Doc. No. 78-1279-07

Router Products Release Notes for Software Release 9.21

January 23, 1995

These release notes describe the features, modifications, and caveats for Software Release 9.21, up to and including Release 9.21(7). Refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications for complete router documentation for Release 9.21.

Note Release 9.21(7) is the last maintenance release for Release 9.21. Maintenance customers will continue to receive phone support from Customer Engineering, but software fixes will be made only to IOS Release 10.0 and higher releases. As of January 23, 1995, IOS Release 10.0(7) or 10.2(2) is the preferred upgrade path for a Release 9.21 user.

Introduction

These release notes discuss the following topics:

Platform Support

Software Release 9.21 is supported on the following router platforms:

- Cisco 7000 series
- Cisco 4000 series
- Cisco 3000 series
- Cisco 2500 series
- AGS+ (with a CSC/4 processor board)
- MGS (with a CSC/4 processor board)
- CGS (with a CSC/4 processor board)
- IGS

Tables 1 through 3 summarize the features supported on each platform.

Table 1 Features Supported by Router Platforms

Feature	Cisco 7000 Series	Cisco 4000 Series	Cisco 3000 Series	Cisco 2500 Series	AGS+	MGS	CGS	IGS
Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bridging	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Packet switching	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protocol translation	No	No	Yes	Yes	No	No	No	Yes
Flash EPROM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Telnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SLIP (with AUX port)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 2 LAN Interfaces Supported by Router Platforms

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

Table 3 WAN Interfaces Supported by Router Platforms

Feature	Cisco 7000 Series	Cisco 4000 Series	Cisco 3000 Series	Cisco 2500 Series	AGS+	MGS	CGS	IGS
Data Rates								
48/56/64 kbps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
1.544/2.048 Mbps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
34/45/52 Mbps	Yes	No	No	No	Yes	No	No	No
Interfaces								
EIA-232	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.21	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
V.35	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EIA/TIA-530	Yes	Yes	Yes	Yes	No	No	No	No
EIA/TIA-613 (HSSI)	Yes	No	No	No	Yes	No	No	No
G.703	No	No	No	No	Yes	No	No	No

IOS Software Feature Sets for the Cisco 2500 Series

Three IOS software feature sets are provided for the Cisco 2500 series. Each set provides a subset of the full Cisco feature set. Table 4 lists the features provided in each subset image.

Table 4 Cisco 2500 Subset Images

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

Memory Requirements

With Software Release 9.21, the Cisco software image size has exceeded 3 Mbytes and, when compressed, will exceed 2 Mbytes. Also, routers now require more than 1 Mbyte of main system memory for data structure tables.

In order for the Cisco 2500, Cisco 3000 series, Cisco 4000, and IGS routers to take advantage of the Release 9.21 features, you must upgrade the code or main system memory as listed in Table 5. Some platforms have specific chip or architecture requirements that affect what can be upgraded and in what increments.

Table 5 Release 9.21 Memory Requirements

Router	Required Code Memory	Required Main Memory	Release 9.21 Runs from ...
IGS/L and IGS/R	4 MB ROM	4 MB RAM	ROM
IGS/TR	4 MB ROM	4 MB RAM	ROM
Cisco 2500	4 MB Flash	See Table 6	Flash
Cisco 3101	4 MB Flash	4 MB RAM	Flash
	4 MB Flash	16 MB RAM	RAM
Cisco 3102	4 MB Flash	4 MB RAM	Flash
	4 MB Flash	16 MB RAM	RAM
Cisco 3103	4 MB Flash	4 MB RAM	Flash
	4 MB Flash	16 MB RAM	RAM
Cisco 3104	4 MB Flash	4 MB RAM	Flash
	4 MB Flash	8 MB RAM	RAM
Cisco 3202[1]	2 MB Flash	16 MB RAM	ROM
Cisco 3204	4 MB Flash	4 MB RAM	Flash
	4 MB Flash	8 MB RAM	RAM
Cisco 4000	4 MB Flash	16 MB RAM	RAM
Cisco 4000M	4 MB Flash	8 MB RAM	RAM

1. The Cisco 3202 image can be booted only from the network. It cannot be loaded from Flash.

Table 6 Cisco 2500 Memory Requirements

Network Size	IP Feature Set	Desktop Feature Set	Enterprise Feature Set
Small	2 MB RAM	6 MB RAM	6 MB RAM
Medium	2 MB RAM	6 MB RAM	6 MB RAM
Large	6 MB RAM	6 MB RAM	6 MB RAM

Boot ROMs

For the Cisco 4000, there are no minimum boot ROM requirements. However, if you plan to open your Cisco 4000 router for any other reason, such as upgrading memory, we recommend that you upgrade to 9.14(6) boot ROMs at the same time.

In addition, some 9.21 images may fail to uncompress after booting from the network or Flash because of a bug in some boot ROMs prior to 9.1(8) or 9.14(4). After the ### sequence is displayed when the image is uncompressing, the router may re-enter the ROM monitor or crash. If this occurs, you have three options or workarounds:

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

You may also wish to upgrade boot ROMs on Cisco 3000 series and Cisco 4000 series routers if you encounter the following problems:

- Flash memory overerasure. Writing Flash memory sometimes causes overerasure of the Flash EEPROMs. The symptoms are that further Flash memory erases or writes fail after exceeding the permitted number of retries. ROMs based on 9.1(4) or 9.14(1), or later, do not have this problem.
- Serial line goes down while erasing or writing Flash memory.

Microcode Software

Table 7, Table 8, and Table 9 list the current microcode versions. Note that for the Cisco 7000 series, microcode software images are bundled with the system software image. Bundling eliminates the need to store separate microcode images. When the router starts up, the system software will unpack the microcode software bundle and load the proper software on all the interfaces.

Note We strongly recommend that the microcode bundled with the system software be used as a package. Overriding the bundle could possibly result in incompatibility between the various interface processors in the system.

Table 7 Current Microcode Versions for AGS+, MGS, and CGS Routers with CCTL2

Processor or Module	Current Microcode Version
CSC-SCI	1.4
CSC-SCI HDX (half duplex)	5.0
CSC-MCI	1.11
CSC-R16M	3.4
CSC-1R/CSC-2R	1.6
CSC-ENVM	2.2
CSC-CCTL2	11.0
CSC-C2MEC	10.1
CSC-C2HSCI	10.1
CSC-C2FCI	10.2
CSC-C2FCIT	10.2
SC-C2CTR	10.2

Table 8 Current Microcode Versions for AGS+, MGS, and CGS Routers with CCTL

Processor or Module	Current Microcode Version
CSC-SCI	5.1
CSC-SCI HDX (half duplex)	5.0
CSC-MCI	1.10
CSC-R16M	3.4
CSC-1R/CSC-2R	1.4
CSC-ENVM	2.2
CSC-CCTL	3.0
CSC-MEC (5.0)	1.7
CSC-MEC (5.1)	2.4
CSC-HSCI	1.1
CSC-FCI	2.2

Table 9 Current Microcode Versions for Cisco 7000 Series Routers

Processor or Module	Current Microcode Version	Minimum Version Required to Run 9.21
SP (Switch Processor)	2.4	2.0[1]
EIP (Ethernet Interface Processor)	1.2	1.0
FIP (FDDI Interface Processor)	1.5	1.3
FSIP (Fast Serial Interface Processor)	1.2	1.1
HIP (HSSI Interface Processor)	1.4	1.1
SIP (Serial Interface Processor)	1.1	
TRIP (Token Ring Interface Processor)	1.2	1.1

1. Minimum level needed to run IPX autonomous switching, multiple IPX encapsulations, autonomous transparent bridging, VINES fast switching, and IP autonomous switching over Frame Relay or PPP. For the AGS+, if you do not want to use these features, refer to the AGS+ microcode release notes for the minimum microcode levels.

New Features in Release 9.21(5)

Maintenance Release 9.21(5) provides support for the 4T NIM for the Cisco 4000 series router.

New Features in Release 9.21(4)

Maintenance Release 9.21(4) provides support for the 2R NIM for the Cisco 4000 series router.

New Features in Release 9.21(3)

The following new features have been added in Maintenance Release 9.21(3):

- The software now runs on the Cisco 2500 router platforms.
- The software now supports the IPX network number feature of IPXCP (IPX over PPP). The local Cisco router informs the remote side of the local router's IPX network number and IPX node number. The remote side must support this PPP negotiation.
- The software now supports the 64-Mbyte RP on Cisco 7000 series routers.
- You can now specify an optional called-party subaddress number in an outgoing ISDN call. You enter the subaddress number after the called-party number separated with a colon in the **dialer string** or **dialer map** commands. This is illustrated in the following configuration example:

  ```
  configure terminal
  interface bri 0
  dialer string 12345:123
  dialer map ip 1.1.1.1 67890:11
  ```

  When DDR makes an outgoing call using the number in the **dialer string** command, the called-party number is 12345 and the called-party subaddress number is 123. In the **dialer map** command, the called-part number is 67890 and the subaddress number is 11.
- For incoming ISDN BRI calls, the software can now verify a called-party number and subaddress number in the incoming setup message if it is delivered by the switch. The verification is always done if a number is configured in either an **answer1** or an **answer2** command:

  interface bri 0
  isdn answer1 5552222:1234

  or

  isdn answer2 9991111:9876

  The 5552222 and 9991111 are the called-party numbers, and the 1234 and the 9876 are the subaddresses. Note that the colon is the separator.

  If nothing is configured, all calls are accepted. In case one or both the answer numbers are configured, the incoming called-party number and the subaddress are verified before accepting the call.

  It is possible to configure just the called-party number or just the subaddress. In such a case, only that part will be verified.

  The verification proceeds from right to left for both the called-party number and subaddress.

  It is possible to declare a digit a "don't care" digit by configuring it as an "x" or "X." In such a case, any incoming digit is allowed.
- You can now configure a dialer rotary group to place additional calls to a single destination if the load for the interface exceeds a specified weighted value. Do this using the **dialer load-threshold** interface configuration command.

New Features in Release 9.21(2)

The following new features have been added in Software Release 9.21(2):

- The software now runs on the Cisco 3104, Cisco 3204, Cisco 4000, and Cisco 7010 router platforms.
- The software now supports source-route bridging, remote source-route bridging, and STUN.

Software Features in Release 9.21(1)

This section describes new features and enhancements made in the initial release, Release 9.21(1), of the router products software.

User Interface

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

- Enhanced command interpreter. The EXEC command interpreter has online help and enhanced editing commands.

System Images, Microcode Images, and Configuration Files

The following feature has been added to Cisco's image and configuration file software:

- AutoInstall procedure. The AutoInstall procedure allows you to configure a new router automatically and dynamically.

Terminal Lines and Modem Support

This following feature has been added to Cisco's terminal line and modem software:

- Displaying line-number information. You can configure the router to display line-number information after the EXEC or incoming banner.

System Management

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

- Priority queuing. You can now assign traffic priorities according to a specific access list for AppleTalk, Banyan VINES, Novell IPX, and XNS. Previously, this feature was available only for IP.
- Network Time Protocol. The router supports the Network Time Protocol (NTP), which is used to time-synchronize a network of machines.
- SNMP statistics. You can monitor SNMP input and output statistics.
- Syslog/trap alert for FDDI. New syslog messages make it easier to check the status of dynamic resolution and NVRAM problems.
- Interface name changes. Instead of emitting, for example, "Ethernet 0," the system now emits "Ethernet0" on all but the Cisco 7000 series routers. The Cisco 7000 series continues to emit "Ethernet0/0" as it has always done. Because the format of no space between the interface type and number has always been a valid input format, there is little or no user impact.
- PAP. The router supports the Password Authentication Protocol (PAP), which is an authentication feature available on serial lines that use PPP encapsulation.

Configuring Interfaces

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

- Fast switching. By default, fast switching is now enabled on all interfaces that support fast switching. The router supports fast switching of the following protocols: AppleTalk, Banyan VINES, DECnet, IP, IPX, ISO CLNS, source-route bridging, and XNS.

- Subinterfaces. The router supports subinterfaces for Frame Relay, which are multiple virtual interfaces on a single physical interface. Subinterfaces can provide full connectivity on partially meshed Frame Relay networks.
- PPP. OSI, DECnet IV, IPX, XNS, and transparent bridging can be configured over the Point-to-Point Protocol (PPP).
- PPP Magic numbers. Magic number support is available on all serial interfaces. When using PPP, PPP will always attempt to negotiate for magic numbers, which are used to detect looped-back nets.
- Link Quality Monitoring (LQM). This is available on all serial interfaces running PPP. LQM monitors link quality. If the quality drops below a configured percentage, the link will be taken down.
- ATM-DXI. The router supports Asynchronous Transfer Mode-Data Exchange Interface (ATM-DXI), which is a method of synchronous serial encapsulation.
- SPIDs. ISDN interfaces on the router support Service Profile Identifiers (SPIDs) to define the services subscribed to by the ISDN device that is accessing the ISDN service provider.
- Auxiliary port. The auxiliary port on the router can be configured as an asynchronous serial interface.
- IP tunneling. The router supports a tunnel interface, which is a virtual interface. Tunneling is a way to encapsulate arbitrary packets inside a transport protocol. A passenger protocol such as AppleTalk, CLNP, DECnet, IP, or IPX can be encapsulated in IP, which acts as the transport protocol.
- Summary of IP interfaces. A new command, **show interfaces ip-brief**, lists a summary of interfaces, their IP addresses, and status.
- FSIP MIB. The FSIP MIB has been implemented for the Cisco 7000 series.

X.25 and LAPB

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

- X.25 MIB. The router supports the SNMP MIB extension for X.25 LAPB (RFC 1381) and the SNMP MIB extension for the X.25 packet layer (RFC 1382).
- Remote PVC switching. A permanent virtual circuit (PVC) can now be forwarded to another router over a LAN using the TCP/IP protocols via a reliable TCP stream connection.
- Alternate IP addresses. IP addresses in the X.25 routing table can now have up to six alternate routes that will be tried in turn to get a successful connection.
- User identification. You can set a user-defined network user identification in a format defined by the network administrator.

Frame Relay

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

- Support for the Inverse Address Resolution Protocol (ARP). The Frame Relay software supports Inverse ARP, as described in RFC 1293, for the AppleTalk, IP, and IPX protocols. It also supports native hello packets for DECnet and CLNP. Inverse ARP allows a router running Frame Relay to discover the protocol address of a device associated with the virtual circuit.

- Conformity to Internet Engineering Task Force (IETF) encapsulation in accordance with RFC 1294. The IETF form of Frame Relay encapsulation is supported at the interface level and on a per-DLCI (map entry) basis. This encapsulation allows interoperability between equipment from multiple vendors. Encapsulation is supported for the following routing protocols: Apollo Domain, Banyan VINES, DECnet, IP, ISO CLNS, Novell IPX, and XNS. It is not supported for transparent bridging or source-route bridging.
- Frame Relay MIB. The router supports the Frame Relay DTE MIB specified in RFC 1315.
- PVC switching. Frame Relay now supports permanent virtual circuit switching.

SMDS

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

- Multiple logical IP subnet (MultiLIS) support as defined by RFC 1209. This RFC describes how to route IP over an SMDS cloud where each connection is considered to be a host on one specific private network.
- Data Exchange Interface (DXI) version 3.2 with heartbeat. The heartbeat mechanism periodically generates a heartbeat poll frame.
- Support for Banyan VINES. You can configure Banyan VINES over SMDS networks.
- Support for transparent bridging. You can configure transparent bridging over SMDS networks.

Dial-on-Demand Routing

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

- IPX over DDR. IPX packets can now be routed over serial interfaces configured for DDR.
- Odd parity.
- Dial backup over DDR. Dial backup, which allows you to specify a backup when the primary line goes down or when the traffic load on the primary line exceeds the defined threshold, is now supported over DDR.

AppleTalk

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

- Tunneling. Tunneling encapsulates an AppleTalk packet inside the packet of a foreign protocol before sending it across a backbone to a destination router. You can tunnel AppleTalk packets via Cayman tunneling, which enables routers to interoperate with Cayman GatorBoxes, or via Cisco's generic route encapsulation (GRE).
- Show interfaces command. The **brief** keyword has been added to the **show appletalk interface** command. Specifying this keyword displays a summary of interface-related information.
- ARP table entries. To display AppleTalk ARP table entries, you can now use only the **show appletalk arp** EXEC command. The **show arp** EXEC command no longer displays these entries. Also, AppleTalk ARP entries now have interface-specific timeouts.
- Priority queuing is supported for AppleTalk traffic.

Banyan VINES

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

- Variable routing update timers. You can now control the interval at which the router sends routing updates, and you can now modify the way that routing information is propagated across the network.
- Load-sharing. The VINES routing tables now maintain multiple paths to each neighbor station, load-share traffic to a neighbor between the set of paths having the lowest cost metric, and allow you to enter static paths to neighbors. Similarly, the routing tables now maintain multiple paths to each server, load-share traffic to a server between the set of paths having the lowest cost metric, and allow you to enter static paths to servers. The output displayed by the **show vines neighbor** and **show vines route** EXEC commands has been changed to reflect the load-sharing support.
- Time-of-day support. The software can now process and generate time-synchronization messages, can authoritatively source local time into the VINES time system (useful when running NTP locally), and can use the VINES time system to set a local clock (such as the Cisco 7000 clock).
- Fast switching. You can now fast switch packets being transmitted out of a VINES interface.
- New IPC layer. A VINES IPC layer has been added, and you can now display all active IPC connections.
- Priority queuing is supported for Banyan VINES traffic.

DECnet

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

- Congestion avoidance. You can now set the congestion threshold. If the number of packets in the router's output queue exceeds this threshold, the congestion-experienced bit is set.
- Advertise feature. You can now explicitly configure which DECnet Phase IV areas to be propagated outwards.
- Ping command. The **ping** command has been extended to handle DECnet Phase IV pings. Also, a user-level (unprivileged) **ping** command is now provided.
- Clear DECnet counters. You can now clear all DECnet counters.

IP and IP Routing Protocols

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

- Route maps. This feature creates tags for each route. These tags are then used to influence route redistribution.
- Integrated IS-IS. The IS-IS routing protocol has been implemented for TCP/IP.
- IPSO enhancements. The authority fields were updated to support RFC 1108. Also, there is a new feature that allows routers to treat packets that have the Reserved1-Reserved4 security levels as invalid. Normally, reserved packets are not allowed.
- Configuring OSPF network and type. You can now configure broadcast networks as nonbroadcast, multiaccess networks, and you can now configure nonbroadcast, multiaccess networks (such as SMDS, Frame Relay, and X.25) as broadcast networks.
- DNS name lookup for OSPF. You can now look up DNS names and use them for OSPF displays.

- IP access lists. When you apply a standard or an extended access list that has not yet been defined to an interface, the router acts as if the access list had not been applied to the interface and accepts all packets. Remember this behavior if you use undefined access lists as a means of network security. Note that you cannot use extended access lists when autonomous switching is enabled.
- IP autonomous switching. IP autonomous switching is now supported over Frame Relay and PPP.
- Ping command. A user-level (unprivileged) **ping** command is now provided.
- BGP weight ranges have been changed.
- BGP sessions. The router can now allow BGP sessions even when the neighbor is not on a directly connected segment. Also, you can now configure the router to allow BGP sessions even when the outbound interface goes down.
- Next-hop processing on BGP updates. You can now configure the router to disable next-hop processing on BGP updates. This is useful in nonmeshed networks such as Frame Relay or X.25 where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.
- Neighbor templates. You can now configure neighbor templates that use a word argument rather than an IP address to configure BGP neighbors. This is an advanced feature requiring a well-thought-out network architecture. Do not use this feature without thoroughly understanding its implications.
- Inbound access lists. You can now apply access lists on inbound interfaces.
- IRDP multicast. You can now send IRDP advertisements to the all-systems multicast address (224.0.0.1) on the specified interface.
- IP network masks. You can now display the masks used for network addresses and the number of subnets using each mask.
- OSPF virtual links. You can now display the parameters and current state of OSPF virtual links.
- Routing table. You can now display a summary of the current state of the routing table.
- Trace command. A user-level (unprivileged) **trace** command is now provided. Use this command to discover the IP routes that packets will actually follow to their destination.
- IP default gateway. You can now display the address of a default gateway (router).
- Invalidation rate. You can now control the invalidation rate of the IP route cache.
- Command syntax changes:
  - The syntax of the OSPF **neighbor** router configuration command has changed. The *interface* argument was removed because the interface can be determined from the specified IP address.
  - The syntax of the **show ip ospf neighbor** EXEC command has changed.

ISO CLNS

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

- Route maps. This new feature creates tags for each route. These tags are then used to influence route redistribution. Route maps apply to IS-IS.
- Ping command. A user-level (unprivileged) **ping** command is now provided.
- CLNP performance improvements. The performance of CLNP fast switching and process switching has been improved.
- OSI access lists (filter expressions). You can now use access lists to control OSI traffic.

- Integrated IS-IS. The IS-IS routing protocol has been implemented for ISO CLNS.
- DNS support for CLNP. You can now perform DNS queries for CLNS addresses using the documented NSAP type. By default, this function is on.
- ISO-IGRP split horizon. You can now perform split horizon of ISO-IGRP updates.
- ISO-IGRP timers. You can now configure ISO-IGRP timers.
- ISO-IGRP metric constants. You can now configure the metric constants used in the ISO-IGRP composite metric calculation.
- Displaying routing tables. The new **which-route** EXEC command shows which routing table a particular OSI destination was found in. The route can reside in the IS-IS Level 1 routing table, the ISO-IGRP system ID or area routing table, the prefix routing table (for IS-IS Level 2 routes, ISO-IGRP domain routes, and static routes), or the adjacency database.
- ESCT option. The new **clns esct-time** interface configuration command supplies an ES Configuration Timer (ESCT) option in a transmitted IS hello packet. The ESCT option tells the end system how often it should transmit ES hello packet protocol data units (PDUs).

Novell IPX

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

- Novell IPX compliance. Cisco routers have been certified as providing full IPX router functionality. You can control specific aspects of the router's IPX compliance.
- Autonomous switching. IPX now supports autonomous switching on AGS+ systems with a ciscoBus2 and on the Cisco 7000.
- GNS processing. The router now uses a round-robin algorithm when process Get Nearest Server (GNS) requests.
- SAP filtering. You can now create SAP access lists for filtering the output of GNS requests.
- Displaying SAP services. You can now display known SAP services by type, cost metric, and name.
- Encapsulation. You can now encapsulate packets in SNAP (Novell's Ethernet_Snap frame type) and SAP (Novell's Ethernet_802.2 frame type) formats.
- Multiple logical networks (multiple Novell encapsulations over a single interface). You can now configure multiple logical networks on an interface. This allows several logical networks to share the same physical medium. The encapsulation type for each logical network must be different so that the router can determine which packets belong to which network.
- IPX over DDR. IPX packets can now be routed over serial interfaces configured for dial-on-demand routing (DDR).
- Type 20 propagation packets. New commands now provide addition control of the forwarding of NetBIOS type 20 propagation broadcast packets.
- Odd-length packets. You can now pad odd-length, process-switched packets so that they are sent as even-length packets.
- Priority queuing is supported for Novell IPX traffic.

Transparent Bridging

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

- Autonomous bridging. This high-speed switching feature allows bridged traffic to be forwarded and flooded on the ciscoBus2 between resident interfaces. It is available on the MEC, FCIT transparent, HSSI HDLC, EIP, FIP, and HIP interfaces.
- Support for RFC 1286. Cisco supports all the mandatory MIB variables specified for transparent bridging in RFC 1286.

Obsoleted Features

This section lists the protocols, device drivers, and boards supported in earlier router software releases that are not supported by Software Release 9.21.

Protocols

The following protocols are no longer supported:

- The CHAOSnet routing protocol is a local-area network protocol developed at the Massachusetts Institute of Technology.
- The IP IEN-116 name server system.
- The HDH protocol (also known as the HDLC Distant Host, or 1822-J, protocol) is a protocol similar to X.25 that is used for attaching to the Defense Data Network.
- The HELLO protocol, as described in RFC 891, is an interior routing protocol developed for the Fuzzball gateways of the Distributed Computer Network project and was used extensively in the early NSFnet backbone network. It is different from the OSPF Hello protocol.
- The PUP routing protocol, Xerox's PARC Universal Protocol.

Device Drivers

The following device drivers are no longer supplied with the router software:

- ACC 1822 card
- Netronix Token Ring
- Parallel printer
- SBE serial (CSC-T and CSC-S)
- Type 1 (3Com) Ethernet
- Type 2 (Interlan) Ethernet
- UltraNet
- 3-MB Ethernet

Cards

Software Release 9.21 does not support the CSC-E card, which is an older Ethernet card. If you have this card, the software will boot, but the interface will not start.

Important Notes

This section describes warnings and cautions about using the Release 9.21 software. The information in this section supplements that given in the section “Release 9.21(7) Caveats” later in this document.

This section discusses the following topics:

- Modifying Cisco 7000 Serial Interfaces
- Cisco 2500 Console Ports
- Using Candidate Default Routes in IP Enhanced IGRP
- Odd-Length Novell IPX Packets
- IPX Type 20 Packet Propagation
- IPX GNS Response Delay
- Forwarding of Locally Sourced AppleTalk Packets
- SMDS DXI

Modifying Cisco 7000 Serial Interfaces

Changing parameters on Cisco 7000 serial interfaces by issuing encapsulation-related interface configuration commands can cause the route processor to repartition the buffers used for memory. This has the effect of resetting the CxBus complex, which comprises the Switch Processor and all the interface processors.

Cisco 2500 Console Ports

Cisco router console ports do not support software (XON/XOFF) or hardware (RTS/CTS) flow control. However, on all routers except the Cisco 2500 series, the console port is wired to connect RTS and CTS. This means that a terminal using hardware flow control sees CTS in response to asserting RTS, and communication between the terminal and the router works properly.

On the Cisco 2500 series, this is not possible. The result is one-way-only communication between the terminal and the Cisco 2500 console port: you will be able to see output from the router on the terminal, but you cannot type anything in. The workaround is to disable hardware flow control on the terminal or to strap the CTS high.

Using Candidate Default Routes in IP Enhanced IGRP

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 Software Release 9.21(4.4), IOS Release 10.0(4.1), IOS Release 10.2(0.6), and later Cisco versions. Upgrade all routers to Software Release 9.21(4.4), IOS Release 10.0(4.1), and IOS Release 10.2(0.6) or later.

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

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

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

Odd-Length Novell IPX Packets

In previous releases, it was possible to force padding of odd-length IPX packets sent on FDDI and serial interfaces by simply disabling fast switching on an interface. This action corrected packet length problems in certain topologies running older software releases. In this situation, it is now necessary to add a new configuration command.

In Software Release 9.21, the default behavior when process switching is identical to fast switching: odd-length IPX packets are always padded on Ethernet interfaces and never padded on FDDI or serial interfaces. To force padding of odd-length packets on such an interface you must disable fast switching as well as issue the following new interface configuration command:

ipx pad-process-switched-packets

IPX Type 20 Packet Propagation

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

ipx type-20-packet-propagation

Note that it will be necessary for you to modify existing configurations if type 20 packet propagation is desired.

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

IPX GNS Response Delay

The original default of the **ipx gns-response-delay** command was 500 ms. This value fixes an issue in NetWare 2.*x* with dual-connected servers in parallel with a router. NetWare 2.*x* was the most common release. NetWare 3.*x* and later do not have the same issue, and a nonzero GNS response delay may cause problems in certain situations. The default of the **ipx gns-response-delay** command has been changed to 0.

Forwarding of Locally Sourced AppleTalk Packets

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

SMDS DXI

By default, the Release 9.21 version of SMDS DXI starts in DXI3.2 mode. However, Release 9.1 does not support SMDS DXI. In order for routers running Release 9.21 and Release 9.1 to interoperate, you must disable DMDS DXI on the router running Release 9.21 using the **no smds dxi** interface configuration command.

Release 9.21(7) Caveats

This section describes possibly unexpected behavior by Release 9.21(7). Unless otherwise noted, these caveats apply to all 9.21 releases up to and including 9.21(7). The caveats listed here describe only the serious problems. For a most current list of caveats against this release, access CIO as described in the section "Cisco Information Online" later in this document.

DECnet

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

IBM Connectivity

- When IPX routing is enabled on a Token Ring interface and there is a source-route bridge network behind the ring, a **multiring ipx all** command is used to cache the RIF in the router. During normal operation all is well. But when a station is moved from one ring to another ring (for example, from 0B8 to 0B1), the station cannot reach the server. Looking at the RIF cache on the AGS+, it is fine. However, by analyzing the frames with a Sniffer, we can see the "create connection request" from the station with a good RIF field, but the answer from the AGS+ shows the previous RIF (the RIF before the station was moved). The workaround is to disable the IPX route cache or to clear the IPX cache when a station is moved. This is a general problem with all routed protocols. The RIF code does not inform the routing protocols when an entry in the table changes. Therefore, the cache entries become invalid. [CSCdi17099]

Interfaces and Bridging

- The Cisco 4000 FDDI interface may not be able to receive traffic smoothly under very heavy loads (greater than 14,000 packets per second), in which case the incoming traffic will only be accepted in small bursts every 10 seconds, until the load falls below that critical threshold. [CSCdi10848]
- When a configuration change occurs that causes the Token Ring interface to initialize, there is a delay between the time the command is entered and the initialization process begins. The Token Ring initialization also impedes other process-level functions. [CSCdi16454]
- Texas Instruments has stopped production of the TMS380C16 and switched to the TMS380C26 Token Ring chip. The new chip disables the SRA (source router accelerator chip) when the TMS380C26 chip is in promiscous mode. This means that the Token Ring interface can no longer support both source-route bridging and transparent bridging on the same interface. Whenever transparent bridging is turned on, the source-route bridging ceases to function. The TMS380C26 chip is used in Cisco 2500, Cisco 4000, and Cisco 4500 routers. [CSCdi22815]

Release 9.21(6) Caveats/Release 9.21(7) Modifications

This section describes possibly unexpected behavior by Release 9.21(6). Unless otherwise noted, these caveats apply to all 9.21 releases up to and including 9.21(6). For additional caveats applicable to Release 9.21(6), see the caveats sections for newer 9.21 releases. The caveats for newer releases precede this section.

The caveats listed here describe only the serious problems. For a most current list of caveats against this release, access CIO as described in the section "Cisco Information Online" later in this document.

All the caveats listed in this section are resolved in Release 9.21(7).

AppleTalk

- AppleTalk ports can get stuck in the restart state when system uptime is greater than 24.85 days. There is no workaround; you must reload the system. [CSCdi25482]
- Global Appletalk ARP commands have a side effect of changing the router ID number for AppleTalk Enhanced IGRP. There is no workaround. [CSCdi25786]
- If AppleTalk is started after the router has been up for more than three weeks, RTMP updates will not be sent out of the router. The workaround is to enable AppleTalk before the router has been up for three weeks, or to reboot the router before enabling AppleTalk. [CSCdi26137]

Interfaces and Bridging

- When TCP/IP routing is enabled along with transparent bridging on the same interface, some SNAP encapsulated TCP/IP packets with destinations on the same network segment may be bridged to other networks. [CSCdi23944]
- When multiple FDDI cards are present in the router, the interfaces in the lower slot positions may lose their downstream neighbors. [CSCdi25764]
- Hitachi-based serial ports might not transmit under a severe load because the underrun interrupt is not properly enabled. [CSCdi26209]

VINES

- The VINES RIF cache becomes corrupted when an end station does an all routes broadcast/nonbroadcast return. The problem is that the router returns a corrupt RIF to the end station. [CSCdi23239]
- When the **vines serverless broadcast** command is configured in a redundant topology and all other router interfaces are configured with the **vines serverless** command, a broadcast storm results. [CSCdi25597]
- When fast switching VINES over a source-route bridged Token Ring network, the router does not build its fast-switching cache entries properly. This prevents communication with stations that are across a bridge from the router. The workaround is to disable fast switching on the Token Ring interface. [CSCdi26288]

Wide-Area Networking

- Routing by NSAP for CMNS does not work. [CSCdi25326]

- The Frame Relay broadcast queue might exhibit drops under high broadcast volume. There will be an increase in "buffer element" misses at the same time the drops happen. [CSCdi25707]

Release 9.21(5) Caveats/Release 9.21(6) Modifications

This section describes possibly unexpected behavior by Release 9.21(5). Unless otherwise noted, these caveats apply to all 9.21 releases up to and including 9.21(5). For additional caveats applicable to Release 9.21(5), see the caveats sections for newer 9.21 releases. The caveats for newer releases precede this section.

The caveats listed here describe only the serious problems. For a most current list of caveats against this release, access CIO as described in the section “Cisco Information Online” later in this document.

All the caveats listed in this section are resolved in Release 9.21(6).

DECnet

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

EXEC and Configuration Parser

- The **access-expression** [**in** | **out**] *expression* interface configuration command is written to configuration memory as a filter for both inbound and outbound packets. [CSCdi24000]

Interfaces and Bridging

- On Cisco 2502 and Cisco 2504 routers, IP and IPX packets of length 920 to 1050 bytes being routed from Token Ring to serial interfaces may be corrupted. The workaround is to disable fast switching on the serial interface. [CSCdi19480]

IP Routing Protocols

- When load balancing IP traffic over multiple equal cost paths, the system’s routing table may reach an inconsistent state, leading to a system reload. Before the inconsistent state is reached, the system must have 3 or 4 equal cost paths for a particular route. A routing update must then be received which causes the system to replace those paths with fewer (but still more than 1), better metric paths. This route must then become used for further locally generated traffic. This problem is most likely to be seen after an interface flap in an environment where there are redundant, but not symmetric, interconnections between routers. The problem also seems more likely in FDDI environments, where interfaces flap before fully coming up. These flaps can result in multiple back-to-back routing table changes. [CSCdi20674]
- Enabling the Hewlett-Packard IP Probe protocol via the **ip probe proxy** command does not correctly enable the protocol. There is no workaround for this behavior. [CSCdi23909]

ISO CLNS

- For serial, nonpoint-to-point interfaces in the configuration

  A --------/----------B ---------- C

  when the remote router (router A) comes up, the middle router (router B) should send a routing update immediately. This is not happening. Rather, the update gets sent after 15 minutes. [CSCdi17808]

- When changing the encapsulation on a serial link from a point-to-point mode (such as HDLC or PPP) to a "cloud" mode (such as SMDS or Frame Relay), IS-IS routing fails to consider the interface as broadcast media. Because of this, the CSNP will not be exchanged and hence the database will not be synchronized. To work around this problem, unconfigure and configure ISIS after changing the encapsulation type. [CSCdi23691]

Novell IPX, XNS, and Apollo Domain

- The interface configuration command **ipx watchdog-spoof** fails to properly enable Novell watchdog timer spoofing. There is no workaround for this behavior. [CSCdi23324]

VINES

- The VINES routing code was building neighbor entries based upon the first RTP packet seen. If the first packet happens to be an SRTP packet, then a neighbor entry is built from invalid data. (Release 9.21 does not understand the SRTP frame format.) This bad neighbor entry can cause a chain of events that leads to a router crash. [CSCdi22826]
- When using a BRI interface as a backup interface, and the backup is being done based on load, the BRI interface may be taken down prematurely, even though the load is still high. [CSCdi20472]
- When using IPX over PPP, if the node number is not acknowledged, we continue to ask to negotiate it. [CSCdi24078]

Release 9.21(4) Caveats/Release 9.21(5) Modifications

This section describes possibly unexpected behavior by Release 9.21(4). Unless otherwise noted, these caveats apply to all 9.21 releases up to and including 9.21(4). For additional caveats applicable to Release 9.21(4), see the caveats sections for newer 9.21 releases. The caveats for newer releases precede this section.

The caveats listed here describe only the serious problems. For a most current list of caveats against this release, access CIO as described in the section "Cisco Information Online" later in this document.

All the caveats listed in this section are resolved in Release 9.21(5).

AppleTalk

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

IBM Connectivity

- When applying NetBIOS access lists with **rsrb remote-peer** access list statements on a system with active SRB traffic, the router may reload due to a bus error. The fix changes the system code so that it handles these conditions in a more graceful manner. [CSCdi18993]

IP Routing Protocols

- In OSPF, when a neighbor goes down, a host route for that neighbor is incorrectly added. A possible workaround is to trigger the rebuild of OSPF router link state advertisement by changing interface metric or reboot. [CSCdi21103]

ISO CLNS

- Fast switching fails if the padding option is on for CLNS packets. The router would drop from fast switching to process switching. [CSCdi20346]

Novell IPX, XNS, and Apollo Domain

- The original GNS response delay of 500 ms was put into place when NetWare 2.*x* was the most common release to fix an issue with dual-connected servers in parallel with a router. NetWare 3.*x* and later does not have the same issue, and a GNS response delay may cause problems in certain situations. The new GNS response delay default will be 0. [CSCdi22285]

VINES

- If the router is maintaining a large table of VINES neighbors and many of those neighbors were learned via RTP redirects, the router will appear to "pause" once every 90 seconds for a couple of seconds. [CSCdi21257]

Wide-Area Networking

- Priority queuing is not supported on BRI interfaces. [CSCdi18843]
- There are times when the **show smds map** command would enter an infinite loop when the right combination of static map entries exist in the configuration. This would only happen if two protocol addresses would hash into the same location. [CSCdi21239]
- When X.25-over-TCP (XOT) sends a Call Confirm that modifies one of the two proposed flow control facilities (window sizes or maximum packet sizes), the values may be set to 0, which is illegal. [CSCdi21602]
- When the system is using Frame Relay maps that were created using Inverse ARP, these maps should be dropped when a DLCI becomes inactive or is deleted. In addition, if the DLCI used by a box at the far end changes, the map entry should be updated. The second scenario might occur when Frame Relay is being accessed using dial-up service and the far end systems makes two calls in rapid succession. [CSCdi21870]
- Dialer rotary groups do not work because they are unable to dial out a phone number. [CSCdi22715]

Release 9.21(3) Caveats/Release 9.21(4) Modifications

This section describes possibly unexpected behavior by Release 9.21(3). Unless otherwise noted, these caveats apply to all 9.21 releases up to and including 9.21(3). For additional caveats applicable to Release 9.21(3), see the caveats sections for newer 9.21 releases. The caveats for newer releases precede this section.

The caveats listed here describe only the serious problems. For a most current list of caveats against this release, access CIO as described in the section "Cisco Information Online" later in this document.

All the caveats listed in this section are resolved in Release 9.21(4).

AppleTalk

- Executing the **show apple interface** command may cause the system to restart itself. This would happen in interfaces configured with many zones. [CSCdi18875]
- If the router's configuration contained the global configuration command **appletalk lookup-type**, the router would crash with a bus error. [CSCdi19463]

Basic System Services

- Under rare circumstances, the **clear line** command fails to clear the process running on that line. A **show process** command shows that the process on that line has an inappropriate and rapidly increasing number in the "invoked" column. [CSCdi16063]
- If a SAP update packet is received with an invalid length, much larger than the data actually contained in the packet, the system may reload. It is also possible, but unlikely, that invalid server entries may appear in the **show ipx server** table. When these packets are received, they should be counted as SAP format errors and the counter on **show ipx traffic** should increment. [CSCdi19010]

DECnet

- DECnet packets received on the FDDI interface of a Cisco 4000 router are always sent to the system processor for processing, ignoring the setting of the **decnet route-cache** interface attribute. This caveat was introduced in the 9.21(1) release. [CSCdi19689]
- While converting from DECnet Phase IV to Phase V (and vice versa), the router holds back a converted packet once in a while and sends it out when some other event happens (for example, routing update, keepalives). This sporadic delay in packet transmission results in degradation of end-to-end DECnet performance. [CSCdi20151]
- The problem reported here occurs because of incorrect interface MTU negotiation, and will be seen on any interface whose default MTU is larger than the Ethernet MTU (for example, FDDI). When the VAX comes up, the router ends up negotiating a block size that is larger than the maximum value that we are willing to process (1524). Consequently, all adjacent routers end up sending larger sized updates, which we reject. This makes all destinations behind the router unreachable. [CSCdi20225]

EXEC and Configuration Parser

- Starting in Release 9.21, with the new parser, the **ip split-horizon** command is generated before the **encapsulation** command in the configuration file during NVGEN. As the encapsulation command has a different default for turning on/off the split-horizon feature for different encapsulation, the [**no**] **ip split-horizon** command may disappear from the configuration after rebooting because it is overridden by the default value of the encapsulation in used. This fix ensures the **ip split-horizon** command comes after the **encapsulation** command in the configuration file. [CSCdi19006]

IBM Connectivity

- FEP-to-FEP local acknowledgment sessions blocked due to after SDLC-TG packet SQN=1 was delivered before packet SQN=0. The code has been optimized to prevent this from happening (automatic resequencing). [CSCdi17904]
- A nonblocking process is trying to dismiss itself. The result is a continuous printout of the following message, such that the system is effectively hung:

  ```
  %SYS-2-NOBLOCK: event dismiss with blocking disabled
  ```

  This occurs at high data rates and the offending process needs to be identified and brought into line with the dismiss rules. [CSCdi17931]
- If an RSRB remote-peer is defined but not currently in use, the router may reload due to a software forced crash. [CSCdi17934]
- After running for an extended period of time with remote source-route bridging configured, the console may display "%SYS-2-LINKED: Bad enqueue of *nnnnnn* in queue *nnnnn*" messages, followed by a traceback message containing several hex numbers. Remote source-route bridging will continue to function normally. [CSCdi18003]
- In low-end routers such as the Cisco 4000 and Cisco 3000, the Token Ring interface ignores IP packets that have single-route or all-route broadcast RIF. The correct behavior is to accept the packet and subsequently route it when IP routing is turned on. [CSCdi18131]
- When source-bridge translational bridging is used in a dual TIC (Token Ring interface) environment, the RIF is cached for the first return explorer from the destination. Subsequently, if another return explorer from the same destination is seen with a shorter RIF, the RIF cache on the router is updated. This causes the end-stations to reinitiate their sessions. The correct behavior for source-bridge translational bridging in a dual TIC environment is to cache the shortest RIF based on the fastest return and locks it. A timer is then started. If there is no packet from the destination and timer expires, the RIF cache for the destination is removed. Subsequently, new returns from an alternate route may be cached. If there are packets from the destination station, then the RIF from the cache is applied and the timer is reset. [CSCdi18169]
- In a local acknowledgment environment incoming disconnect packets where not handled properly and remained on the input queue. The Token Ring input queue would fill up completely and cause continuous Token Ring resetting. [CSCdi18222]
- A reverse Ethernet SDLLC configuration with local acknowledgment enabled may cause a reload due to a software forced crash (jump to zero). [CSCdi19067]
- Use of **rsrb remote-peer 100 tcp** *n.n.n.n* **lsap-output-list** *number* causes a slow memory leak under heavy RSRB load. The **show process memory** command will show an increasing amount of memory taken by the SRB background process. [CSCdi19106]

- The **stun cos-enable** command causes unnecessary FID4 frame resequencing. The network gains no benefit and the routers are performing unnecessary work, so the feature is being removed. In addition, the feature was causing packets to be delivered out TG-sequence, which in rare occasion causes blocking TGs. [CSCdi19357]
- When the T1 timer is coded too short on a multidrop SDLC line, SDLC messages of the form "data from wrong address! got address" (where are SDLC poll addresses in hex) appear on the console. In a large multidrop configuration, the amount of these messages is excessive. The code changes this behavior so that the messages appear only when **debug sdlc** is turned on. Note that these messages are informational only and that polling of the down-stream SDLC devices does continue. [CSCdi19376]
- In a local acknowledgment startup phase, the router was dropping the first I-frame received when the peers were still in pending state. For some end stations, this causes session startup failures. [CSCdi19999]
- This fix allows an FEP operating as a secondary SDLC station to load a remote FEP operating as a primary SDLC station. The opposite has been possible since 9.1(9). Before a FEP is loaded with an NCP gen, it does not have an SDLC role. The SDLC role is negotiated via XID exchange when the remote FEP is activated. [CSCdi20463]

Interfaces and Bridging

- On Cisco 7000 systems with a Serial Interface Processor (SIP) installed (not the FSIP), removing or replacing an EIP, TRIP, or other interface cards may cause the router to execute a system reload. [CSCdi13319]
- Under certain rare conditions, the Token Ring interface would erroneously increment the token error counter. This counter can be seen with the **show controller token** command. [CSCdi17292]
- Remote transparent bridging configured for PPP encapsulation fails for AppleTalk Phase 2, CLNS, and Apollo protocols. [CSCdi18136]
- On Cisco 4000 routers that are running XX-K images and that have bridging configured between FDDI and serial interfaces, if there is a **bridge-group** *group* **output-type-list** *list* interface configuration command [CSCdi18464]
- SRB frames are garbled when switching from Token Ring to FDDI. Turning off RSRB fast switching at the Token Ring interface (**no source-bridge route-cache**) clears the problem. [CSCdi18478]
- In systems configured to support the spanning-tree bridging protocol, the root bridge BPDUs reappears at the root bridge in a HSSI environment. [CSCdi18812]
- On the Cisco 3000 series routers, when using dial-on-demand routing, a transition of CTS or DSR can appear as a transition of DCD when spoofing. [CSCdi19053]

IP Routing Protocols

- If the router is configured for routing Enhanced IGRP and IGRP with the same process number, the system crashes under configuring **no router igrp process-number**. [CSCdi18710]
- The router and communication servers allow remote users to Telnet into VTY ports by connecting to ports 20xx/40xx/60xx/80xx. All the standard VTY/TTY security features, such as passwords, tacacs, and the ability to block access with the **access-class in** command have always been supported, even when connecting to a high port. However, because many customers are unaware of this functionality, they do not take it into account when constructing packet filtering

firewalls. Because this functionality can be explicitly enabled and configured by use of the VTY rotary feature, the default behavior is not necessary. This is not a security bug or hole, but rather a behavior that should be avoided as a matter of prevention due to its obscurity. [CSCdi20050]

- OSPF can choose and install nonoptimal interarea and external routes when there are multiple link state advertisements for the same destination advertised by multiple area border routers (or autonomous system boundary routers for external routes). This can cause a routing loop if other neighboring routers still install the shortest path to the destination. This problem will happen only after the system has been up for a period of time. The length of this period depends on how much connectivity changes have occurred. In a fairly busy network, the estimated length of this period is around five to six weeks. [CSCdi20071]
- After an OSPF router installed a default route to network 0.0.0.0 that is advertised in an external link state advertisement (LSA) by an autonomous system boundary router (ASBR) and there is any connectivity change happens in the network that triggers SPF calculation, the router will not reinstall the default route. This problem is introduced in the following software version: 9.1(11.4), 9.17(9.2) and 9.21(3.1). [CSCdi20401]

ISO CLNS

- The IS does not put dynamically learned ESs over point-to-point links in the L1 LSP, so the other ISs do not have a route to that ES. [CSCdi18856]

Novell IPX, XNS, and Apollo Domain

- When an interface goes down some of the routes learned through that interface may be left in the routing table in an unusual state, and error message is displaying saying there is a path mismatch for these routes. The **show ipx route** command display may not show the entire routing table. In the correction for this condition the routes will be in the table for one minute after the interface goes down but will display on **show ipx route** "No current path." After one minute, they will be completely removed from the routing table. [CSCdi19664]
- The router hangs in cbus_ipxcache_invalid in Release 10.0(0.20). While running an overnight multiprotocol test on a Cisco 7000 with autonomous IPX enabled on Token Ring, the router is spinning in a loop inside cbus_ipxcache_invalidate. [CSCdi20321]

TCP/IP Host-Mode Services

- TCP segments arriving out of order (due to packet losses or redundant paths) were not being removed from the TCB's save queue on TCP driver-managed connections. This condition causes even more packet drops, and conditions degenerate badly until throughput drops very low. The features affected by this problem are RSRB/TCP, STUN/TCP, and X.25 remote switching. [CSCdi18582]

VINES

- If VINES is already enabled, reissuing the command **vines routing** after it has already been specified may cause a software failure. This exists only in the 9.21(2.6) and 9.21(2.7) releases. [CSCdi19291]
- Prevent potential timer problems when the high-order bit of the timer changes or when a timer wraps around. [CSCdi19877]

- VINES potential memory corruption found in 9.21 and 10.0. The VINES code is currently taking a pointer in the VINES BSS data space, and treating it as a VINES idb pointer. Depending upon the pre-existing contents of memory in these locations, the code might overwrite random memory in the VINES BSS area thus causing unexpected results. [CSCdi19977]
- If VINES users have login location restrictions configured, it is possible that the router will reload when queried by the user's home server. [CSCdi20165]

Wide-Area Networking

- The 9.14 code merge added Token Ring and FDDI fast switching to 9.21; however, PPP was forgotten (not in 9.1, but already in 9.21). The PPP encapsulation is added to HDLC, Frame Relay, and SMDS as a valid encapsulation. [CSCdi12076]
- On MCI/Cbus serial cards, when DDR is configured with priority queueing, a packet may get stuck in the output queue and released only when the next packet replaces it in the queue. This one-packet delay may cause packets to be delayed, increasing response time or causing packet drops in case of timeout. [CSCdi17666]
- In X.25 environments, the message "System restarted by error - Jump to zero" appears. If you do a **show stack**, you will see a two-line stack trace. The cause is related to failed PAD Calls; an area of memory is modified after it has been returned as no longer in use. Under circumstances of heavy load and/or slow X.25 performance this invalid reference may modify critical data, causing unpredictable results. [CSCdi17688]
- AppleTalk zones are not set when running over a Frame Relay point-to-point subinterface. This problem is caused by incorrect DLCI mapping by the router. [CSCdi18233]
- When a router is configured for **encap frame-relay ietf**, ARP requests received on this interface are dropped. When configured for IETF encapsulation, the router sends only inverse ARPs and drops the ARP requests. [CSCdi19107]
- DLCIs that have been deleted will still show up as active in the **show frame-relay map** command. [CSCdi19127]
- All non-IP packets were being transmitted into the SMDS cloud using the SMDS bridge multicast address. Users could not Telnet into bridge routers from remote hosts. All non-IP packets now use the address stored in the spanning tree tables, which should be all unicast E.164 addresses. [CSCdi19248]
- Cisco routers with an ISDN BRI interface running the basic-dms100 or basic-ni1 switchtype may have B-channels become unavailable for usage. This may occur if there are long dialing delays for outgoing calls through an ISDN network. Also, when a call is connected on Channel B2 and the dialer idle timer attempts to hang up the call. The B-channels may become stranded and unavailable for usage. [CSCdi19671]
- A router with an ISDN BRI interface using switchtype basic-net3 or basic-ts013 may run out of memory. This may occur after the successful completion and disconnection of a number of outgoing calls. The **debug isdn-event** will indicate that an outgoing call is being placed, but no call will be made. [CSCdi20437]
- Protocols other than IP and CLNS over IETF Frame Relay will not interoperate with RFC 1294 compliant devices when the pad byte in the frame header is of size zero. [CSCdi20942]

Release 9.21(2) Caveats/Release 9.21(3) Modifications

This section describes possibly unexpected behavior by Release 9.21(2). Unless otherwise noted, these caveats apply to all 9.21 releases up to and including 9.21(2). For additional caveats applicable to Release 9.21(2), see the caveats sections for newer 9.21 releases. The caveats for newer releases precede this section.

The caveats listed here describe only the serious problems. For a most current list of caveats against this release, access CIO as described in the section "Cisco Information Online" later in this document.

All the caveats listed in this section are resolved in Release 9.21(3).

Basic System Services

- If the source-route bridging is used, the LAN Network Manager functions such as CRS, REM, and RPS are automatically enabled. An error in the system code causes rapid accumulation of small buffers. The workaround is to add the configuration statement **no lnm crs**. [CSCdi16384]

DECnet

- Connect initiate packets sent to a Phase V cluster alias cause the router to display SYS-2-INLIST messages. This does not happen if the packets are sent to a "real" address. [CSCdi16801]

IBM Connectivity

- The SDLLC local acknowledgment feature may not enable properly despite being configured correctly due to an internal code error. [CSCdi16675]
- Due to the incorrect frame translation when SR/TLB is enable, the **bridging access-list input-lsap-list** and **bridging access-list output-lsap-list** commands fail to stop the frame correctly. [CSCdi17037]
- During SDLLC start up, the system does not respond to the XID POLL frame sent by some upstream devices that require a response to properly bring up the LLC2 session. [CSCdi17093]
- The **netbios access-list** feature does not function properly for permit/deny decisions against NetBIOS names that contain special nonalphanumeric characters. The workaround is to change the NetBIOS names of the end stations to use only alphanumeric characters. [CSCdi17163]
- Reverse Ethernet SDLLC configurations do not work properly under certain conditions. [CSCdi17314]
- A system reload may happen while configure source-route bridging, and a **no vines routing** is entered. [CSCdi17862]
- When you enter the **source-bridge proxy-netbios-only** command, it is put in the configuration file as **source-bridge cos-enable**. This is an unrecognized command. You have to enter **no source-bridge proxy-netbios-only** to get the **source-bridge cos-enable** command out of the configuration. [CSCdi17997]
- When trying to open more than one FST remote peer version 3 connection, only one peer can open successfully. The remaining FST remote peers stay in a closed state. The workaround is to use TCP or direct encapsulation. [CSCdi18117]

- The router fails to accept the command sequence **sdlc rts-timeout**, **sdlc cts-delay** even though the interface is configured for half duplex. After the command is entered, the following message will be displayed on console: [CSCdi18135]

```
SDLC : rts-timeout only applies to half duplex interfaces.
SDLC : cts-delay only applies to half duplex interfaces.
```

- The configuration command does not allow the **no source-bridge active** configuration command to remove the SRB definition from a Token Ring interface. [CSCdi18280]
- The old default SDLC hold queue depth of 50 is too low in some configurations and does not allow sufficient time to apply back pressure on the LLC connection before packets are dropped. The default SDLC hold queue value has been changed to 200. The value is still user configurable via the **sdlc holdq** interface configuration command. This problem is most likely to be an issue in configurations with high-speed RSRB connectivity feeding a slow-speed SDLC line. [CSCdi18461]
- The local acknowledgment feature of remote source-route bridging sends a SABME to the end station with the incorrect direction bit set in the RIF portion of the MAC frame. [CSCdi18617]
- The **show source-bridge** command does not count autonomously switched frames. [CSCdi18714]

Interfaces and Bridging

- When transparent bridging is enabled on Multibus Token Ring cards, the monitor bit is not cleared in the token when the packet is flooded to another Token Ring interface.The active monitor on the destination ring will see this bit set, assume the packet has already passed around the ring, purge it, and reissue a new free token. The workaround for this problem is to add a static bridge table entry for each destination address, for example, **bridge 1 addr 0208.6ce2.088e forward t 0**. Note that the address must be in Ethernet canonical format.This ensures that packets destined for this address will not have to be flooded via transparent bridging.This problem may not happen consistently, since the location of the active monitor on the destination ring may change over time. [CSCdi12451]
- A Cisco 4000 FDDI interface goes into administratively down status and stays there. A **show interface fddi** includes a message saying:

```
Forced FDDI shutdown when CMT rate exceeded 10358 events/sec
```

  A **show controller fddi** will report:

```
last non zero cmt rate 10358/sec, peak rate 23/sec
```

  This is a bug in how we determine the rate of CMT (connection management) events. In this example the actual rate never exceeded 23 per second. In early testing of the FDDI interface on the Cisco 4000, an excessive CMT rate could use up 100% of the processor and lock it up, so the router checked for excessive rates and if the rate exceeded 1000/second would shut down the interface to protect the rest of the router. This fix prevents an incorrect CMT rate from being reported and causing an interface to be administratively shut down. [CSCdi17010]
- Fast-switching cache values for all protocols are incremented when a serial interface cannot send a frame out a serial link. [CSCdi17332]
- When setting queue limits on any interface, the ciscoBus complex resets itself. This causes Token Rings to reinitialize. [CSCdi17646]

- The system software configuration parser incorrectly accepts the interface configuration of bridging over LAPB encapsulation. Interfaces cannot be configured to support both LAPB encapsulation and bridging at the same time. [CSCdi18420]
- The command **show interface** when issued on a system with 4T NIM configured for half-duplex operation may cause the system to restart. [CSCdi18752]

IP Routing Protocols

- Priority queuing does not classify IP fragments as expected. This is because some of the information required to classify the fragment is not in the packet. [CSCdi17905]
- The router continually reports "%SYS-2-NOBLOCK: event dismiss with blocking disabled" errors, preventing the router from processing other information. Reloading the router temporarily resolves the issue. [CSCdi18565]
- The **default-network** command does not work properly depending on subnet used. [CSCdi18743]

ISO CLNS

- When CLNS cluster aliasing was enabled on an interface and there were more than two members in the cluster, we would have a memory leak. [CSCdi18550]
- IS-IS stops sending IS-IS hellos after 49 days. This leads to loose adjacencies. [CSCdi18757]

Novell IPX, XNS, and Apollo Domain

- Novell updates could stop being issued out an interface after three weeks of uptime. [CSCdi18168]
- The destination MAC address is not being properly bit swapped for FDDI media. The result is an incorrect destination MAC address in show XNS cache and the outgoing packet. In the cache the destination MAC address should be bit swapped but is not, and the outgoing FDDI frame has a bit swapped destination MAC address. Turning off **xns route-cache** on the FDDI interface is a workaround. [CSCdi18273]
- Lotus Notes OS/2 servers appear to send Service Advertisement Protocol packets with a tc equal to one. Originating hosts are supposed to set the tc field to zero. Release 9.21 software was ignoring RIP and SAP Updates with tc field greater than zero. A workaround is to configure a static SAP entry on the router that is ignoring the Notes OS/2 Advertisement. [CSCdi18737]

VINES

- If there has been a very long interval (greater than one minute) between the time a router proxies a request from a server and the time that the server replies to that proxy, the router may reload. [CSCdi18285]
- When a redirect is received, it is entered into the routing table with a wrong metric value. This can cause circular routes in a network. [CSCdi18287]
- Sites with highly dynamic neighbors (that is neighbors going up and down a lot) could experience system crashes. [CSCdi18994]
- When running VINES, certain routing activity such as route deletion may cause the router to reload. [CSCdi19079]

Wide-Area Networking

- Configuring SMDS on serial lines that are shut down and subsequently reenabling them can in some circumstances cause a reload. A Token Ring interface appears to be required to trigger this problem. [CSCdi15880]
- Pings fail when using point-to-point subinterfaces. This is a symptom of the router using an incorrect map entry for a subinterface. [CSCdi17686]
- After ISDN DDR connection is already established, sometimes the line gets a DISCONNECT message from the remote end and the line drops. The only way to get the line back to where you can redial the distant end is to issue a **clear int bri 0** command. [CSCdi17908]
- A Cisco 2500 or Cisco 3000 series router with a BRI can now support the Australian switchtype. The basic-ts013 switchtype should be used in the configuration file. [CSCdi18128]
- A Cisco 2500 or Cisco 3000 series router with a BRI interface that is configured with a basic-net3 switchtype may encounter problems sending and receiving data on the B-channel. This may occur if a SETUP_ACK message, instead of a CALL_PROCEEDING message, is received in response to an outgoing SETUP message. It is also possible for buffers to be lost when running the basic-net3 switchtype. This can occur on the router requesting a disconnect from the network. Eventually the router will run out of available buffers and reload. [CSCdi18423]
- A router with an ISDN BRI interface configured for the basic-1tr6 switchtype may have problems connecting on Channel B2. An incoming SETUP message using Channel B2 can be incorrectly answered using Channel B1. This may cause the PPP protocol to keep the BRI channel interface in a Protocol-Up and Line-Down situation. It will also prevent the B2 channel from receiving any more calls. [CSCdi18562]
- The parser does not accept encapsulating PVC configuration commands. [CSCdi18671]
- IPX over PPP (IPXCP) now negotiates for the IPX network number. If the local router is requested, it can supply our network number. If the local network number is different than the remote network number, the local router asks the remote side to become our number if appropriate (their number smaller than ours), or the local router issues a warning message and negotiates with no network numbers. The warning is of the following format:

  `mismatched IPX network numbers. ours = %x, theirs = %x`

  ours and *theirs* display the IPX network numbers each side desires. [CSCdi18917]
- IPX over PPP now negotiates both network number and node number. The local node number is provided to the other side, which cannot change it, nor can the local node assign a node number. [CSCdi19077]

Release 9.21(1) Caveats/Release 9.21(2) Modifications

This section describes possibly unexpected behavior by Release 9.21(1). Unless otherwise noted, these caveats apply to all 9.21 releases up to and including 9.21(1). For additional caveats applicable to Release 9.21(1), see the caveats sections for newer 9.21 releases. The caveats for newer releases precede this section.

The caveats listed here describe only the serious problems. For a most current list of caveats against this release, access CIO as described in the section “Cisco Information Online” later in this document.

All the caveats listed in this section are resolved in Release 9.21(2).

Basic System Services

- After a system has been up for some time, the small buffer pool will start to record large number of misses (in the **show buffers** command), even though it claims that there are large numbers of buffers in the free list. The most visible effect is that all XRemote will slow down considerably, and the client XRemote statistics will show that nearly all packets are being transmitted twice. [CSCdi16843]

Interfaces and Bridging

- CTR cards hear their own DECnet hellos, resulting in a "%DNET-3-HEARSELF: Hello type 1 for my address." error message. This has no operational impact. [CSCdi07368]
- Certain combinations of system code and FDDI microcode may cause packet duplication on the FDDI ring. [CSCdi14083]
- The downstream neighbor in **show interface fddi** remains 0000.0000.0000. The issue is resolved in microcode and an additional workaround was created at system image level. [CSCdi15780]
- Corrupt and invalid Ethernet frames where incorrectly bridged to the FDDI interface resulting in FDDI transitions. The source of the corrupt frame was a Hirschmann hub sending diagnostic packages. [CSCdi15992]
- System issues link down traps from the FDDI interface when in fact the interface did not go down. The **debug fddi-cmt-events** command shows link down and link up trap without any corresponding CMT data. [CSCdi16506]
- FDDI trace counter can increment when there are no beacons on the ring. [CSCdi16744]
- VINES may not work properly on CTR interfaces that are also part of a transparent bridge group. [CSCdi16797]
- If a **no dialer** command of any type is issued and the interface is not configured as a dial on demand interface, the router may restart. [CSCdi16886]

IP Routing Protocols

- OSPF does not sufficiently validate received data, which in some cases can cause system failure. There is no workaround to this problem. [CSCdi16521]
- When an interface goes down, the system fails to poison the corresponding subnet route in RIP or HELLO routing advertisements sent out other interfaces that are part of the same major network number. The system also fails to poison a network summary route advertised by RIP or HELLO to other networks.The result is that adjacent routers must time out the corresponding route in their tables, instead of being notified of the routing change immediately. [CSCdi16698]
- Issuing the command **no router ospf** hangs the system. [CSCdi17080]

ISO CLNS

- The packet forwarding rate on a Cisco 4000 is lower than expected. [CSCdi16639]

Novell IPX, XNS, and Apollo Domain

- In 9.21(1.5), a problem was introduced in low-end (Cisco 2000s, Cisco 3000s, and Cisco 4000s) IPX fast-switching where the 802.3 MAC length field was being set incorrectly. Certain PC IPX drivers would count these packets as errors, while others would accept them. Novell IPX SAP, SNAP, and NOVELL-ETHER encapsulations are affected. This problem exists only in 9.21(1.5). [CSCdi17645]

VINES

- VINES may not work properly on CTR interfaces that are also part of a transparent bridge group. [CSCdi16797]
- Disabling **vines split-horizon** does not allow VINES StreetTalk broadcasts to be forwarded out an interface that they were received on. This will break "hub-and-spoke" Frame Relay networks because spoke StreetTalk broadcasts will not be forwarded from the hub router to other spoke sites. [CSCdi17488]

Wide-Area Networking

- There is a slight chance of the system crashing if a PVC is being used by one protocol and this one protocol is disabled at the same time the system is checking to see if an Inverse ARP request should be sent. [CSCdi16672]
- X.25 calls received on a serial interface cannot be routed to a CMNS host. [CSCdi17212]
- The **no atm-dxi map** *protocol protocol-addr* command does not require VPI and VCI as arguments. By default, they are set to zero. This means the command must bypass the check for nonzero values which is applicable only when maps are configured, not when they are removed. [CSCdi17375]
- When an asynchronous interface is configured for both SLIP and demand dialing (with the **dialer in-band** command), the link will dial correctly but packets will never be transmitted across the link. The **debug ip packet** command will show each packet failing encapsulation. [CSCdi17609]

Microcode Revision History

The following sections describe the revisions of microcode that have changed since the initial release of Release 9.21 on January 17, 1994.

Switch Processor (SP) Microcode Revision Summary

SP Microcode Version 2.3

Version 2.3 of the SP microcode was released on March 14, 1994.

Modifications

This release fixes the caveat that autonomous FDDI-to-FDDI source-route bridging exhibited poor packet processing performance.

SP Microcode Version 2.4

Version 2.4 of the SP microcode was released on June 27, 1994.

Modifications

This release fixes two problems:

- The HIP shuts down when forwarding IPX packets larger than 2048 bytes. [CSCdi19399]
- With source-route bridging, IP access lists do not work on the Cisco 7000 series. [CSCdi19911]

Ethernet Interface Processor (EIP) Microcode Revision Summary

EIP Microcode Version 1.1

Version 1.1 of the EIP microcode was released on March 14, 1994.

Modifications

This release fixes two problems:

- A DEC system on an Ethernet link might have experienced DECnet DAP CRC errors.
- At a load greater than 30%, performance might have dropped due to retransmission.

EIP Microcode Version 1.2

Version 1.2 of the EIP microcode was released on June 27, 1994.

Modifications

This release fixes two problems:

- Occasionally, the EIP would hang with the error 800E.
- If the Cisco 7000 series router also contained FSIP and FIP cards and the router was heavily loaded, a ciscoBus access error could occur.

FDDI Interface Processor (FIP) Microcode Revision Summary

FIP Microcode Version 1.4

Version 1.4 of the FIP microcode was released on April 18, 1994.

Modifications

This release fixes an AMD ENDEC chip problem.

FIP Microcode Version 1.5

Version 1.5 of the FIP microcode was released on August 15, 1994.

Modifications

This release fixes the following problems:

- Under heavy load, FIP microcode Version 1.4 could experience a transmitter hang.
- If another station on the FDDI ring causes the FIP to beacon and then goes to QLS (Quiet Line State) within a very short interval, the FIP may trace.

Fast Serial Interface Processor (FSIP) Microcode Revision Summary

FSIP Microcode Version 1.2

Version 1.2 of the FSIP microcode was released on August 15, 1994.

Modifications

This release fixes the problem that with microcode prior to Version 1.2, fast switching SAP encapsulated packets to Frame Relay-encapsulated serial lines sometimes failed.

HSSI Interface Processor (HIP) Microcode Revision Summary

HIP Microcode Version 1.2

Version 1.2 of the HIP microcode was released on April 18, 1994.

Modifications

This release fixes transmitter delay, which did not work properly in previous versions. It also adds support for CSC32. HIP CRC32 also requires hardware version 1.1.

HIP Microcode Version 1.3

Version 1.3 of the HIP microcode was released on November 7, 1994.

Modifications

CRC16 is now default. Previously CRC32 had been the default.

HIP Microcode Version 1.4

Version 1.4 of the HIP microcode was released on January 23, 1995.

Modifications

When in CRC-32 mode, previous versions of the HIP microcode treated frames that were of size MTU or MTU – 1 as giants.

Token Ring Interface Processor (TRIP) Microcode Revision Summary

TRIP Microcode Version 1.2

Version 1.2 of the TRIP microcode was released on May 10, 1994.

Modifications

This release fixes the following caveats:

- AppleTalk multiring causes RTMP problems [CSCdi10878]
- Under high data rates and with a frame size greater than 120 bytes, the transmitter may hang, and the following error message is displayed: `tx0 output hung (800E - tx queue full), resetting interface`. [CSCdi18682]

Cisco Information Online

Cisco Information Online (CIO) is Cisco Systems' primary, real-time support channel. You can use your product serial number to activate CIO for a single user during your warranty period. Maintenance customers and partners can self-register on CIO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CIO provides a wealth of standard and value-added services to Cisco's customers and business partners. CIO 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.

CIO 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 CIO (called "CIO Classic") supports Zmodem, Kermit, Xmodem, FTP, Internet e-mail, and fax download options, and is excellent for quick access to information over lower bandwidths. The WWW version of CIO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CIO in the following ways:

- WWW: `http://www.cisco.com`.
- Telnet: `cio.cisco.com` (198.92.32.130).
- 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 CIO's Frequently Asked Questions (FAQ), contact `cio-help@cisco.com`. For additional information, contact `cio-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`.

UniverCD

The complete caveats against this release are available on UniverCD, which is the Cisco Systems library of product information on CD-ROM. On UniverCD, access the Software Release 9.21 Caveats in the "System Software Release 9.21" database.

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