CISCO SYSTEMS

Terminal Server Release Notes for Software Release 8.3

This release note describes the features, modifications, and caveats for Software Release 8.3, including 8.3(1) through 8.3(9).

Complete documentation for Release 8.3 is contained in the Cisco Systems publication *Terminal Server Configuration and Reference* dated October 1991. A list and description of the current software versions available from Cisco Systems is included in the "Software Version Levels" section in this document.

Note: Release 8.3(9) is the last maintenance Release for 8.3. Maintenance customers will continue to receive phone support from CE, but fixes will be made only to Release 9.0 and higher releases. As of August 2, 1993, Release 9.1(5) is the preferred upgrade path for a Release 8.3 user.

Introduction

This release note covers the following topics:

Software Version Levels

The table that follows describes the current software versions for Cisco terminal server software. Refer to these descriptions when ordering software updates for Software Release 8.3.

Versions	System	Description	ROMs
8.3(1-9)	TS3	CSC/3 Terminal Server Sets	
	TS3-S		4
	TS3-L		4
	TS3-X		4
8.3(1-9)	TS2	CSC/2 Terminal Server Sets	
	TS2-R		8
	TS2-LR		8
8.3(1-9)	TR3	CSC/3 TRouter Sets	
	TR3-X		4
8.3(1-9)	TR2	CSC/2 TRouter Sets	
	TR2-RX		8
	TR2-X		8
8.3(1-9)	STS-10x	Extended Small Terminal Server Sets	
	STSX-R		2
	STSX-LP		2

Letter Key:
S—Standard system software
R—Standard system software that executes directly from ROM
X—Standard and Commercial/DDN X.25 software
L—LAT software

The procedures for updating your system with the latest software version, including procedures for EPROM replacement, are contained in the Cisco Systems publication *Modular Products Hardware Installation and Reference*, October 1991.

New Software Features for Software Release 8.3(1)

This section describes the major functions introduced in Release 8.3(1) of the router software.

New Functionality

New functionality in Release 8.3(1) of the terminal server software includes the following features:

- Support for TN3270 terminal emulation on all Cisco terminal servers except the STS-10X. TN3270 support includes extensive custom termcap and keymap support.
- Support for XRemote.
- ROM-based software for the STS-10X.
- Support for a new router discovery mechanism.
- Support for SLIP access lists.

Software Release 8.3(1) Enhancements

Release 8.3(1) includes these enhancements to the terminal server software.

System Configuration

- The **setup** command facility has been modified to include configuration of the DEC Maintenance Operation Protocol (MOP) and LAT protocols in the initial configuration query sequence.
- Unusual terminal baud rates are now supported on the terminal server. The line configuration subcommands **speed**, **txspeed**, and **rxspeed** allow for the specification of any baud rate from 75 to 57,600 baud. The global configuration command **extra baud-rate** has been added to allow the replacement of a specific baud rate for 38,400.
- Username authentication has been extended to networks that cannot support TACACS services. A new global configuration command, **username**, includes several optional arguments.
- The **session-timeout** command has been modified. The *seconds* argument has been removed and replaced with the **output** optional keyword to allow specification of timeout interval for outbound data (from the terminal server to the asynchronous device). The new command syntax follows:

    session-timeout *minutes* [**output**]

- A new line configuration command, **session-limit**, has been added. This command defines the maximum number of remote sessions that can be established per line.

- Support has been added for TCP state machine-based packet dispatch capability. Two new commands control this feature: **state-machine**, a global configuration command, and **dispatch-machine**, a line configuration subcommand.

- The TCP keepalive protocol is now supported as a **service** command option.

- MOP sysid messages now include the system's burned-in MAC address.

- Netbooting capabilities have been added for DEC MOP. Two new system management commands control this feature: **mop enabled** and **mop sysid**.

- When a system image has been netbooted, the **show hardware** command shows the boot host and the name of the boot file.

- SNMP support has been extended to include SNMP MIB II (RFC 1157).

- A new global configuration command, **snmp-server system-shutdown**, has been added. This command is equal in results to Cisco's **send** and **reload** commands issued in tandem.

- The following **service** commands have changed format for Release 8.3(1):

Old Format	New Format
service domain	**ip domain-lookup**
service ipname	**ip ipname-lookup**

Note: The old formats for the service commands are accepted in configuration input, but the output of the **write terminal** or **show config** commands will display the new forms.

- Extensions have been added to the **banner** command to display a message-of-the-day banner and to display a banner upon opening an EXEC process or an incoming message.

- Addition of the [**no**] **exec-banner** line command allows users to enable or disable banner commands.

- Support for configurable buffer sizes has been added through the new **buffers** global command.

- The **error-threshold** command now provides a means to configure the frequency at which the error recount will be set.

- A new **clear counters** EXEC command has been added to clear interface counters.

LAT

Several changes have been made to Cisco's software implementation for the DEC LAT protocol.

- A new line subcommand, **insecure**, has been added. Execution of this command results in the terminal server reporting the line as a dialup-type to remote systems.

- A new interface subcommand, **lat enabled**, has been added to control the use of LAT on an interface.

- Group code processing for LAT has been improved to be more flexible. The previously supported **lat hic-group** line configuration subcommand has been eliminated and replaced with the new global configuration command, **lat service-group**.

- The **lat server-group** global configuration command is no longer supported. The group list that has previously been provided through execution of that command is now calculated dynamically from the logical-OR of the line-specific **lat out-group** lists on all the lines.

- Users can now reduce group code lists using the **terminal lat out-group** command. A group can be set so long as it is set in the permanent mask for the given terminal.

- Software support for LAT is now more responsive to abort requests from remote hosts.

Internet Protocol (IP)

- With Release 8.3(1), a router discovery mechanism has been added to the IP implementation for the terminal server software. A new command, **ip gdp**, has been added to enable this capability.

- Support has been added for SLIP access lists. The following command has been added to support this feature:

  slip access-class number [**in** | **out**]

Documentation Enhancements

As of Software Release 8.3(1), Cisco's documentation set has a new format and includes the following changes:

- A comprehensive error message appendix that includes error messages for all Cisco products has been added.

- Manuals have been reorganized to support specific tasks. Each new software manual provides sections on using the **setup** command facility, using the system, configuring the system, managing the system, and performing protocol-specific configuration. The new manuals also provide summaries of relevant commands with each chapter.

System Requirements

In order to netboot Release 8.3(1) software, modular systems (that is, the ASM, MSM, and TRouter) must include a CSC/3 processor. The STS-10x terminal server cannot netboot an 8.3(1) image.

New Software Features for Software Release 8.3(2)

This section describes new software features and enhancements that were added to the software with Release 8.3(2).

Enable and Console Passwords and the SNMP Community String

With Software Release 8.3(2), the software no longer allows the enable password or the console password to be used as the community string for SNMP.

Additional User Notes

This section provides technical notes that supplement information found in the software and hardware manuals.

Token Ring Restarts

If the system receives an indication of a cabling problem from a CSC-R16 Token Ring interface, that interface is placed in a reset state. The system does not attempt to restart the interface. To restart the interface, correct the cabling problem and use the **clear interface** command to reset it.

The system functions in this manner because periodic attempts to restart the Token Ring interface have drastic effects on the stability of routing tables and sometimes on the stability of Token Ring networks themselves.

Netboot Restrictions

Netbooting over X.25 or Frame Relay is not allowed to a broadcast address. You must specify the address of a server host to successfully netboot the system files. Use an off-net map entry of the destination. This means that you cannot simply have an X.25 or Frame Relay map entry for the next hop router. You need a map entry (use **x25 map** or **frame-relay map** command) for the host from which you will boot, even if that host is not on a directly connected network.

X.25 Example

The **x25 map** command is used to map an IP address into an X.121 address. There *must* be an **x25 map** command that matches the IP address given on the **boot system** command line. In order to netboot over X.25, the address of the system from which to netboot *must* be given explicitly, and an **x25 map** entry must exist for that site, as the following example illustrates.

```
boot system ts3-bfx.83-2.0 131.108.13.111
!
interface Serial 1
ip address 131.108.126.200 255.255.255.0
encapsulation X25-DCE
x25 address 10004
x25 map IP 131.108.13.111 10002 BROADCAST
lapb n1 12040
clockrate 56000
```

Frame Relay Example

If file *ts3-bfx* is to be booted from a host with IP address *131.108.126.2*, the following would need to be in the configuration:

```
boot system ts3-bfx 131.108.126.2
!
interface Serial 0
encapsulation frame-relay
frame-relay map IP 131.108.126.2 100 broadcast
```

8.3(9) Caveats

This section describes possibly unexpected behavior by release 8.3(9). Unless otherwise noted, these caveats apply to all 8.3 releases up to and including 8.3(9).

Basic System Services

- It is possible for system reloads to occur when the nonvolatile configuration memory is manipulated from more than one terminal session. Only one terminal at a time should do commands from the set {**show config**, **write memory** (or **write** with no argument), **write erase**, **config** from memory}. [CSCdi03856]

EXEC and Configuration Parser

- In certain cases, the terminal server buffers are not cleared during a modem hangup. This can result in lines stuck in XOFF mode, or echoing of garbage to the next user to seize that line. [CSCdi11792]

Interfaces

- The **mac-address** *address* command does not work on serial interfaces, even though a serial interface may want to use this, for example when a communications server is originating LAT packets on the serial link. [CSCdi09015]

LAT

- A LAT protocol translation session can fail to be destroyed properly under some circumstance when output is still in progress as the connection is closed by the remote LAT host. [CSCdi07506]

TN3270

- TN3270 sessions may pause indefinately when attempting to connect to Unisys mainframes. [CSCdi09547]

- The Cisco TN3270 implementation partially implements transparent mode. It will pass data in the Yale transparent mode (also known as Series 1 mode), but it does not respond to the "Are you a series1?" query. Because of this, customers wishing to use KERMIT or other programs that use Yale transparent mode must explicitly tell the program that the controller is a series 1 type controller. For KERMIT, the command **set controller series1** is given to the IBM mainframe KERMIT program. [CSCdi07845]

Wide-Area Networking

- The **x25 pvc bridge number** interface command is not properly stored in the system's configuration memory. [CSCdi06683]

- Under unusual circumstances, a RESET of a virtual circuit may not properly discard all in-transit data. This may cause an additional RESET of the VC to occur. [CSCdi07811]

- The Cisco X.25 implementation allows both modulo 8 and modulo 128 virtual circuits to co-exist on the same interface; this is non-standard. [CSCdi07812]

- Regarding the **x25 map ip ipaddr broadcast** command, all x25 map commands must accept an X.121 address for association with each protocol address mapped to. Rather than having the **broadcast** taken as an X.121 address incorrectly, the configuration will now contain an X.121 address before the **broadcast** keyword is specified. [CSCdi08630]

- The X.25 idle timer previously applied to SVCs that were switched (via the **x25 route** command) or nonswitched on an interface. Now only nonswitched SVCs are subject to the X.25 idle timer. [CSCdi09927]

8.3(8) Caveats/8.3(9) Modifications

This section describes possibly unexpected behavior by Release 8.3(8). Unless otherwise noted, these caveats apply to all 8.3 releases up to and including 8.3(8). For additional caveats applicable to Release 8.3(9), see the caveats sections for newer 8.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 8.3(9).

EXEC and Configuration Parser

- The parser sometimes claims that incomplete command names are not unique. [CSCdi10554]

TN3270

- TN3270 may return modified data fields to the host in the incorrect order. This is primarily manifested in applications complaining of invalid data in fields that do indeed have the correct data. [CSCdi10344]

8.3(7) Caveats/8.3(8) Modifications

This section describes possibly unexpected behavior by Release 8.3(7). Unless otherwise noted, these caveats apply to all 8.3 releases up to and including 8.3(7). For additional caveats applicable to Release 8.3(7), see the caveats sections for newer 8.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 8.3(8).

Basic System Services

- A terminal line configured for flowcontrol will not successfully time out (due to a session-timeout configuration) if the line is xoffed at the time of the timeout. [CSCdi09310]
- The parser sometimes claims that incomplete command names are not unique. [CSCdi10554]

IP

- When initiating a TFTP read request, the system can generate TFTP packets with invalid UDP checksums. This only happens when the request is transmitted out an unnumbered interface. If the TFTP server has UDP checksumming enabled, TFTP read requests via the unnumbered interface will fail. Turning off UDP checksumming at the TFTP server, or restricting TFTP reads to numbered interfaces avoids this problem. [CSCdi09577]

Local Services

- If an attempt is made to either write a read-only object or read a write-only object, the wrong error code is returned. [CSCdi09714]

TCP/IP Host-Mode Services

- When a TCP connection has a closed window, packets containing valid ACKs are discarded if they also contain any data (since the data is outside of the window). The correct behavior is to continue to process the ACKs for segments with reasonable ACK values. This is especially a problem in the initial stages of a connection, when we send the SYN-ACK with a 0 window. If the ACK to our SYN contains data also, we will not process that ACK, and the connection never gets to ESTABLISHED state. [CSCdi05962]

8.3(6) Caveats/8.3(7) Modifications

This section describes possibly unexpected behavior by Release 8.3(6). Unless otherwise noted, these caveats apply to all 8.3 releases up to and including 8.3(6). For additional caveats applicable to Release 8.3(8), see the caveats sections for newer 8.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 8.3(7).

Basic System Services

- The **stopbits 1.5** command is never written to nonvolatile RAM or to remote network configuration files, even for lines that have been configured using it. [CSCdi05124]

- Entering multiple **logging buffered** commands without an intervening **no logging buffered** command can cause meaningless output to be included in the output of the **show logging** command. [CSCdi08459]

- System images from the 8.3, 9.0, 9.1, and 9.14 releases could not be successfully netbooted on IGS boxes with 8.2 EPROMs. The ROM monitor in the 8.2 EPROMs did not support some functions that the newer releases use. The system image should protect itself by error checking the return code from all ROM monitor calls. [CSCdi08521]

Interfaces

- When a communication server line is configured for modem control and with a session timeout, the session timeout will not be honored if the line is running in SLIP mode. [CSCdi08562]

- The **clear counter** [*type unit*] command always clears the counters regardless of the user's response to confirmation. [CSCdi08774]

- When using a protocol translator or communication server without IP routing enabled, ARPs for IP aliases or addresses associated with translate commands may not be answered correctly. As a workaround, turn on IP routing to restore the expected behavior. [CSCdi08981]

- The system does not properly process RARP response packets received where these packets are responses for requests not initiated by the system. The system allows such packets to remain in the input queue, resulting in two user visible problems. First, the network interface input queue can fill up with RARP response packets, causing all subsequent packets destined for the system to be dropped. Second, the system fails to bridge these RARP response packets. The correct behavior is to bridge such packets in the case where the system is configured to bridge RARP packets; otherwise, ignore these packets. [CSCdi08651]

Local Services

- Any attempt to query an unimplemented SNMP MIB variable will cause the system to return the snmpEnableAuthenTraps variable. The correct behavior is to indicate that the variable requested is not available. This will be corrected in a future release. [CSCdi04806]

- If **enable use-tacacs** is configured without defining a **tacacs-server host**, then ANY username/password combination will allow any user to enable. [CSCdi08070]

- On systems without NVRAM, part of the sequence used to determine IP addresses is to send a BOOTP request. The replies to these requests are being ignored. [CSCdi08893]

TCP/IP Host-Mode Services

- TCP connections can exhibit long pauses in data delivery if the Cisco system is attempting to send data faster than the foreign host can use that data. This happens most often in cases of protocol translation, SDLC tunneling, remote source route bridging, and X.25 switching. [CSCdi07964]

Terminal Service

- When TN3270 has a buffer of data to send which is exactly the same size as the packet that it is sending it in, the packet is sent without the TCP PUSH flag set. Some host implementations will not act on the data unless the TCP PUSH is set. Connections to these hosts can pause for the session timeout period. This will be fixed by having all TN3270 packets sent with the push flag set. [CSCdi08034]

- If a line is configured withthe **session-timeout** *n* **output** command, the **output** part of the command will remain in effect even if a new **session-timeout** *n* command is given (without "output" specified). A workaround is to turn off the "output" part explicitly with a **no session-timeout 0 output** command. [CSCdi08625]

TN3270

- Keymaps are not currently parsed correctly. Each keymap consists of the name of the keymap, the terminal types to which it applies, and the various mappings. When parsing the terminal types, only the first one is read correctly. The result is that the keymap will only be selected when the user's terminal type matches either the name of the keymap or the first terminal type in the keymap. This will be fixed by changing the software to correctly parse the terminal types in the keymap. [CSCdi05677]

- The login-string configuration command is not correctly implemented for TN3270 connections. As currently implemented, it merely sends the ASCII text of the login-string to the host at the other end of the connection. This is fine for Telnet and rlogin connections, but for TN3270 connections, the login-string must be passed through the TN3270 input path. The problem will be fixed by passing the login-string through the TN3270 input path on TN3270 connections. Additionally, two special escape characters have been added, %t for tab, and %m for carriage return. In order to place a tab in a login-string, one will enter %t. Likewise, one will use %m at the end of the login-string to achieve a carriage return, as normal telnet processesing would send an undesirable line feed after the carriage return. [CSCdi08252]

- Clear to end of line is currently done by writing spaces. This is very slow and can be painful on low-speed dialup lines. It will be fixed by using two attributes in the ttycap, ms:, and cx:. If both attributes are in the terminal's ttycap, the TN3270 implementation will use the clear to end of line command rather than sending spaces to the terminal. This will be the default behavior. Note that this may not be appropriate when a terminal is in underline mode. Removing the cx: attribute from the termcap will cause the TN3270 to clear to the end of line by sending spaces. [CSCdi08441]

8.3(5) Caveats/8.3(6) Modifications

This section describes possibly unexpected behavior by Release 8.3(5). Unless otherwise noted, these caveats apply to all 8.3 releases up to and including 8.3(5). For additional caveats applicable to Release 8.3(5), see the caveats sections for newer 8.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 8.3(6).

Basic System Services

■ The server does not change the source address it uses for syslog messages after the address is no longer valid. The correct behavior is for a new address to be selected. A workaround is to reload the server after a reconfiguration that has invalidated the address the server was using to source syslog messages. [CSCdi04906]

■ If a user connected via Telnet to a server leaves the **show process** display at the --more-- prompt, and the virtual terminal session idle timer expires, a system reload can occur. [CSCdi05633]

■ The get_pak_size string is missing support for huge buffers. There is no further information available concerning this problem. [CSCdi07091]

■ Configuring a location string longer than 69 characters can cause the system to reload. After configuring, the system prints out a message displaying where the system was configured from and gives the location. If the location is greater than 69 characters in length, it can cause a system reload. The correct behavior would be to truncate the location string. This will be implemented in a future release. [CSCdi07834]

Interfaces

■ Under rare conditions, it is possible for a race in the code for the **show ip arp** command to result in system reloads. This command should be used with care. [CSCdi02706]

■ Keepalives will not bring back an Ethernet interface that is down (transceiver cable disconnected, cable unterminated, and so on) on a CSC/4 processor with an Ethernet MCI. For an Ethernet with keepalives enabled, a keepalive packet is sent every keepalive interval. In this scenario, if a user disconnects the transceiver cable to the Ethernet, and three keepalives were sent but not received, "line protocol" would go down, and the interface would be unusable, as expected. If the user then reconnects the transceiver cable, the correct behavior would be for the keepalives to bring the interface back up within the keepalive period. This does not happen with the CSC/4 processor. The interface remains down despite attempts to lengthen the keepalive period, generate more keepalives, or attempt to clear the ethernet interface with the **clear interface** command. The work-around is to toggle the

keepalives for that particular Ethernet interface using the **no keepalive** command followed by the **keepalive** *n* command. Note: The only action that is *required* for the interface to come back up is to turn off keepalives. Turning them back on is optional, but doing this will correctly turn off "line protocol" if the line goes down in the future. [CSCdi05172]

■ The server will reload if the interface subcommand **bandwidth** is set to zero. [CSCdi05964]

■ The server has problems netbooting when there are multiple paths to the remote TFTP server. [CSCdi06088]

Local Services

■ The sysLocation is read-only. As a workaround, the location can be set with the **snmp-server location** configuration command. [CSCdi07909]

TCP/IP Host-Mode Services

■ The **service tcp-keepalive** command only applies to terminal ports and vtys. [CSCdi05905]

■ In some cases the server sends TFTP ACK responses after an out-of-order packet has been received by a client while netbooting. If the server is busy, this event is quite possible. Sending a second ACK response causes the client and server to get into an argument over what packet to send, and in many topologies it will fail. Common cases look like the following example: [CSCdi06319]

```
!!!!!!.O.........[timeout]
!!!!!!OOOOOOOOO!OOOOOOOOOO!OOOOOOOOOO!OOOO....[timeout]
!!!!!!.!O...... [timeout]
```

X.25

■ An interface input queue may fill up and not recover if an X.25 provider violates the LAPB protocol by exiting from the RNR state with an RR frame instead of an REJ frame. This can cause the serial interface to pause indefinitely and cease transmission. [CSCdi05957]

■ The error message and traceback

```
%X25-3-INTIMEQ Interface [chars], LCN [dec] already in timer queue,
new time [dec]
```

is used as a diagnostic aid; although an unexpected condition was detected and reported, the operation of the server and the X.25 protocol are not affected. If this message is produced, contact Cisco Systems and include the text and traceback of this message as well as the information from the **show version** command. [CSCdi07238]

8.3(4) Caveats/8.3(5) Modifications

This section describes possibly unexpected behavior by Release 8.3(4). Unless otherwise noted, these caveats apply to all 8.3 releases up to and including 8.3(4). For additional caveats applicable to release 8.3(4), see the caveats sections for newer 8.3 releases. The caveats for newer releases precede this section. All the caveats listed in this section are resolved in Release 8.3(5).

Note: There were no reported 8.3(4) caveats/8.3(5) modifications.

8.3(3) Caveats/8.3(4) Modifications

This section describes possibly unexpected behavior by Release 8.3(3). Unless otherwise noted, these caveats apply to all 8.3 releases up to and including 8.3(3). For additional caveats applicable to Release 8.3(3), please see the caveats sections for newer 8.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 8.3(4).

Basic System Services

- Extra lines of default buffers clutter the NVRAM listing. If a user does a write memory command, it will save this configuration to the NVRAM. This will cause them to stay permanently in your configuration even in future releases. A user must use the NO commands for each line to clear the extra messages. [CSCdi04904]

- CLNS hosts do not increment the line count correctly in the **show host** display. Consequently, the command does not respect the **term length n** settings. [CSCdi05083]

EXEC and Configuration Parser

- If during setup user input is delayed, a possible timeout will occur. The server will then loop indefinitely requesting user input. However, no input will be accepted. At this point, the server would have to be reloaded to clear the condition. [CSCdi04427]

- The command **service exec-wait**, which causes the EXEC process to wait if there is input pending on a modem line, has been implemented. This command is intended as a workaround for problems with modems sending junk characters during various types of speed negotiation. The command is disabled by default. [CSCdi04852]

Frame Relay

■ If the **frame relay map** command is issued before the **encapsulation frame relay** command, no action is taken. This is the correct behavior. So although no action is taken, no error message is generated. Not generating an error message in this case was incorrect; an error message is now generated. [CSCdi04576]

■ When a frame relay interface transitions from up to down and vice versa, the system variables are updated but no SNMP trap is generated. This is incorrect behavior. The correct behavior is to generate the SNMP trap. [CSCdi05198]

■ There are instances where the frame relay initialization does not clear the loopback flag. An interface will incorrectly report that it is in loopback if the interface is in loopback mode with HDLC encapsulation, then reconfigured for frame relay encapsulation without shutting down the interface. The workaround is to administratively shut down the interface and then reinitialize it. [CSCdi05483]

Interfaces

■ When multiple IP helper addresses are defined, broadcast packets going out the first interface in the list could be sent with bad checksums. [CSCdi04326]

■ The **no priority-group** command does not accept a number argument. For instance, the command **no priority-group 10** would incorrectly generate an error. [CSCdi04527]

■ Very high average output rates can result in overflows in the computation of the five-minute data rates in the **show interface** command display. This manifests itself as the appearance of nonsensically large values. [CSCdi04665]

■ When an IP packet with options and a time-to-live field of one is received on a fast-switching interface, the packet is erroneously treated as having an IP header checksum error. This is most noticeable when a **traceroute** program is being used with source-routing options. [CSCdi04830]

■ When issuing the command **show interface token 0**, the bia is displayed as *0000.0000.0000*. The correct behavior is for the actual burned-in address of the board to be displayed. [CSCdi05404]

■ If an interface enabled for multiring is reset, either by user action or by keepalives, the server may issue "Bad enqueue" messages. The format of the message follows: [CSCdi05570]

```
 %SYS-2-LINKED: Bad enqueue of 26BFE8 in queue 1E5450
-Process= "Net Background", ipl= 4, pid= 9
-Traceback= 7442 323F8 2EFF2 13ABA 10FF6 2434
```

LAT

■ LAT break sequences sent by connected hosts are not always honored until the host has sent the next data character. [CSCdi03935]

- Certain LAT implementations generate messages with invalid (non-zero) contents of reserved fields. The Cisco implementation, adhering to the specification, rejected such invalid messages. This causes problems communicating with some LAT implementations. [CSCdi04803]

- Enabling **debug lat-packet** may cause a system reload to occur. [CSCdi05100]

Local Services

- The **tacacs last-resort succeed** command does not work on lines configured for dynamic assignment of SLIP addresses. [CSCdi02330]

- Under circumstances that are not well understood, badly formed tty traps are output when the SNMP table becomes corrupted. [CSCdi04744]

- Setting the SNMP tsMsgIntervaltim variable to zero prevents any issuance of the message. The correct behavior is for the message to be issued at intervals decided by the system itself. [CSCdi04860]

- Any authenticated extended TACACS request will change the user's access class. If the field is set in the packet, the TACACS server supplied leaves it set to zero for everything except the login and SLIP address. This should only happen for responses to login requests. [CSCdi05175]

SMDS

- The OUI fields of outgoing SMDS packets may contain random data. This can interfere with communication to nodes that do very strict packet checking. The correct behavior is to zero these fields. [CSCdi05119]

TCP/IP Host-Mode Services

- IP accounting reports the length of fast-switched IP packets incorrectly. [CSCdi04472]

- Incoming connections fail to return to default settings once the session is terminated. [CSCdi04522]

- When multiple connections come very quickly for the same port, a race condition can occur that will cause a system reload. [CSCdi04569]

- If a FIN arrives out of order (for example, because of a lost packet), the connection (now in the CLOSEWAIT state) will no longer accept the missing packets in between, leaving the connection permanently paused. [CSCdi04615]

- When a server has been up more than approximately 25 days, TCP connections to VTYs may take 4 to 6 minutes to be removed after they have been closed. [CSCdi04738]

- Under some obscure conditions (TCP connection receives an RST packet while the connection is closing, and you are waiting for data to go to the terminal), TCP does not release all buffers. Eventually this causes the interface input queue to fill up. The server must be reloaded in order to clear up this condition. This problem is not so serious because it occurs infrequently. [CSCdi04957]

- The success rate for the **ping** command may incorrectly report a low success if ping is run for a very long time. The counter containing the successful ping count overflows. [CSCdi05163]

Terminal Service

- A system reload may occur if a modem line gets in a stuck TCP state and the user hangs up. [CSCdi04585]

- Autobaud does not work to 19.2k with databits 7. [CSCdi04657]

- If there are two or more LAT sessions on a terminal line, one of which has been suspended, the session timeout set by the **session-timeout** command will not affect any of the LAT sessions. [CSCdi05480]

TN3270

- A user cannot put a character in the top left corner of a CICS request for transaction. A workaround is to process the tab key, which will move the cursor over one character to the right. [CSCdi04643]

- Transparent mode is not supported. Applications that depend on the passthrough function of this mode will not work correctly. Some applications known to use this mode are KERMIT, SAS graphics applications, and a serial printing application called TPRINT. [CSCdi04645]

- This problem is caused by the IBM host sending a SET BUFFER ADDRESS command for a 132-column terminal. The IBM 3278-2 terminal (and Cisco's implementation of TN3270) does not support 132 columns. In releases prior to 8.3(4), sending a SET BUFFER ADDRESS command that was out of range could cause the terminal server to pause indefinitely. [CSCdi05323]

X.25

- A number of races exist in the X.25 code. These may result in the issuance of spurious trace back messages, or, rarely, in system reloads. Problems will be observed most often on busy X.25 links connected to busy servers. [CSCdi04049]

- If X.25 encapsulation fails, buffers may be lost. This manifests as a slow loss of memory. [CSCdi04449]

- Under some conditions, the server may reload when the **show x25 vc** command is typed. [CSCdi04481]

- With X.25 TCP enabled, if data continues to be sent to a TCP connection in the CLOSEWAIT state after the X.25 connection has been removed, the server may reload. [CSCdi05031]

- Under some conditions the server may reload when the **show x25 map** command is entered. [CSCdi04536]

- The X.25 switch code does not properly handle forwarding of a RESET packet, causing it to be returned on the line instead of forwarded over the TCP connection. [CSCdi04663]

- When an X.25 PAD connection receives an INDICATION OF BREAK packet, that indication is not forwarded into the data stream of any possible outgoing connection. [CSCdi04908]

- X.25 virtual circuits over which no data have ever been sent are not closed when the configured idle time has passed. If any traffic whatsoever is sent over a virtual circuit, the idle timer will be applied thereafter. [CSCdi05123]

- The **no x25 facility throughput** command does not work. There is no way to remove this facility. [CSCdi05217]

- If more than 22 parameter/value pairs are entered in an **x29 profile** command, memory will become corrupted, leading to a possible system failure. [CSCdi05307]

- Additional calls cannot be made if all available VCs are open, and the first VC is busy, even if the remaining VCs are idle. The correct behavior is to check all VCs and not just the first one on the list. [CSCdi05374]

XRemote

- The restriction that limited XRemote X clients to 31 has been removed. The new maximum is 127. [CSCdi04672]

- XDM will not allow a user to abort a session being set up (with the ^x sequence) once a host has been selected. This can cause the session to hang if the TCP connection to actually start the session is never made. [CSCdi05184]

8.3(2) Caveats/8.3(3) Modifications

This section describes possibly unexpected behavior by Release 8.3(2). Unless otherwise noted, these caveats apply to all 8.3 releases up to and including 8.3(2). For additional caveats applicable to Release 8.3(2), see the caveats sections for newer 8.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 8.3(3).

EXEC and Configuration Parser

- The **setup** dialog for terminal servers support defaults to yes for the "XRemote font servers" response. The default should be no. [CSCdi03928]

- If the user issues multiple **configure** commands, specifying configuration from the network, only the first dialog will default to the correct TFTP server. Subsequent dialogs will default to broadcast TFTP. [CSCdi04128]

- Depending on the different types of error correction enabled (V.42, MNP, none) at the two modem sides, junk input characters may be passed to the terminal server as one modem attempts to negotiate a type of error correction that the other modem does not support. As a result, these junk characters are passed as input to the password prompt, and generally fail the login and disconnect the modem. [CSCdi04261]

- Under some conditions the server may reload when the **show users** command is entered. [CSCdi04339]

- If a **clear line** *n* command is issued for a line that has no process associated with it (for instance a SLIP line), the command will fail, and the line will not be cleared. [CSCdi04530]

Interfaces

- If an error is made while configuring the encapsulation method, the encapsulation will incorrectly be set to NULL. This will be displayed as encapsulation unknown. [CSCdi03593]

Local Services

- The tsMsgTmpBanner and tsMsgSend variables can be neither read nor written. [CSCdi03894]

- The ifMTU variable reflects the configured IP-specific MTU for the interface. It should reflect the configured overall/physical MTU. [CSCdi04022]

- Under rare circumstances, sending of SNMP tty enterprise traps may result in server reloads. [CSCdi04138]

- If extended TACACS is enabled, under certain rare conditions involving retransmissions, corrupted memory could cause the server to reload. [CSCdi04165]

TCP/IP Host-Mode Services

- TFTP over parallel links does not always behave correctly. [CSCdi01274]

- Computation of UDP checksums for packets whose UDP length fields have been corrupted may cause system reloads. [CSCdi03433]

X.25

■ Under some conditions the server may reload when the **show x25 status** command is entered with X.25 debugging enabled. [CSCdi00832]

■ If X.25 switching is enabled, X.29 calls subaddresses of the system's main X.25 address will not be accepted and forwarded to rotaries as documented. [CSCdi03285]

■ Under heavy load, LAPB could mishandle the N(R) field in outgoing I-frames after receipt of an REJ frame. This caused the other end of the link to issue an FRMR frame to reset the link level, which has the side effect of clearing any X.25 virtual circuits going over the link. [CSCdi03558]

■ In an SABM collision, it was possible for LAPB to get confused about its state. The link did come up, but only after a prolonged and unusual exchange of frames. [CSCdi03559]

■ X.29 access lists are not checked for outgoing X.29 connections. [CSCdi03891]

■ A number of races exist in the X.25 code. These may result in the issuance of spurious traceback messages, or, rarely, in system reloads. Problems will be observed most often on busy X.25 links connected to busy servers. [CSCdi04948]

XRemote

■ XRemote font loading does not send a file data reply until additional data is sent by the remote terminal. This causes delays in font loading. [CSCdi02032]

■ The terminal server uses 7-bit comparison to identify escape, flowcontrol, and dispatch characters in the user data stream. This can result in problems when 8-bit character sets are in use, since ordinary user characters may be misinterpreted as control characters. The correct behavior is to give the user control over the type of comparison used. [CSCdi03972]

■ XRemote rejects as invalid any request larger than 64K bytes. Some newer X servers use requests of up to 256K bytes. [CSCdi04105]

8.3(1) Caveats/8.3(2) Modifications

This section describes possibly unexpected behavior by Release 8.3(1). Unless otherwise noted, these caveats apply to all 8.3 releases up to and including 8.3(1). For additional caveats applicable to Release 8.3(1), see the caveats sections for newer 8.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 8.3(2).

Basic System Services

- The **show interface** command display does not mention the fact that the interface counters have never been cleared if they have not been, but it does mention when they were cleared if they have been. [CSCdi02882]

- It is possible for use of the **show host** command while the host-name cache is being updated to result in system reloads. The **show host** command should be used with care. [CSCdi02918]

- The **clear line** command has no effect on lines configured for SLIP. [CSCdi03372]

EXEC and Configuration Parser

- The **arp** interface configuration command does not work on STS-10X terminal servers. [CSCdi02979]

Interfaces

- It is possible for interface-related counter values returned by SNMP to decrease between successive samples when they are expected to increase monotonically. The conditions under which this occurs are not yet well understood. [CSCdi02452]

- It is theoretically possible for garbage messages to be issued when certain types of CSC-R16 failures occur. These failures have never been observed with released Cisco software. [CSCdi02618]

- Type 2 (Interlan) CSC-E Ethernet interfaces may experience rare output hangs. Type 2 interfaces were eliminated from Cisco's product line several years ago and are not supported with CSC/3 processors. [CSCdi02927]

- Frame relay DLCI numbers are not learned properly for the MAC addresses of nodes across frame relay networks. This results in excessive frame relay multicasting of bridged traffic. [CSCdi03103]

- It is possible for the caching of Token Ring RIFs to cause server reloads. This is especially likely in busy networks. This limitation can sometimes be worked around by disabling multiring mode on Token Ring interfaces. [CSCdi03298]

- Entries may occasionally be dropped from the frame relay DLCI map for an interface. This occurs when new entries are added, and is more likely when large numbers of map entries exist. [CSCdi03355]

- The system will allow configuration of priority queueing for LAPB interfaces. This should not be done; configuring priority queueing on a LAPB interface will result in LAPB protocol errors. [CSCdi03500]

- The **slip access-class** configuration command is written to nonvolatile memory and to remote configuration files as **slip access-class**. The system will not parse the files correctly when they are read back in. [CSCdi03630]

- The D15 mode of SMDS is not supported. [CSCdi03660]

- If an asynchronous connection is lost while a SLIP packet is being transmitted over the line, the packet buffer for that packet will not be returned to the free buffer pool. In addition, the packet will remain permanently charged against the input queue quota for the interface on which it arrived. Over very long periods, these conditions can have the cumulative effect of shutting down a terminal server and/or its network interface. This can often be worked around by remedying conditions that lead to unexpected modem line drops and/or by occasionally reloading the terminal server. [CSCdi03785]

- A **frame-relay local-dlci** command will be written to NVRAM or to a network configuration file even if the configured local DLCI is the default. This is harmless. [CSCdi03846]

Local Services

- If no domain name has been set using the **ip domain-name** command, the value returned for the SNMP sysName variable will be invalid. [CSCdi03250]

- When multiple **boot host** commands are specified, there is no failover from the primary server to the secondary server(s). [CSCdi03290]

- The fact that the system enable password is always accepted as a read-write SNMP community string creates a security hole. Correct behavior is to require the user to explicitly configure any community strings to be used. [CSCdi03418]

TCP/IP Host-Mode Services

- Overly optimistic assumptions are made about path latency when an incoming TCP connection is accepted. This may result in over-eager retransmission during the early life of the connection. [CSCdi03099]

- When a TCP segment is acknowledged, the software does not reset the time for retransmission based on the original transmission time of the following segment (if one is queued), but does the first retransmission of the following segment at the time it would have retransmitted the acknowledged segment. This can cause many extra retransmissions when the time between packet sends is close to the calculated initial round-trip time. [CSCdi03136]

- If a TFTP transfer is in progress, and the system receives a retransmission or other packet while expecting an acknowledgment, the transfer will be aborted completely. This can generally be worked around by retrying transfers or configuring the system to retry automatic transfers. Operational impact is usually minor. [CSCdi03810]

X.25

- Clearing X.25 virtual circuits with the **clear x25-vc** command may result in system reloads, especially when many circuits are being established and cleared by other means. The **clear x25-vc** command should be used with caution in busy environments. [CSCdi01622]

- Servers that are heavily loaded and that are sending traffic into congested X.25 networks may issue the SYS-2-INTSCHED messages. These messages may appear in such numbers as to make the server's console unusable. Servers that are running dynamic routing protocols and injecting large routing updates into X.25 networks are especially vulnerable to this failure. The workaround is to reduce network congestion. [CSCdi02772]

- If the NVC option is changed for an interface, this change is not properly executed. It may be applied to another unrelated X25 interface. [CSCdi03790]

- System software cannot be booted over X.25 links. [CSCdi03811]

Customer Information Online

Cisco Systems' Customer Information Online (CIO) system provides online information and electronic services to Cisco direct customers and business partners. Basic CIO services include general Cisco information, product announcements, descriptions of service offerings, and download access to public or authorized files or software. Maintenance customers receive a much broader offering, including technical notes, the bug database, and electronic mail access to the TAC. (Maintenance customers must have authorization from their Cisco contract administrators to receive these privileges.)

For dialup or Telnet users, CIO supports Zmodem, Kermit, Xmodem, FTP PUT, Internet e-mail, and fax download options. Internet users also can use FTP to retrieve files from CIO.

Registration for CIO is handled on line. To reach CIO via the Internet, use Telnet or FTP to `cio.cisco.com` (131.108.89.33). To reach CIO by dialup, phone 415 903-8070 (Mountain View, CA), or 331 64 464082 (Paris, France).