Doc. No. 78-1281-06

Communication Server 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 *Communication Server Configuration Guide* and *Communication Server Command Reference* publications for complete communication server 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, page 2
  If you are booting an ASM/3-CS over the network, read this section for booting restrictions.
- Memory Requirements, page 2
- New Features in Release 9.21(3), page 2
- Software Features in Release 9.21(1), page 2
- Important Notes, page 7
  This section describes warnings and cautions about using the Release 9.21 software. One note of general interest discusses how to boot ASM/3-CS systems.
- Release 9.21(7) Caveats, page 9
- Release 9.21(6) Caveats/9.21(7) Modifications, page 9
- Release 9.21(5) Caveats/9.21(6) Modifications, page 9
- Release 9.21(4) Caveats/9.21(5) Modifications, page 11

Platform Support

Software Release 9.21 is supported on the following communication server platforms:

- ASM-CS platforms—ASM/3-CS and ASM/4-CS
- 500-CS platforms—508-CS and 516-CS
- CPT

Memory Requirements

In order for Cisco 500-CS communication servers to take advantage of the Release 9.21 features, you must upgrade the code or main system memory as outlined in Table 1. There are no special memory requirements for ASM-CS platforms.

Table 1 Release 9.21 Memory Requirements

Communication Server	Required Code Memory	Required Main Memory	Release 9.21 Runs from ...
500-CS	4 MB ROM	4 MB RAM (10 MB if netbooting)	ROM

New Features in Release 9.21(3)

The following new feature has been added in Software Release 9.21(3):

- The software now supports AppleTalk Remote Access (ARA), which gives Macintosh users direct access to information and resources at a remote location. ARA is described in the *Communication Server Addendum for AppleTalk Remote Access* publication.

Software Features in Release 9.21(1)

This section describes features and enhancements in the initial Release 9.21 of the communication server 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 communication server automatically and dynamically. A new communication server connected to a network on which there exists a preconfigured communication server can be enabled immediately with a configuration file that is automatically downloaded from a TFTP server.

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 Novell IPX. 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.
- PAP. The communication server 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:

- Subinterfaces. The communication server supports subinterfaces on Frame Relay, which are multiple virtual interfaces on a single physical interface. Subinterfaces can provide full connectivity on partially meshed Frame Relay networks.
- 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.
- 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.

X.25 and LAPB

This 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).
- User identification. You can set a user-defined network user identification in a format defined by the network administrator.

Dial-on-Demand Routing (DDR)

This following features have been added to Cisco’s dial-on-demand (DDR) software:

- Full dial-on-demand routing (DDR) for IP and IPX. This implementation supports the use of chat scripts for placing and receiving calls on asynchronous lines.
- Dial backup.This provides protection against WAN downtime by allowing you to configure a backup serial line circuit-switched connection.

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.

Frame Relay

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

- Support for the Inverse Address Resolution Protocol (InvARP). The Frame Relay software supports InvARP, as described in RFC 1293, for the IPX protocol. InvARP 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.

LAT

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

- Sending of periodic broadcast service announcements.
- Controlling the maximum number of sessions multiplexed onto a single LAT virtual circuit.
- Controlling the number of receive buffers negotiated by a LAT host.
- Controlling the number of receive buffers negotiated by a LAT server.

TN3270

The following feature has been added to Cisco’s TN3270 software:

- Two-way binding, or character mapping, between EBCDIC and ASCII characters.

SLIP and PPP

The following features have been added to Cisco's SLIP and PPP software:

- When using **login** and **slip** EXEC commands to access a system with TACACS security, you can specify a TACACS server. If the user specified a TACACS server host with the *user@host* argument, the specified TACACS server will be used for all subsequent authentication or notification queries, with the possible exception of SLIP address queries.
- The SLIP EXEC command now supports the **/routing** option, which allows the user to implement routing.
- To make it easier to debug PPP links, PPP now uses its own set of debugging commands, and no longer uses any other non-PPP debugging commands.
- Debugging for asynchronous interfaces has been improved and made consistent across protocols. The old SLIP debugging commands have been removed. The new commands apply across all asynchronous packet protocols, including SLIP, PPP, and XRemote.
- Dialup support (SLIP and PPP) has been rewritten for Release 9.21. Many old **slip** line configuration commands have been replaced with **async** interface configuration commands. The old commands are translated into the new command syntax automatically.

  The syntax of the SLIP configuration commands has been changed to reflect the fact that they apply to both SLIP and PPP encapsulation on asynchronous interfaces, as listed in Table 2.

Table 2 SLIP Configuration Commands with New Syntax

Old Command	New Command
show slip	**show async status**
show async-bootp	**show async bootp**
show interactive	**async mode interactive**
slip dedicated	**async mode dedicated**
slip address dynamic	**async dynamic address**
slip routing	**async dynamic routing**
slip address ip-address	**async default ip address**

  The preferred way to configure SLIP and PPP is to use the new **async** interface configuration commands rather than the old **slip** line configuration commands.

- Other **slip** commands have been replaced by **ip** commands. Table 3 shows the relationship between the old and new commands.

Table 3 SLIP Configuration Command Replacements

Old Command	New Command
slip access-class	**ip access-group**
slip hold-queue	**hold-queue**
slip mtu	**ip mtu**
slip header-compression	**ip tcp header-compression**

IP

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

- The old commands listed in Table 4 were converted to new commands in Software Release 8.3. In Release 9.21, the old commands are no longer supported.

Table 4 IP Command Changes

Old Command	New Command
domain-list name	**ip domain-list**
service-ipname	**ip ipname-lookup**
service-domain	**ip domain-lookup**
name-server server-address1	**ip name-server**

- You can configure the communication server to act as a terminal using the new **ip host-routing** global command.
- Route maps. This new feature creates tags for each route. These tags are then used to influence route redistribution. Route maps apply to OSPF and IS-IS.
- 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.
- 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 communication server 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.

- Multicast groups. Multicast groups are now supported and information about them is shown in the output of the **show ip interface** EXEC command.
- 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).
- Command syntax changes:
    - The syntax of the OSPF **neighbor** router configuration command has changed. The *interface* parameter 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.

Novell IPX

Communication servers now support full Novell IPX routing.

Protocol Translation

Two new options have been added to the **translate** command: **stream** and **printer**. The **stream** option performs stream processing, which enables a raw TCP stream with no Telnet control sequences. The **printer** option supports LAT and X.25 printing over a TCP network among multiple sites.

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.”

Cisco 500-CS Jumpers

When you upgrade your EEPROMs to the Software Release 9.21(1) or later cs500-kr image, you need to install or move jumpers on the Cisco 500-CS system card. Table 5 indicates the locations of the pins on jumper J4 that must be installed. For more information, refer to the *Cisco 500-CS Memory and Software Upgrade Instructions* document.

Table 5 J4 Jumper Settings

Pins	Description
5-6	Temperature control
7-8	256 KB EPROM
9-10	512 KB EPROM
13-14	EPROM speed: 3 wait states

Booting an ASM/3-CS

If you have an ASM/3-CS, which has a CSC/3 processor, and you cannot netboot due to a “buffer overflow” error, you must load the bootstrap program gs3-boot. This program is available either on floppy disk or from Cisco CIO by way of File Transfer Protocol (FTP). Once you have the program, transfer it to your system using Trivial File Transfer Protocol (TFTP). In addition, you must access the front edge of the CSC/3 processor card and verify the positions of three jumpers in the configuration register. You also must enter a combination of software commands in your configuration file.

To load the bootstrap program and enable the system to first boot the bootstrap program and then boot the system image, follow this procedure:

Step 1 Use appropriate procedures to make the gs3-boot file available:

- Floppy disk version—Establish network access to a PC (with an appropriate 3.5-inch floppy disk drive) that is configured as a TFTP server
- Electronic version—Establish network access to a TFTP server that holds the file

Step 2 Access the configuration register on the front edge of your CSC/3 processor card by following the procedure in your hardware installation and maintenance publication.

Step 3 Reset bit 0 on the configuration register to 0 (remove the jumper). This disables booting from system read-only memory (ROM). Refer to your hardware installation and maintenance publication for details.

Step 4 Using the jumper removed from bit 0, set bit 1 of the configuration register to 1 (insert the jumper). This enables netbooting.

Step 5 Using the extra jumper provided with the gs3-boot software, set bit 9 of the configuration register to 1. This causes the system to look for and load the secondary bootstrap procedure (bootstrap program).

Step 6 Rename the gs3-boot file to boot-csc3, or create a logical link from the file gs3-boot to boot-csc3. When the communication server reboots, it expects to boot a file named boot-csc3.

Step 7 If your communication server has Flash capability, enter the following commands in the configuration memory (otherwise proceed to Step 8):

```
boot bootstrap flash gs3-boot.91-9
boot system flash filename
^z
cs# write memory
```

filename is the name of your 9.1(9) or later image.

The system then looks for and loads the bootstrap program, and then looks for and loads the 9.1(9) system image as defined by *filename*.

Step 8 If your communication server does not have Flash capability, enter the following commands in the configuration memory:

```
boot bootstrap gs3-boot.91-9
boot system filename
^z
cs# write memory
```

filename is the name of your 9.21(4) or later image.

The system then looks for and loads the bootstrap program, and then looks for and loads the 9.21(4) or later system image as defined by *filename*.

Release 9.21(7) Caveats

There are no serious caveats reported against Release 9.21(7). For a most current list of caveats against this release, access CIO as described in the section “Cisco Information Online” later in this document.

Release 9.21(6) Caveats/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).

Communication Server

- The communication server leaks memory if the **nohangup** keyword of the **username** global configuration command is used to define special username entries. [CSCdi25520]

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]
- Hitachi-based serial ports might not transmit under a severe load because the underrun interrupt is not properly enabled. [CSCdi26209]

TCP/IP Host-Mode Services

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

Wide-Area Networking

- 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/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).

Communication Server

- The changes in Release 9.21 to the “host” IP module apparently cause the software to try proxy ARP for a destination befor etrying to use the default gateway. This worked correctly in Release 9.1 (used the default -gateway first). [CSCdi14799]
- The use of extended TACACS in conjuction with the **tacacs-server last-resort password** command can cause the Ethernet input queue to fill up and the box to pause indefinately if repsonses to the TACACS queries are received while the last-resort password is being entered. [CSCdi18919]
- Certain types of “poison packets” cause communication servers to reload as an attempt is made to forward the packets. [CSCdi23494]
- A communication server can spontaneously reload while attempting to hangup a line configured with the **autohangup** command once the last network connection on the line is closed. This happens only if the last connection was resumed using the **resume** EXEC command. [CSCdi24025]

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]

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]

Novell IPX

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

Protocol Translation

- Removing a **translate** command from the configuration can cause other translations using the same inbound IP address to stop working. A workaround is to configure the remaining translations again, for example, by issuing the **write memory** and **config memory** commands. [CSCdi23621]
- In LAT-to-PAD (X25) translated sessions, a Ctrl-S followed by the entry of any character can sometimes cause a continuous stream of empty LAT messages, causing a session disconnect. [CSCdi24491]

TCP/IP Host-Mode Services

- Under rare circumstances, an opening TCP connection can get stuck in CLOSEWAIT state. This can also result in a STUN peer session getting stuck in an OPENING state at the same time. [CSCdi23455]

Release 9.21(4) Caveats/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).

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 the OSPF router link state advertisement by changing the interface metric or by rebooting. [CSCdi21103]

Novell IPX

- 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 aGNS response delay may cause problems in certain situations. The new GNS response delay default is 0. [CSCdi22285]

Wide-Area Networking

- If you use the **local** *global-option* keyword on incoming X.25-to-TCP **translate** commands in conjunction with the **profile** keyword, ECHO Telnet protocol negotiation cannot be translated. Echoing of character is perforemed by the remote PAD. [CSCdi21087]
- 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/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).

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]

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 overrided by the default value of the encapsulation in used. [CSCdi19006]

Interfaces and Bridging

- 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]

IP Routing Protocols

- The router and communication servers allow remote users to Telnet into VTY ports by connecting to ports 20xx/40xx/60xx/80xx. All of 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 unoptimal inter-area 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 only happen after the system has been up for a period of time. The length of this period depends on how much connectivity changes have occured. In a fairly busy network, the estimate 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). There is no workaround for this problem. [CSCdi20401]

Novell IPX

- 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 an error message is displaying saying there is a path mismatch for these routes. The **show ipx route** 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]

TCP/IP Host-Mode Services

- The system implements diagnostic TCP servers on ports 7 (ECHO) and 9 (DISCARD). Release 10.0 adds a server on port 19 (CHARGEN). These services cannot be disabled, which is worrisome to users implementing firewalls. Also, the system mistakenly listens for XRemote connections on port 10000, corresponding to the non-existent rotary group 0. [CSCdi20077]

TN3270

- In come cases, TN3270 fails to display highlighted characters properly. [CSCdi19420]

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/ciscoBus 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]
- 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(1) Caveats/Release 9.21(3) 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(3).

Note that Release 9.21(2) of the communication server software was never released.

Basic System Services

- Under rare circumstances, the **clear line** command will fail to clear the process running on that line. A **show process** command will show that the process on that line has an inappropriate and rapidly increasing number in the “invoked” column. [CSCdi16063]
- 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]
- Attempts to establish host-initiated connections to remote destinations get placed in the terminal port queue if the remote destination is busy. By default, the terminal queue is scanned every 60 seconds. The remote destination for each entry is polled. If the destination has become idle, the connection is established and the entry is removed from the queue. The terminal queue

commands, which always follow a **terminal-queue** command, modify the operation of the terminal queuing system. The **entry-retry-interval** command changes the default polling interval to the number of seconds specified on the command line. The maximum interval is 255seconds. The **no terminal-queue entry-retry-interval** command restores the default value. [CSCdi17780]

IP Routing Protocols

- 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]
- 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 system from processing other information. Reloading the system temporarily resolves the issue. [CSCdi18565]
- The **default-network** command does not work properly depending on subnet used. [CSCdi18743]

Wide-Area Networking

- Configuring SMDS on serial lines that are shutdown, and subsequently reenabling them can in some circumstances cause a reload. A Token Ring interface appears to be required to trigger this problem. [CSCdi15880]
- 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]
- 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]
- X.25 calls received on a serial interface cannot be routed to a CMNS host. [CSCdi17212]
- 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 shows each packet failing encapsulation. [CSCdi17609]
- Pings fail when using point-to-point subinterfaces. This is a symptom of the router using an incorrect map entry for a subinterface. [CSCdi17686]
- The parser does not accept encapsulating PVC configuration commands. [CSCdi18671]
- IPX over PPP (IPXCP) now negotiates for the IPX network number. If the local system is requested, it can supply our network number. If the local network number is different than the remote network number, the local system asks the remote side to become our number if appropriate (their number smaller than ours), or the local system 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]

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 *Communication Server Configuration Guide* and *Communication Server Command Reference* publications.