco software image size exceeds 4 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 the Cisco communication servers to take advantage of the Release 10.3 features, you must upgrade the code or main system memory as listed in Table 6. Some platforms have specific chip or architecture requirements that affect what can be upgraded and in what increments.

Table 6 Cisco IOS Release 10.3 Memory Requirements

Platform	Required Code Memory	IBM Base Option	Required Main Memory	IBM Base Option	Release 10.3 Runs from
ASM-CS	—	—	16 MB RAM	—	RAM
500-CS	—	—	10 MB RAM	—	RAM
Cisco 2500 Series					
IP Set	4 MB Flash	4 MB Flash	4 MB RAM	4 MB RAM	Flash
IP/IPX Set	4 MB Flash	8 MB Flash	4 MB RAM	4 MB RAM	Flash
Desktop Set	4 MB Flash	8 MB Flash	4 MB RAM	4 MB RAM	Flash
Enterprise Set	8 MB Flash	—	6 MB RAM	—	Flash
Remote Access Server	4 MB Flash	—	4 MB RAM	—	Flash
AS5100[1]					
IP Set	4 MB Flash	4 MB Flash	6 MB RAM	6 MB RAM	Flash
IP/IPX Set	4 MB Flash	8 MB Flash	6 MB RAM	6 MB RAM	Flash
Desktop Set	4 MB Flash	8 MB Flash	6 MB RAM	6 MB RAM	Flash
Enterprise Set	8 MB Flash	—	6 MB RAM	—	Flash
Remote Access Server	4 MB Flash	—	6 MB RAM	—	Flash

[1] Memory requirements listed are per card. Each Cisco AS5100 supports up to three cards so that the maximum memory needed for any Cisco AS5100 is three times the listed number.

New Software Features in Release 10.3(4)

This section describes new features and enhancements in Release 10.3(4) of the access and communication servers software.

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

Cisco AS5100 Access Server

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 Software Features in Release 10.3(3)

This section describes new features and enhancements in Release 10.3(3) of the access and communication servers software.

System Management

- Buffer management—The buffer cache that was shared by all the public buffer pools has been removed. Instead, each interface buffer pool has its own buffer cache. A new buffer size exists, and the **show buffers** output is enhanced.
- AAA/TACACS+—This latest version of Terminal Access Controller Access Control (TACACS) combines enhanced functionality and new authentication, authorization, and accounting (AAA) features.
- Configure synchronization of logging messages—You can configure the system to synchronize unsolicited messages and **debug** output with solicited communication server output and prompts for a specific line.

Interfaces

- Dynamic Host Configuration Protocol (DHCP)—DHCP manages a group of IP addresses that are dynamically allocated to users logging in on asynchronous lines using SLIP or PPP. After the connection is terminated, the address is recycled into the address pool to be used again.
- Stacker compression over LAPB.—Cisco now supports Stacker compression over Link Access Protocol, Balanced (LAPB) or multi-LAPB encapsulation, in addition to the previously supported predictor-algorithm compression. Stacker compression is recommended when the bottleneck is line bandwidth.

Routing Protocols

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

- BGP COMMUNITIES attribute—To facilitate and simplify the control of routing information in BGP, destinations can be grouped into communities upon which routing decisions can be based.
- IP multicast routing—The communication server can be configured to forward IP multicast traffic.

Wide-Area Networking

- Snapshot routing—The communication server can learn routes dynamically and keep the routes available for a specified period, even through routing updates are not exchanged during that period.
- DDR over LAPB—You can customize a DDR network to support LAPB encapsulation for various types of interfaces.
- DDR over X.25—You can customize a DDR network to support X.25 encapsulation for various types of dialers.
- Dialer hold queue—You can configure a hold queue that can prevent interesting packets from being dropped as a modem connection is being established.

New Software Features in Release 10.3(1)

This section describes new features and enhancements in the initial Cisco IOS Release 10.3 of the access and communication servers software.

Access Servers

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

- UNIX line printer daemon—This feature allows devices on a LAN that supports the UNIX line printer daemon (lpd) to send print jobs to a printer directly attached to an access server. This feature implements the queuing function of the UNIX lpdin software on the access server.
- TN3270 enhancements—The TN3270 terminal emulation support is more adaptable, easier to use, and able to support new features. This new implementation is a UNIX-style TN3270 with enhanced graphics and three logical modules: Telnet, the TN3270 emulation, and screen output routines. Features include data stream commands and data stream orders, Yale extensions, 7171-style transparent mode, structured fields, Kermit file transfers through transparent mode, and IBM-3179-2 terminal keyboard support. Attributes include foreground color, extended highlighting (underline, reverse video, flashing) and EBCDIC character sets.
- PPP/SLIP protocol translation on virtual terminals—This enhancement to the protocol translation software allows a user on a Telnet, X.25 PAD, or LAT terminal server to make an appropriate connection to an access server running protocol translation and then run SLIP or PPP for packet-oriented traffic.
- Asynchronous mobility—Asynchronous mobility allows mobile users with modems to connect to their private networks via a public network. Asynchronous mobility supports most remote node protocols in the first version. This means a mobile user can connect to an IPX private network using a public network that supports only IP protocols. The public network can be either a large corporate network or the Internet.
- Enable password—This feature allows you to specify an additional layer of security over the **enable password** command, first by enforcing the use of two passwords, and then by storing the **enable secret** using a nonreversible cryptographic function.

Backbone Protocol Routing Features

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

IP Features

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

- Next Hop Resolution Protocol (NHRP)—Access servers and hosts can use NHRP to discover the addresses of other access servers and hosts connected to a nonbroadcast, multiaccess (NBMA) network. NHRP provides an ARP-like solution whereby systems attached to an NBMA network can dynamically learn the addresses of the other systems that are part of that network. These systems can then directly communicate without requiring traffic to use an intermediate hop.
- Virtual private network—NHRP can be used to facilitate building a virtual private network. In this context, a virtual private network consists of a virtual Layer 3 network that is built on top of an actual Layer 3 network. The topology you can use over the virtual private network can be largely independent of the underlying network, and the protocols you run over it can be completely independent of it.
- Hot Standby Router Protocol (HSRP) enhancements—HSRP now allows multiple access servers on a LAN to provide fast backup for each other. Another new HSRP feature is the ability to configure an access server so that its Hot Standby priority changes based on the availability of its interfaces.
- BGP COMMUNITIES attribute—To facilitate and simplify the control of routing information in BGP, destinations can be grouped into communities upon which routing decisions can be based.
- Flexible netmask display—IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. This feature allows you to display the netmask in dotted decimal, hexadecimal, or bitcount format.
- Offset to routing metrics enhancement—You can now limit an offset list to a particular interface or apply an access list to it. An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP and IGRP.
- IP extended access list enhancements—Improvements include the following:
    - The **established** keyword is now independent of port number filtering. Previously, you could not use **established** and filter on a port number. This enhancement allows more granularity in the use of **established**.
    - Port filtering and the **established** keyword are no longer presented as options during configuration unless they are applicable.
    - The Cisco IOS software now recognizes many names for TCP and UDP port numbers (for example, FTP, gopher, and talk).
    - The keyword **any** is now an abbreviation for "0.0.0.0 255.255.255.255" in standard and extended access lists.
    - Port filtering now supports filtering on a range of port numbers.
    - ICMP messages can be filtered on type and code. In addition, the Cisco IOS software now recognizes the names of all ICMP messages, so these can also be specified by name as well as number.
    - IGMP messages can now be filtered by message type (number) or message name (DVMRP, host-query, host-report, PIM, and trace).

- — Packets can now be filtered by precedence level. Levels can be selected by name or number. Known names are critical, flash, flash-override, immediate, internet, network, priority, and routine.
- — When IP extended access lists are used to control access to and from access server services (for example, **access-class 101 in**), ICMP, IGMP, precedence, and type of service filtering are not performed.
- — You can now filter on source ports for TCP and UDP using all of the same operators as destination ports.
- — The protocols Enhanced IGRP, ipinip (IP in IP), and OSPF are now known to the parser. Previously, you had to use explicit protocol numbers.

- A **show ip access-list** command has been added. Its output is identical to **show access-list**, but is IP specific and allows you to specify a particular access list. With no argument, it displays all simple and extended IP access lists.

Desktop Protocol Features

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

AppleTalk Features

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

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

Novell IPX Features

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

- NetWare Link Services Protocol (NLSP)—NLSP is a link-state routing protocol based on the OSI IS-IS protocol. Cisco's implementation of NLSP also includes NLSP MIB variables and tools to redistribute routing and SAP information between NLSP and other IPX routing protocols such as RIP, SAP, and Enhanced IGRP.
- IPXWAN Version 2.0—Our access servers support IPXWAN Version 2.0 as defined in RFC 1634. The major enhancements to IPXWAN Version 1.0 are the ability to negotiate the use of NLSP and support for unnumbered IPX links. IPXWAN Version 2.0 is supported over permanent serial lines, X.25 switched and permanent virtual circuits, and Frame Relay permanent virtual circuits.
- IPX floating static routes—Static routes are traditionally implemented to always take precedence over any dynamically learned routes to the same destination network. A floating static route is a statically configured route that can be overridden by dynamically learned routing information. Thus, a floating static route can be used to create a path of last resort that is used only when no dynamic information is available.

Wide-Area Networking Features

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

Frame Relay Feature

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

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

X.25 and LAPB

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

- LAPB priority queuing.

Network Management Features

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

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

Important Notes

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

- Upgrading to a New Software Release
- Using Candidate Default Routes in IP Enhanced IGRP
- IP Multicast and Mrouted
- Forwarding of Locally Sourced AppleTalk Packets
- Using Source-Route Transparent Bridging (SRT) and Source-Route Bridging (SRB) on Cisco 2500 Access Servers

Upgrading to a New Software Release

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

Using Candidate Default Routes in IP Enhanced IGRP

If you are using candidate default routes in IP Enhanced IGRP, there is a backwards compatibility problem between Cisco versions earlier than Releases 9.21(4.4), 10.0(4.1), 10.2(0.6), and later Cisco versions. Upgrade all access servers to Releases 9.21(4.4), 10.0(4.1), and 10.2(0.6) or later.

The problem is as follows: When access servers running the later versions are directly attached with neighbors running the earlier version, some Enhanced IGRP internal routes appear as candidate default routes to the access servers running the later version. This can cause the gateway of last resort to be set incorrectly. 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 can loop.

A candidate default route is a route that is tagged as the default route. An access server 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 with Releases 10.0(4.7), 10.2(0.11), and 9.21(5.1). Access servers running a version older than those versions are unable to mark Enhanced IGRP internal routes as candidate default routes.

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 access servers. Cisco access servers do have multicast tracing utilities that can be used to manage multicast internetworks. An interoperable solution will be provided in an early maintenance release of Cisco IOS Release 10.3.

Forwarding of Locally Sourced AppleTalk Packets

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

Using Source-Route Transparent Bridging (SRT) and Source-Route Bridging (SRB) on Cisco 2500 Access Servers

Certain products containing a particular revision of Token Ring controllers do not support source-route transparent bridging (SRT). SRT is the concurrent operation of source-route bridging (SRB) and transparent bridging on the same interface. The issue is confined to products containing the Texas Instruments TMS380C26 Token Ring controller. The affected products, shipped between March 30, 1994 and January 16, 1995, are the Cisco 4000 NP-1R, Cisco 4000 NP-2R, Cisco 2502, Cisco 2504, Cisco 2510, Cisco 2512, Cisco 2513, and Cisco 2515.

Units shipped before March 30, 1994 or after January 16, 1995 are not affected. They use the TI TMS380C16 Token Ring controller, which supports SRT.

SRT support is necessary in two situations. In one, Token Ring networks are configured to source-route bridge protocols such as SNA and NetBIOS, and transparently bridge other protocols, such as IPX. In the other situation, SNA or NetBIOS uses source-route bridging and Windows NT is configured to use NetBIOS over IP. Certain other configuration alternatives do not require SRT (contact the Technical Assistance Center).

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

Release 10.3(15) Caveats

This section describes possibly unexpected behavior by Release 10.3(15). Unless otherwise noted, these caveats apply to all 10.3 releases up to and including 10.3(15). The caveats listed here describe only the serious problems. For a complete list of caveats against this release, use the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described at the end of this document.

Basic System Services

- A Route Switch Processor (RSP1, RSP2, or RSP7000) might crash if the system receives a reserved exception. If this crash occurs, the following messages will display:

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

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

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

IBM Connectivity

- The data-link switching (DLSw) ring-list is intermittently not recognized. [CSCdi33453]
- If you are using a direct Escon-attached CIP, the CIP might enter a boxed state if the router is reloaded. This problem is more likely to occur if the CIP is connected through a director, or if the CIP is taken off-line before the router is reloaded. To work around this problem, vary the device off-line before reloading the router. [CSCdi59440]
- LSAP filters and NetBIOS host filters applied to data-link switching (DLSw) remote-peer statement(s) do not work on DLSw border routers. [CSCdi66251]
- Some IBM llc2 implementation devices send a RNR when they run out of buffer and drops the frame. This will cause no data traffic flow for 30 seconds. Non IBM llc2 devices use IEEE llc2 will send REJ rather than RNR and no delay will be noticed. [CSCdi49447]

- Systems Network Architecture (SNA) sessions using Qualified Logical Link Control (QLLC) over X.25 permanent virtual circuits (PVCs) do not come active. The following tracebacks are a symptom of this problem: [CSCdi66340]

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

- If you have a serial tunnel (STUN) virtual multidrop configuration that is running local acknowledgment and STUN quick-response to accommodate AS/400 polling requirements, an AS/400 NPR time-out will occur if a remote physical unit (PU) T2.1 or T1 controller fails to activate when responding to the initial XID poll. To work around this problem, disable STUN quick-response, configure Synchronous Data Link Control (SDLC) k1 on all SDLC interfaces, and configure idle-character mark on the SDLC line(s) to the AS/400. [CSCdi66681]

Interfaces and Bridging

- High-end routers intermittently drop Sequenced Packet Exchange (SPX) keepalive packets between local Token Rings. [CSCdi36291]
- In a heavily loaded router that is transparently bridging over a serial link, it is possible for a session to indefinitely suspend. As a workaround, clear the bridge table. [CSCdi58928]
- If an RSP FDDI interface is reset, during the reset while the hardware linestate of the FDDI interface is still down, an IP route cache entry is created that references a different interface. When the FDDI interface finishes resetting, the route cache entry remains pointing at the now incorrect interface. [CSCdi63587]

IP Routing Protocols

- IP packets sent to a Hot Standby Router Protocol (HSRP) virtual MAC address are not received if the packet is Subnetwork Access Protocol (SNAP)-encapsulated and the receiving interface is part of the CiscoBus or Switch Processor (SP) complex. [CSCdi39274]
- IP addresses configured under an interface do not show up when you view the running configuration. [CSCdi62477]
- A SegV exception might cause a router to crash. [CSCdi64972]
- Offset list processing is not available. [CSCdi65889]

ISO CLNS

- If secondary addresses are configured on an unnumbered interface, the interface routes corresponding to these secondary addresses will not be advertised in the Intermediate System-to-Intermediate System (IS-IS) protocol. A workaround to this problem is to number the interface. [CSCdi60673]

Protocol Translation

- When doing large file transfers on vty-async interfaces which must cross a X.25 network with large RTT, an aggressive TCP implementation can cause return traffic on the vty-async interface to be delayed. [CSCdi54905]

Wide-Area Networking

- TCP header compression does not work over Point-to-Point Protocol (PPP), Integrated Services Digital Network (ISDN), and asynchronous dialer interfaces. To work around, turn off **ip tcp header-compression**. Note that "nondialer" asynchronous interfaces used for dial-in PPP access are not affected. [CSCdi19199]
- Infrequently, if the ATM Interface Processor (AIP) is reset while traffic is passing through it, the AIP, Switch Processor (SP), or Route Processor (RP) starts dropping packets. A soft reset occurs when AppleTalk, Connectionless Network Service (CLNS), or bridging protocols are enabled or when the **clear interface** command is performed. Typically, every 64th packet is dropped, but packets might be dropped more often. The router starts by dropping packets larger than 2 KB. The workaround is to issue a **microcode reload** command to send a hard reset to the entire CiscoBus complex and to reload the microcode in each card. [CSCdi30254]
- Sometimes, a Basic Rate Interface (BRI) port used as a backup interface might not revert to standby mode once the primary interface has recovered. Performing the **shut** and **no shut** commands on the backup BRI interface will cause it to correctly revert to standby mode. [CSCdi53644]
- Dialing into an async line and starting a SLIP/PPP session may fail even though the same IP address was previously allocated successfully for the particular user. [CSCdi63143]
- When you are using software flow control on the AUX port, the line might suspend in a Hung 0 state if it is under heavy load. The output of the **show line** command will then read:

  ```
  Status: Ready, Connected, Active, Waiting for XON, Sent XOFF
  ```

  To reenable the line, issue the **clear line** command. [CSCdi56432]
- On lines running software flow control without modem control, attached devices might get stuck in a flow-controlled state if the Cisco tty is reset while flow-controlling the attached device. [CSCdi60204]
- ISDN NET3 cannot handle incoming FACILITY messages when a call is connected. [CSCdi60340]
- Over a period of three to five weeks, an active communication server slowly runs out of I/O memory. This problem might be related to ARAP or TACACS+ usage. [CSCdi61152]
- A router running an igs-g-l image might crash with a bus error at address 0xD0D0D0D. This might be a memory-related problem. [CSCdi65228]

Release 10.3(14) Caveats

Release 10.3(14) was not officially released.

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

This section describes possibly unexpected behavior by Release 10.3(13). Unless otherwise noted, these caveats apply to all 10.3 releases up to and including 10.3(13). For additional caveats applicable to Release 10.3(13), see the caveats sections for newer 10.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 10.3(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]
- A router configured with AppleTalk and Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) takes too long to age out routes, even when the link is down. This causes too long of a convergent time for features like backup interface. [CSCdi62796]
- IPTalk does not function correctly. No IPTalk packets are processed through the router. [CSCdi64165]

Basic System Services

- If you issue the **snmp-server party** and **snmp-server context** configuration commands, the system will sometimes reload. Neither of these commands verify that the configured OID is not already in use, which permits multiple records to be configured with the same OID. This violates the rule that each record must have a unique OID. To work around this problem, do not configure OIDs that conflict with the initial party and context OIDs as specified in RFC 1447. [CSCdi63694]

IBM Connectivity

- In a parallel SDLLC network, sometimes ACTPU responses are not received by the host. [CSCdi55142]
- DLSW NetBIOS cannot connect to Windows NT. [CSCdi62784]
- Configuring the **dlsw remote-peer cost** command has no effect on peer selection. All peers displayed in the **show dlsw capabilities** command show equal costs. [CSCdi64537]
- If you are using Synchronous Data Link Control with data-link switching plus, sessions will fail to be reestablished after a physical unit is reset. [CSCdi64828]

Interfaces and Bridging

- If a packet has a Hot Standby Router Protocol (HSRP) destination MAC address, it is process switched, regardless of the route-cache status on the interface. [CSCdi44437]
- A router running Frame Relay crashes at bridge_enq even when bridging is not configured. The fix put in for this bug does not fix the crash. The fix for CSCdi67157 is the correct fix. [CSCdi63140]
- FSIP microcode does not recognize DCE leads during a cutover from a Cisco 2501 serial port. [CSCdi64735]

IP Routing Protocols

- A problem introduced in Cisco IOS Releases 10.3(11.1), 11.0(7.3), and 11.2(0.5) causes OSPF to crash when an OSPF external LSA with a nonzero forwarding address exists and the router has a non-OSPF route for the forwarding address. If the non-OSPF route is removed, OSPF crashes when it reprocesses the external LSA. There is no workaround for the problem. However, in general, no more than one routing protocol should be run over the same topology. If you follow this guideline, no non-OSPF route for forwarding address will exist and the router will not crash. [CSCdi61864]
- A directly connected route might disappear from the IPX Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) topology table if the interface that is configured for IPX Enhanced IGRP goes down and goes back up in a brief period of time (for example, 2 seconds). The workaround to this problem is to issue the commands **shut** and **no shut** for the interface. [CSCdi65345]

Novell IPX, XNS, and Apollo Domain

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

Wide-Area Networking

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

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

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(12). These caveats apply to all 10.3 releases up to and including 10.3(12). For additional caveats applicable to Release 10.3(12), see the caveats section for Release 10.3(13), which precedes this section.

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

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

AppleTalk

- AppleTalk Remote Access (ARA) connection failures occur at higher rates with the use of 28,800 kbps modems (for example, V.34, V.fc, and V.FAST modems). These connection failures result in “bad exit” and “forced quit” error messages. [CSCdi57713]
- A MacIP server will not give an IP address to MacIP clients if the next address to give out is currently being use by a genuine IP device. This causes the processor to get stuck. The problem is that the MacIP server does not skip over that IP address and assign the next available address. [CSCdi61526]

Basic System Services

- The AutoInstall feature does not work in an RSP. [CSCdi59063]
- If you reload or issue the **configure memory** command after issuing the **aaa authorization exec** command, you might lose your configuration. However, if you do not issue the **aaa accounting exec start-stop tacacs+** command during configuration, this problem will not occur. [CSCdi60172]

DECnet

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

EXEC and Configuration Parser

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

IBM Connectivity

- Removing remote source-route bridging (RSRB) peers might cause the router to suspend indefinitely. [CSCdi39270]
- If your router is using promiscuous TCP peers, the router might crash with the message "System restarted by bus error at PC 0xD0D0D0D, address 0x0." The crash occurs when peer structures get deleted because of transmission line problems, peer routers reloads, or other connection problems, while still being used by TCP. The workaround to this problem is to define static peers. [CSCdi58842]
- Data-link switching (DLSw) Ethernet 802.5 frames will be corrupted after a logical link control (LLC) retransmission. [CSCdi60102]

Interfaces and Bridging

- If you issue the **show controllers cache** command and press the space bar to page down, the router will suspend indefinitely. The only workaround is to power cycle the router. [CSCdi56241]
- NetBIOS SABME (set asynchronous balanced mode extended) messages are not correctly bridged from FDDI to serial lines using High-Level Data Link Control (HDLC) encapsulation, even though the bridging of SABME messages from FDDI to Ethernet works correctly. [CSCdi58733]

IP Routing Protocols

- If an Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) candidate default route is overwritten by another protocol, the Enhanced IGRP topology table might be left in a state where the candidate default route will not return to the routing table. A workaround to this problem is to clear all Enhanced IGRP neighbors. [CSCdi59276]
- A router running Enhanced IGRP with AppleTalk, IPX, or IP that has input route filters configured may improperly filter routes that it should install. Additionally, if a router running IPX-Enhanced IGRP receives an update containing an external route that was originated by the router itself, the rest of the update will be ignored. [CSCdi61491]
- The Open Shortest Path First (OSPF) protocol might crash if there are parallel intra-area paths. [CSCdi62870]

ISO CLNS

- A router reload may occur when Connectionless Network Service (CLNS) traffic is fast-switched. [CSCdi57629]
- If your router is under a heavy load and you use Intermediate System-to-Intermediate System (IS-IS) or NetWare Link Services Protocol (NLSP), packets might be dropped unnecessarily. [CSCdi58433]

- If a non-Cisco router is running IS-IS on a level-1-only circuit and the router is sending End System-to-Intermediate System (ES-IS) End System Hello (ESH) messages, a Cisco router might not recognize the ESH messages. A workaround is to filter out the ESH packets using the **clns adjacency-filter es** configuration command in conjunction with setting an appropriate filter. The filter should specify a wildcard (**) in the last byte of the address. [CSCdi58621]
- A router running IS-IS will not clean up its adjacency database properly when switched from being a level-1/level-2 router to being level-1 only. A workaround to this problem is to manually clear the adjacency database using the **clear clns neighbors** command on the reconfigured router and on all of its neighboring routers. You can also restart the router to work around this problem. [CSCdi58953]

Novell IPX, XNS, and Apollo Domain

- Infrequently, Intermediate System-to-Intermediate System (IS-IS) and NetWare Link Services Protocol (NLSP) link-state packets (LSPs) are not transmitted on point-to-point interfaces. [CSCdi58613]
- If you issue the **no ipx router eigrp xxx** command, the router might reload if there are a lot of service access points (SAPs) defined in the router and if the SAP table was changing while the command was performed. [CSCdi60174]

VINES

- The Cisco 1001 LAN extender does not work with VINES if a remote LAN is connected to a core router through the LAN Extender. [CSCdi57934]

Wide-Area Networking

- The amount of free system memory might decrease if you issue the **dialer hold-queue** command over an ISDN interface. [CSCdi58402]

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

This section describes possibly unexpected behavior by Release 10.3(11). Unless otherwise noted, these caveats apply to all 10.3 releases up to and including 10.3(11). For additional caveats applicable to Release 10.3(11), see the caveats section for Release 10.3(12), which precedes this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section “Cisco Connection Online” later in this document.

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

AppleTalk

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

Basic System Services

- Under some conditions, Simple Network Management Protocol (SNMP) queries of the Cisco Environmental Monitor MIB can cause the system to reload. This behavior occurs when an SNMP get-request operation tries to retrieve instance 0 of an object in the ciscoEnvMonSupplyStatusTable. Because the instances of this table start with 1, the correct processing is to return a *noSuchName* error (or *noSuchInstance* if SNMPv2 is used). A workaround is to not use SNMP get-requests that specify instance 0 for objects in the Cisco Environmental Monitor MIB. Instead, applications should either use SNMP get-request operations starting with instance 1, or else use SNMP get-next-requests or get-bulk-request operations. [CSCdi55599]

Access Server

- Asynchronous lines may become stuck in a “Carrier Dropped” state when running TACACS+ against a slow TACACS+ server. Only a reload can make the lines usable again. [CSCdi54618]

DECnet

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

IBM Connectivity

- In certain mixed-vendor bridge environments, the automatic spanning tree (AST) never becomes active if a Cisco device is the root bridge. Bridge protocol data units (BPDUs) are constantly exchanged, but the spanning tree topology never develops or becomes active. [CSCdi53651]
- A LAN Network Manager (LNM) might fail to link to an access server’s source bridge, after a Token Ring interface is shut down on a remote access server. The **show lnm bridge** command continues to display an active link to the LAN network manager. This problem does not occur with bridges that are locally linked to the LAN manager. To work around, first remove and then reconfigure the **source-bridge** command from the Token Ring interface. [CSCdi53954]
- New Systems Network Architecture (SNA) sessions fail to connect to a front-end processor, when duplicate ring numbers are in the Routing Information Field (RIF). To work around, issue the **clear rif-cache** command. [CSCdi55032]
- Packets might be dropped if they are received for a Fast-Sequenced Transport (FST) nonselective peer while that peer is still setting up the connection. [CSCdi55219]
- Connections to dependent logical units (DLUs) with downstream physical unit (DSPU) or Advanced Peer-to-Peer Networking (APPN) across RSRB might fail when the remote service access point (SAP) address is not enabled at the destination access server. The workaround is to enable the remote SAP address. [CSCdi56660]
- DLSw Fast-Sequenced Transport (FST) encapsulation does not work over a WAN Token Ring or over FDDI. [CSCdi57207]

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 that has a higher sequence number, OSPF cannot resolve the conflict and is unable to remove the LSA. The old LSA copy is most likely received from some new neighbors through database exchange. You will observe a self-originated LSA stuck in the database. [CSCdi48102]
- OSPF sometimes puts incorrect information in the source field for stub routes. This prevents the Border Gateway Protocol (BGP) from advertising the stub route to peers, as the route will not be synchronized. [CSCdi49377]
- Attempting to copy an empty startup configuration to the network causes the access server to reload. [CSCdi58040]

ISO CLNS

- No method exists for altering the transmission rate of Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs) in cases where the rate would add undue load to the receiving system. [CSCdi54576]
- If IS-IS is running, and a Connectionless Network Service (CLNS) static route is configured that points to a point-to-point interface on which IS-IS is not configured, and the static route is removed, the system might suspend indefinitely. A workaround is to either disable IS-IS before removing the static route, or to enable IS-IS on the point-to-point interface before removing the static route. [CSCdi56815]

Novell IPX, XNS, and Apollo Domain

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

Wide-Area Networking

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

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

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

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section "Cisco Connection Online" later in this document.

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

Access Server

- A busy access server sometimes pauses indefinitely, indicating an invalid address error. This is usually seen in environments where a number of short duration modem calls are answered. A workaround is to configure **modem answertimeout 10**. [CSCdi48100]

IBM Connectivity

- When two or more access servers are connected to the same Token Rings, and each uses source-route bridging (SRB), a station on one of the rings might choose a non-optimal route with a path through both access servers. In typical (large) networks, this behavior might result in explorer storms as well as suboptimal routes. [CSCdi45116]
- A Cisco access server might report inaccurate traffic statistics. In particular, non-broadcast frame counts might be incorrect if the access server is acting as a source bridge on a Token Ring. [CSCdi46631]
- An incorrect timer reference causes explorer frames to be flushed on interfaces, even when the maximum data rate for explorers on the interface is not exceeded. [CSCdi47456]
- The number of downstream PUs supported should be increased from 256 to 1024. [CSCdi49448]
- If peer A and peer B are DLSw priority peers (the keyword **priority** is on the remote peer definition), and peer A is reloaded, peer B may crash. [CSCdi50155]
- Low end platforms will cache invalid rif entries when using any form of the **multiring** command. This can also be seen in the dlsw reachability cache and possible loops with lnm. [CSCdi50344]
- Peer-on-demand peers (peers that learn of each other through border peers) do not connect. The options **inactivity** *timeout* and **lf** *lfsize* should be added to the **dlsw peer-on-demand-defaults** command. [CSCdi50574]
- Removing DLSw configuration by configuring **no dlsw local-peer** and adding the DLSw configuration back can cause a memory leak in the middle buffer. [CSCdi51479]
- Applying a **source-bridge output-lsap-list** to a Token Ring interface when **source-bridge explorer-fastswitch** is enabled may cause packets permitted by the output-lsap-list to be dropped. The workaround is **no source-bridge explorer-fastswitch**. [CSCdi51754]

- When a very large number of i-frames are sent by an end station to a DLSw access server at the same instant, the following message may appear on the console:

  DLSW:CPUHOG in CLS background, PC=0x60549f3c

  Since the CPU is being occupied by the cls background process for a period of time, protocols that involve polling may lose their connections due to poll starvation. [CSCdi52382]
- Ethernet sessions don't come up or drop. The llc frames are bad after a retransmission. [CSCdi52934]

IP Routing Protocols

- Running multiple Enhanced Interior Gateway Routing Protocol (EIGRP) autonomous systems might consume all available memory in the access server. [CSCdi36031]
- Unconfiguring OSPF can cause the access server to reload. [CSCdi51283]
- If two IP-EIGRP autonomous systems are configured, and then an interface address is changed such that the interface moves from one autonomous system to the other, EIGRP will fail to operate on that interface. The workaround is to delete the IP address (using the **no ip address** command) before configuring the new address. [CSCdi52078]
- Under certain conditions, EIGRP may stop transmitting packets. This may manifest itself as large numbers of routes repeatedly Stuck-In-Active. The workaround is to deconfigure and restart EIGRP, or reload the system. [CSCdi53466]

TCP/IP Host-Mode Services

- Under unknown circumstances, random lines on an ASM will pause indefinitely in Carrier Dropped state. The only way to clear the line is to reload the ASM. [CSCdi44663]

VINES

- Vines SRTP on serverless segments 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

- Under certain conditions, the access server can reload with the following message:

  System was restarted by error–Illegal Instruction, PC 0x300D646

  This problem is related to ISDN. There is currently no workaround. [CSCdi45085]
- If CHAT script operations fail over asynchronous interfaces, a reload might occur during later operations because data was left in an inconsistent state. [CSCdi47460]

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

This section describes possibly unexpected behavior by Release 10.3(9). Unless otherwise noted, these caveats apply to all 10.3 releases up to and including 10.3(9). For additional caveats applicable to Release 10.3(9), see the caveats sections for newer 10.3 releases. The caveats for newer releases precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section “Cisco Connection Online” later in this document.

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

Access Server

- The **service hide-telnet-address** command does not hide the Telnet address in the connection closing message. The **busy-message** command does not suppress connection closing message. [CSCdi47740]

AppleTalk

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

Basic System Services

- Available memory will slowly decrease on an access server that is bridging IP and which 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-IGRP, if there are DECnet L2 routes on the DECnet side. These area routes show up as “AA00” and are propagated to other access servers. [CSCdi47315]

IBM Connectivity

- When source-route transparent (SRT) bridging is configured on the access server, 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 QLLC connection, a virtual circuit is established, but the XID negotiation never proceeds to completion. The access server sends XID responses as commands, rather than as responses. [CSCdi44435]
- An access server might crash if running QLLC and using RSRB over a serial line to provide the Logical Link Control, type 2 (LLC2) connection from QLLC to an end station or host. The crash only occurs if multiple changes are made to the encapsulation type on the RSRB serial line. [CSCdi45231]

- If an access server receives a source-route bridging (SRB) packet with bit 2 of the routing control field set, the access server 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]
- When Synchronous data-link control (SDLC) attached physical unit 2.1 (PU 2.1) devices are connected over data link switching plus (DLSw+), if the host device does not respond because the application is down, the DLSW+ circuit does not correctly disconnect. This problem causes the circuit at the SDLC end to be in a CONTACT PENDING state even with no circuit at the host end. This is cleared by shutting down the SDLC interface at the access server or by reloading the PU 2.1 device. [CSCdi48227]

IP Routing Protocols

- If an access server is incorrectly configured with an autonomous system (AS) placed in a confederation it is not part of, the confederation information within the AS path will be incorrectly propagated. The workaround is to configure the access server correctly. [CSCdi46449]

ISO CLNS

- ISO Interior Gateway Routing Protocol (IGRP) in millions of instructions per second (mips)-based access servers does not interoperate with 68 Kbps-based access servers. [CSCdi44688]

TN3270

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

VINES

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

Wide-Area Networking

- An X.25 interface might hang if the Link Access Procedure, Balanced (LAPB) layer gets stuck in the RNRSENT state. This might occur if virtual circuits (VCs) receive encapsulated datagram fragments that are held for reassembly, and the number of these fragments approaches the interface input queue count. The LAPB protocol will not exit the RNRSENT state until the number of held buffers decreases. This condition can be cleared if a **shut**/**no shut** is performed on the interface, or if the other end of the LAPB connection resets the protocol. [CSCdi41923]
- If Cisco’s enhanced Terminal Access Controller Access Control System (TACACS+) is enabled, you cannot specify inbound authentication on the Point-to-Point Protocol (PPP) authentication configuration line. [CSCdi49280]

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

This section describes possibly unexpected behavior by Release 10.3(8). Unless otherwise noted, these caveats apply to all 10.3 releases up to and including 10.3(8). For additional caveats applicable to Release 10.3(8), see the caveats sections for newer 10.3 releases. The caveats for newer releases precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section "Cisco Connection Online" later in this document.

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

Access Server

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

Basic System Services

- Fast switching with some encapsulations might cause the access server to crash. The workaround is to disable fast switching. [CSCdi45414]
- The access server might reload if a user is authenticating access with Terminal Access Controller Access Control System (TACACS) or extended TACACS with Password Authentication Protocol (PAP). This reload occurs if the interface is not an asynchronous line and the user's username and password also exist in the local database. [CSCdi45530]
- Issuing Simple Network Management Protocol (SNMP) sets commands to the *writeNet*, *hostConfigSet*, or *netConfigSet* variables might cause the access server to reload. The workaround is to not issue sets to these variables. [CSCdi45948]
- Using Hot Standby Router Protocol (HSRP) in heavy traffic conditions might cause cbus resets and the error report "RSP-3-ERROR." [CSCdi46654]

IBM Connectivity

- When an SDLLC or Qualified Logical Link Control (QLLC) virtual ring is configured, explorer frames might incorrectly forwarded to the interface corresponding to the third ring listed in the Routing Information Field (RIF). [CSCdi43378]
- On low-end systems for a data terminal equipment (DTE) access server interface, after an access server reload the following error might occur. Synchronous Data Link Control (SDLC) packets are identified as High-Level Data Link Control (HDLC) packets by the serial driver, until a **shut/no shut** command is performed for the interface. This error causes occasional packet drops without any trace, if the byte pattern happens to match that of other protocols. The dropping of packets can be significant performance problems. [CSCdi43686]
- Source-route bridging (SRB) bridged packets might be dropped when an access server is configured for remote source-route bridging (RSRB) direct, and when priority/custom queueing is enabled on the output serial interface. A workaround is to disable priority/custom queueing on the serial interface. [CSCdi44430]

- Under certain conditions with RSRB local acknowledgment, workstations are unable to immediately reconnect to an AS400 after a session loss. The server continues to send SABMEs to the workstation, even after receiving a UA response. [CSCdi45565]
- Using data-link switching (DLSw) might cause traceback messages to occur. [CSCdi45407]
- When an access server is configured for Data Link Switching Plus (DLSw+) with SDLC, and an application is taken down on the host system, the SDLC controller will not respond. To recover, reload the SDLC attached controller. Issuing **show interfaces** command on the access server indicates that the interfaces are in the XIDSENT state. [CSCdi46028]
- Outbound access lists are not always applied to fast switched explorer frames. [CSCdi46182]
- An access server configured for downstream physical unit (DSPU) might crash while making DSPU configuration changes. [CSCdi46820]
- DSPU/remote source-route bridging (RSRB) connections are sometimes unable to be established. [CSCdi46949]

Interfaces and Bridging

- High-end access servers check collisions and keepalives to determine line protocol up/down. However, low-end access servers do not. [CSCdi32464]
- Secure Data Exchange (SDE) encapsulation used with bridged virtual LANs (VLANs) might be corrupted in some environments. This results in lost traffic between VLAN-connected networks. The environments known to be affected include connections across High-Speed Serial Interfaces (HSSIs) and Token Rings. The SDE encapsulation works correctly across Ethernet connections. [CSCdi36792]
- With two access servers on a ring, Open Shortest Path First (OSPF) neighbors disappear after a few hours because the Internet Protocol (IP) process does not receive the multicast packet for OSPF hellos. [CSCdi38185]
- Enabling the silicon switching engine (SSE) for IP might cause the system to crash. The workaround is to perform the **no ip route-cache sse** command. [CSCdi44414]

IP Routing Protocols

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

Novell IPX, XNS, and Apollo Domain

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

Protocol Translation

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

TCP/IP Host-Mode Services

- With **encap lapb** or **encap X.25** configured, under certain conditions the command **lapb N1 xxx** disappears from the working configuration, and N-1 falls back to the default. This is most likely to occur after an interface reset or a reload. [CSCdi44422]
- Using autoinstall over Frame Relay, after downloading the host specific config file, might result in access server reload(s). This happens when point-to-point subinterfaces are used. [CSCdi44643]
- With **encap lapb** or **encap X.25** configured, under certain conditions the command **lapb n1** *bits* disappears from the working configuration, and N1 falls back to the default. This is most likely to occur after an interface reset or a reload. [CSCdi44422]
- After downloading a host-specific configuration file, using AutoInstall over Frame Relay with point-to-point subinterfaces, might result in an access server reload. [CSCdi44643]
- A serial interface running X.25 encapsulation under heavy load conditions might stop sending the Link Access Procedure, Balanced (LAPB) protocol. [CSCdi46024]
- IGRP protocol routing broadcasts sometimes fail to dial static routes on Point-to-Point Protocol (PPP) backup interfaces. A workaround is to configure SNMP or *syslog* to a host on the remote side. [CSCdi46312]
- Access servers with the **isdn switch-type basic-net3** command in use with Integrated Services Digital Network (ISDN) Basic Rate Interfaces (BRIs), might experience BRI port failures. A reload of the access server is required to use the BRI interface. [CSCdi46668]

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

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(7). Unless otherwise noted, these caveats apply to all 10.3 releases up to and including 10.3(7). For additional caveats applicable to Release 10.3(7), see the caveats section for newer 10.3 releases, which precedes this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section “Cisco Connection Online” later in this document.

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

IBM Connectivity

- When using local-ack, the following error messages may result in an access server reload or loss of session: [CSCdi34930]

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

- DSPU sends TEST (P) in response to a NULL XID (P) on Connect-ins. This causes problems with certain LLC2 implementations. [CSCdi40809]
- IPX All Stations Broadcasts Explorers will not be fast switched, when IPX source route bridged. [CSCdi41043]
- The access server’s serial interface driver software occasionally drops SDLC frames if the bit patterns are identical to HDLC LEX frames. This dropping occurs on interfaces using STUN-basic encapsulation with non-IBM SNA data traffic (for example, COMM10 CNS protocol). Note, there is no indication in the access server when this problem occurs. The access server does not increment the interface “drop” counter or the STUN “drop” counters. Detection is only possible with a media tracing tool. [CSCdi41558]
- The Find Name NetBIOS broadcast is sent from the Token Ring interfaces even though the proxy-explorer and NetBIOS name caches are configured on the interface. To workaround, run backlevel software. [CSCdi41972]
- Although access servers with sufficient memory and CPU horsepower should be able to support more than 1000 LLC2 sessions, the actual number of sessions allowed is erroneously limited to significantly fewer. [CSCdi42181]

Interfaces and Bridging

- For a given bridge table entry, bridging may fail to forward packets to one destination, although packets to other destinations will be properly forwarded.This can be seen by a **show bridge nnnn.nnnn.nnnn** command. The TX count increments, but the RX count stays constant. The workaround is to issue a **clear bridge** command. [CSCdi42445]
- At times stations are not able to establish connectivity over transparent bridging, since some dlc frames are not forwarded when they should be. [CSCdi42690]
- When you configure SLIP or PPP framing on the auxilliary port of an access server, “Low memory modified by Input Helper” messages erroneously appear in system error log. [CSCdi43970]

Novell IPX, XNS, and Apollo Domain

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

TCP/IP Host-Mode Services

- BOOTP attempts might fail over an asynchronous VTY PPP connection when **async-bootp** commands are used. This is due to an incorrect UDP checksum on the BOOTP reply. [CSCdi41168]

VINES

- Under heavy loads, the VINES access server system process may not run frequently enough for proper VINES operation. Symptoms include a high amount of route and neighbor flappage. Reducing the load on the access server may help alleviate the problem. [CSCdi41922]
- When using the Cisco 2500 series terminal servers with PPP, packets might pass after IPCP has completed negotiation, but before the interface is declared to be up. This can cause problems with applications that send out immediate requests, since the response may be dropped by the terminal server due to the interface being down. The workaround is to place a slight pause after IPCP has been negotiated and before sending out requests. [CSCdi37400]
- Hardware flow control might be inadvertently disabled on the Cisco 2509, 2510, 2511 and 2512 asynchronous ports after issuing a **configure network** or a **copy tftp running-config** command. To restore flowcontrol, simply issue **flowcontrol hardware** on all of the lines. [CSCdi43306]

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

This section describes possibly unexpected behavior by Release 10.3(6). For additional caveats applicable to Release 10.3(6), see the caveats sections for newer 10.3 releases. Unless otherwise noted, these caveats apply to all 10.3 releases up to and including 10.3(6). The caveats for newer releases precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section “Cisco Connection Online” later in this document.

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

AppleTalk

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

Basic System Services

- IPX SAP process may consume more memory than required causing a memory leak and potential memory exhaustion. [CSCdi38381]
- When using Protocol Translation for virtual asynchronous connections, the system may restart and display the message “System was restarted by error - Illegal Instruction, PC 0x0.” [CSCdi40681]

IBM Connectivity

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

IP Routing Protocols

- When **ip ospf network broadcast** is configured on WAN interfaces like Frame Relay and the **ip ospf hello-interval** command is used to set the interval to 30, the hello-interval is lost upon reload. To work around the problem, set the hello-interval to 30. [CSCdi40729]

TCP/IP Host-Mode Services

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

VINES

- The VINES access server system process runs at low priority. It should run at normal priority. [CSCdi41380]

Wide-Area Networking

- Frame Relay DLCIs that are deleted using the **no frame-relay interface dlci** command are not actually deleted from the system. [CSCdi39555]
- When using DTR dialing and PPP encapsulation, DTR does not stay “low” after the call is disconnected. [CSCdi39576]
- In rare circumstances, an SDLLC connection failure can cause the access server to reload. [CSCdi39832]
- On Cisco 2509 through Cisco 2512 devices, asynchronous lines stop accepting input under certain conditions. One of these conditions occurs when a user connected to a LAT host types a Control-C character. A **clear line x** or a change to the line parameters will cause the line to start accepting input again. [CSCdi40994]

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

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

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section “Cisco Connection Online” later in this document.

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

AppleTalk

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

Basic System Services

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

DECnet

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

EXEC and Configuration Parser

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

IBM Connectivity

- NetBIOS connections occasionally fail to connect through remote source-route bridging when local acknowledgment is enabled. The workaround is to disable local acknowledgment. [CSCdi37525]
- LLC2 parameters on IETF are not recognized when entered. [CSCdi37921]

- DSPU does not recognize the 2-byte ACTLU RSP as a valid response and, therefore, does not activate the LU. [CSCdi38299]
- The DLSw+ state machine can hang so that on an SDLC line, a **show dls circuit** command will show one index in a HALT PENDING NOACK state and another at DISCONNECT PENDING. During this state, no DLSw+ traffic will flow over these circuits. A **clear dls circuit** command has no effect, requiring an access server reload to recover. [CSCdi39046]

Interfaces and Bridging

- Very intermittently, the FSIP controller detects a spurious error on the transmit buffer size resulting in a controller fatal error. [CSCdi30344]
- On the partner product (a Cisco 2500 variant co-developed with DEC), when an Ethernet interface goes down, the output of a **show interface** command still shows that the interface is up. The SNMP replies are also incorrect. [CSCdi37135]

IP Routing Protocols

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

ISO CLNS

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

Protocol Translation

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

TCP/IP Host-Mode Services

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

VINES

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

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

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

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section “Cisco Connection Online” later in this document.

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

AppleTalk

- The problem that prevented the access server from invalidating the old cache entries was corrected. [CSCdi35967]

DECnet

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

IP Routing Protocols

- Access lists using the **tacacs-ds** keyword will not be parsed correctly in 10.3(4). This bug was introduced in CSCdi34944, which was integrated into 10.3(3.4). [CSCdi36962]

Novell IPX

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

Wide-Area Networking

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

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

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

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section “Cisco Connection Online” later in this document.

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

Basic System Services

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

IP Routing Protocols

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

Novell IPX

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

Wide-Area Networking

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

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

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

- Invalid packets received on an SMDS interface are discarded incorrectly, and remain counted against the input queue, causing the interface to stop receiving traffic. [CSCdi34116]
- The command **autocommand ppp** produces the error message "%Unable to find address for you" upon startup of the connection. This problem first appeared in Release 10.3(2.0.1). To work around the problem for async connections only, use the line configuration command **autocommand ppp default**. There is no workaround for virtual asynchronous connections. [CSCdi34519]

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

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(2). For additional caveats applicable to Release 10.3(2), see the caveat sections for newer 10.3 releases, which precede this section. All the caveats listed in this section are resolved in Release 10.3(3).

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section “Cisco Connection Online” later in this document.

AppleTalk

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

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

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

Basic System Services

- TACACS notify requests do not use the user-configurable retransmit and timeout parameters. [CSCdi30113]
- SLARP can cause the system to reload on access servers that have dual flash bank. [CSCdi30588]

Interfaces and Bridging

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

IP Routing Protocols

- The [**no**] **ip summary-address** command can cause the access server to reload. [CSCdi23646]
- This bug was introduced in Release 10.3(0.16). The configuration of **ip ospf dead-interval** is lost after reload. No workaround is available. If necessary, the command can be reconfigured after reload to ensure proper operation. This fix solves the problem. [CSCdi31279]

Novell IPX

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

Wide-Area Networking

- DLCI’s can not be reassigned to subinterfaces from a primary interface. [CSCdi28765]
- The Defense Data Network (DDN) and Blacker Front End Emergency (BFE) modes do not encode the needed local facilities when originating a call. [CSCdi31252]

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

This section describes possibly unexpected behavior by Cisco IOS Release 10.3(1). Unless otherwise noted, these caveats apply to all 10.3 releases up to and including 10.3(1). For additional caveats applicable to Release 10.3(1), see the caveat sections for later 10.3 releases, which precede this section.

The caveats listed here describe only the serious problems. For the complete list of caveats against this release, the Cisco Connection Documentation, Enterprise Series CD-ROM or access Cisco Connection Online (formerly CIO) as described in the section “Cisco Connection Online” later in this document.

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

Basic System Services

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

EXEC and Configuration Parser

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

IP Routing Protocols

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

  The problem is as follows: When access servers 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 access servers 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. An access server that is selected as the gateway of last resort is one that advertises the best metric for candidate default routes.)

  A complete fix to the backwards compatibility problem is available as of Releases 9.21(5.1), 10.0(4.7), and 10.2(0.11). Access servers running a version older than those versions cannot mark Enhanced IGRP internal routes as candidate default routes. [CSCdi23758]

Novell IPX

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

VINES

- The VINES address the access server retains to assign to clients is not incremented after it is assigned to a client until the access server receives an RTP or SRTP update from the client. This leaves a short window in which duplicate address assignments can occur. [CSCdi29886]
- There is no form of modem control that offers the capabilities of **modem cts-required** or **modem callout** and also allows simultaneous hardware flow control. [CSCdi26270]
- In certain traffic-loading conditions on async lines (generally, an async line with receive and transmit looped), using reverse Telnet can cause garbage characters to be output on the line. [CSCdi29696]
- If an ASM async interface is configured with the **flowcontrol hardware in** command, the CTS line does not honor flow control requests. Issue the **flowcontrol hardware** command to cause correct operation. [CSCdi30054]

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.

Cisco Connection Documentation CD-ROM

The complete list of caveats against this release is available on Cisco Connection Documentation, Enterprise Series CD-ROM, formerly UniverCD, which is Cisco System’s library of product information on CD. On CD, access the Cisco IOS Release 10.3 Caveats in the Cisco Product Documentation, Cisco IOS Release 10.3 database..

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

969R