



# *Terminal Server Release Notes for Software Release 9.0*

These release notes describe the features, modifications, and caveats for Software Release 9.0, up to an including maintenance release 9.0(9). Refer to the *Terminal Server Configuration and Reference* document set, dated April 1992, for complete product documentation for Release 9.0.

---

**Note:** Release 9.0(9) is the last maintenance release for 9.0. Maintenance customers will continue to receive phone support from CE, but fixes will be made only to later software releases. If you want to upgrade to a later software release, there is a choice of upgrade paths. Consult your account representative for further information.

---

---

## *Introduction*

These release notes describe the following topics:

- Current software versions, page 2
- Release 9.0 features, page 2
- Terminal server documentation enhancements, page 4
- 9.0(9) software release caveats, page 4
- 9.0(8) caveats/9.0(9) modifications, page 4
- 9.0(7) caveats/9.0(8) modifications, page 4
- 9.0(6) caveats/9.0(7) modifications, page 5
- 9.0(5) caveats/9.0(6) modifications, page 6
- 9.0(4) caveats/9.0(5) modifications, page 7
- 9.0(3) caveats/9.0(4) modifications, page 9

- 9.0(2) caveats/9.0(3) modifications, page 11
- 9.0(1) caveats/9.0(2) modifications, page 14
- Customer Information Online, page 18

---

## *Current Software Versions*

Refer to the Cisco Price List for the version number and ordering instructions for the current 9.0 software release.

---

## *Release 9.0 Features*

This section describes the new functions and new features provided in Release 9.0.

## *New Functions*

New functionality in Release 9.0 of the terminal server software includes the following features:

- The terminal server supports the Flash Memory card system image storage and downloading feature with systems that have the MC+ card. This feature allows writing the system image to Flash memory for booting and system upgrades.

Configuration commands that support this feature include:

### **boot system rom**

EXEC commands that support this feature include:

### **copy tftp flash**

### **copy flash tftp**

### **show flash [all]**

- An online Telnet help feature displays the list of special Telnet control sequences.
- A new option was added to the **buffers** global configuration command that allows dynamic allocation of the buffer settings. The new option is as follows:

### **buffers huge size *number***

- Optional password verification feature is supported on TACACS logins. The new command that supports this feature is as follows:

### **tacacs-server optional-password**

- A transport input feature now allows the system administrator to define the protocols to use to connect to a specific line. The new command that supports this feature is as follows:

**transport input** [telnet | lat | pad | none]

- The ability to connect to multiple X.25 interface is supported. Regular expressions are accepted for the X.121 address and Call User Data. New commands that support this feature are as follows:

[no] **x25 route** [# position]x121-pattern [cud pattern] **interface** interface-name

[no] **x25 route** [# position]x121-pattern [cud pattern] **ip** ip-address

[no] **x25 route** [# position]x121-pattern [cud pattern] **alias** interface-name

- Default SLIP addresses are supported on the **slip address dynamic** command.
- Support is provided for extended Boot Protocol (BootP) requests in SLIP mode. The new command that supports this feature is as follows:

**async-bootp tag** [hostname] data ...

- LAT access lists for specifying access conditions to LAT groups are supported. Regular expressions are accepted for LAT node names, to simplify configuration. The new command that supports this feature is as follows:

**lat access-list** number {permit | deny} regular-expression

- Font download is provided by means of the LAT protocol from DECwindows XRemote sessions, thereby allowing fully operational XRemote over LAT.
- The **translate** command is enhanced. The **swap** keyword now allows X.3 parameters to be set by the host originating the X.25 call or by an X.29 profile. The **unadvertised** keyword prevents service advertisements from being broadcast to the network. The **pvc** keyword specifies that an incoming connection is actually a permanent virtual circuit.

## New Features

New features in Release 9.0 of the terminal server software includes the following:

- The Trivial File Transfer Protocol (TFTP) server now displays verbose messages during file transfer sessions to help you monitor TFTP sessions.
- The terminal server supports protocol translation and the X.3 PAD functionality with appropriate software options on A and M chassis configurations.
- The A chassis terminal server configuration supports the CSC/3 processor card for increased processing efficiency.

---

## *Terminal Server Documentation Enhancements*

The Release 9.0 *Terminal Server Configuration and Reference* manual has undergone slight organizational changes to increase its usability and to include the protocol translation options. All user-related tasks and commands are now found in Chapter 3, "Terminal Server User Commands." The chapters are further divided into system configuration and management tasks and transmission protocol configuration and management tasks. The latter are written for a system administrator. Additional interface configuration information is included to support the Token Ring, SMDS, and Frame Relay media and the serial encapsulation methods available on the terminal server.

In addition, a User Quick Reference booklet is available for Release 9.0 that provides quick reference to and examples of the EXEC user commands. The 5 x 8.5-inch booklet was designed as a portable quick reference for use in making connections and starting sessions on the terminal server.

---

### *9.0(9) Caveats*

There are no outstanding caveats against Release 9.0(9).

---

### *9.0(8) Caveats/9.0(9) Modifications*

No caveats in Release 9.0(8) were fixed in Release 9.0(9).

---

### *9.0(7) Caveats/9.0(8) Modifications*

This section describes possibly unexpected behavior by release 9.0(7). Unless otherwise noted, these caveats apply to all 9.0 releases up to and including 9.0(7). For additional caveats applicable to release 9.0(7), please see the caveats sections for newer 9.0 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 9.0(8).

### *Basic System Services*

- Certain debugging messages are unexpectedly displayed to the console regardless of the state of the **logging console** configuration command. [CSCdi12665]

- Under conditions of high network or TACACS authentication server load, multiple responses can be received by the router or communication server. The multiple responses can be lost and cause the input queue to fill up on the interface the responses were received on. [CSCdi13626]

## *Interfaces and Bridging*

- In certain environments, use of the **source-bridge proxy-explorer** command may cause a router to reload, reporting a “Jump to Zero” error. [CSCdi12328]

## *IP Routing*

- Under extreme circumstances, if autonomous switching is enabled (that is, **ip route-cache cbus** is configured), the router will reload. [CSCdi12415]

## *TN3270*

- Under certain rare circumstances, the communication server may hang running TN3270. [CSCdi13290]

## *Wide-Area Networking*

- The **dialer-list 10** command would cause the router to take an exception. This is because only dialer lists from 1 to 9 are allowed. [CSCdi11279]

---

## *9.0(6) Caveats/9.0(7) Modifications*

This section describes possibly unexpected behavior by release 9.0(6). Unless otherwise noted, these caveats apply to all 9.0 releases up to and including 9.0(6). For additional caveats applicable to release 9.0(6), please see the caveats sections for newer 9.0 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 9.0(7).

## *Basic System Services*

- Changing the logging level via the **logging console** global configuration command does not limit the display of logging messages to the console. The workaround is to login via a virtual terminal and control the logging of messages with the **logging monitor** global configuration command. [CSCdi11676]

## *Interfaces*

- There is a window in which commands to the interface get dropped. [CSCdi11046]

## *TN3270*

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

---

## *9.0(5) Caveats/9.0(6) Modifications*

This section describes possibly unexpected behavior by release 9.0(5). Unless otherwise noted, these caveats apply to all 9.0 releases up to and including 9.0(5). For additional caveats applicable to release 9.0(5), please see the caveats sections for newer 9.0 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 9.0(6).

## *Basic System Services*

- A terminal line configured for flow control will not successfully time out (due to a “session-timeout” configuration) if the line is XOFFed at the time of the timeout. [CSCdi09310]

## *EXEC and Configuration Parser*

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

## *IP*

- A terminal server was continuously looping running SPF, which resulted in locking the terminal server. [CSCdi08089]
- Static routes with destination gateways routed to via an interface that goes down (or is shutdown) are not always removed from the main routing table. [CSCdi09374]
- 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]

- Upon receipt of IP directed broadcast packets, the system erroneously attempts to resolve the directed broadcast address via HP Probe address resolution broadcasts. This occurs if the directed broadcast is destined for a directly connected interface, and that interface is configured for **arp** probe. The system then also correctly forwards the directed broadcast as a data link layer broadcast (if not disabled via the configuration command **no ip directed-broadcast**). The system should be sending the directed broadcast as a (data link layer) broadcast out the directly connected interface, but should not be attempting to perform address resolution on the IP directed broadcast address. [CSCdi09627]
- If an interface flaps, or if an IP routing protocol is removed from the configuration, then the “gateway of last resort” will be lost. [CSCdi09903]

## *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]
- If two users attempt a TACACS login or SLIP address request at the same time, the password one user types in can be sent with both authentication requests, causing authentication failures. This is due to the use of a static buffer. [CSCdi10479]

## *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]
- Telnet connections to a terminal server will not transfer any data during the first couple of seconds after a connection is first opened, resulting in a visible pause if the user begins typing immediately. [CSCdi09576]

---

## *9.0(4) Caveats/9.0(5) Modifications*

This section describes possibly unexpected behavior by release 9.0(4). Unless otherwise noted, these caveats apply to all 9.0 releases up to and including 9.0(4). For additional caveats applicable to release 9.0(4), please see the caveats sections for newer 9.0 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 9.0(5).

## Basic System Services

- If **enable use-tacacs** is configured without defining a **tacacs-server host**, then ANY username/password combination will allow any user to enable. [CSCdi08070]
- If a terminal server is configured with a username having an encrypted password of invalid format, it is possible that the unit will reload when someone tries to log in using that username. The only way to get an encrypted password is for the terminal server to create it. You should not enter **username myname password 7 mypassword** because *mypassword* is not a valid format for a type 7 encrypted password. [CSCdi08805]
- On terminal servers 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]
- The **lapb hold-queue** interface subcommand is not properly stored in the terminal servers configuration memory. [CSCdi08957]

## IP

- When a system is attempting to TFTP boot, it may not know a route to the TFTP server. If the system has multiple interfaces by which it might contact the TFTP server, it can fail to continue to use the interface on which the tftp transfer was just established. The result is that the TFTP boot attempt fails. The system should remember by means of its arp table the interface to use to reach the TFTP server. Configuring the systems NVRAM so that it can only reach the server by one interface at boot time avoids this problem. [CSCdi09068]

## 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]
- Run from ROM software (igs-kr or igs-bprx) may not properly advertise LAT services defined in the terminal server or protocol translator. [CSCdi08837]

## Terminal Service

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



---

## 9.0(3) Caveats/9.0(4) Modifications

This section describes possibly unexpected behavior by release 9.0(3). Unless otherwise noted, these caveats apply to all 9.0 releases up to and including 9.0(3). For additional caveats applicable to release 9.0(3), please see the caveats sections for newer 9.0 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 9.0(4).

### Basic System 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, and this will be corrected in a future release. [CSCdi04806]
- The **show process memory** command can be inaccurate due to incorrect accounting of deallocated memory. [CSCdi07586]
- `sysLocation` is read-only. As a workaround, the location can be set with the **snmp-server location** configuration command. [CSCdi07909]
- The terminal server may experience a software error when the command **show memory free** is executed, and the command must pause for output at any time in displaying the results of the command. The workaround for this is to ensure that the output does not pause by using the command **terminal length 0** before issuing the **show memory free** command. [CSCdi08368]
- 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]

### Interfaces

- Regarding Multibus timeouts and RESETFAIL errors, the linkage between the following system versions and the SBEMON and STRMON Token Ring firmware versions:

FIRMWARE	SYSTEM 8.3	SYSTEM 9.0	SYSTEM 9.1
sbemon 3.2	8.3(5.14)	9.0(3.1)	9.1(1.4)
strmon 1.2	N/A	9.0(3)	9.1(1.4)

It is the firmware that is linked to the system versions and will cause a crash if earlier systems are used. [CSCdi08087]

- When a terminal 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]

## *IP Host-Mode Services*

- If the subnet mask is changed after a system has been operational, the new subnet mask will not be reflected in the IP routing table. A workaround is to reload the system after changing the subnet mask. [CSCdi05915]
- While routing IP, if two ARP style interfaces have the same IP address and one of those interfaces is shut down, the wrong MAC address could get entered into the ARP table. The workaround is to remove the duplicate IP address from the shutdown interface with the **no ip address** interface subcommand. [CSCdi07036]
- TCP connections can exhibit long pauses in data delivery if the cisco 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. TCP connections can exhibit long pauses in data delivery if the Cisco 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]
- 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 to ignore these packets. [CSCdi08651]

## *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 users terminal type matches either the name of the keymap or the first terminal type 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 processing 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 terminals ttycap, Cisco's 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 Cisco's TN3270 to clear to the end of line by sending spaces. [CSCdi08441]

## *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. [CSCdi08034]

## *Wide-Area Networking*

- Once enabled, disabling X.25 routing with the **no x25 routing** command does not disable X.25 call forwarding. [CSCdi06840]

---

## *9.0(2) Caveats/9.0(3) Modifications*

This section describes possibly unexpected behavior by release 9.0(2). Unless otherwise noted, these caveats apply to all 9.0 releases up to and including 9.0(2). For additional caveats applicable to release 9.0(2), please see the caveats sections for newer 9.0 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 9.0(3).

## *Basic System Services*

- The terminal 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 terminal server after a reconfiguration that has invalidated the address the terminal server was using to source syslog messages. [CSCdi04906]
- Users are starting to find that they are running out of memory (seen by a "buffer overflow" message) on their CSC/3 processors when netbooting 9.1 images on top of 9.1 ROMs. Due to Cisco's expanding software base, the CSC/3 does not hold enough memory to directly do this. As a workaround, try one of the following: consider buying a CSC/4 which has 16 Mbytes, use the secondary bootstrap by putting a jumper in bit 9 on your CSC/3, or netboot a compressed image. This will run just a fast once uncompressed. [CSCdi05751]

- Attempting a LAT connection to a line configured with an extended access list (access list of 100 or greater) will cause an error message to be generated and the connection to fail. [CSCdi05928]
- Configuring a location string longer than 69 characters can cause the system to reload. After configuring, the system prints out a message saying that 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 and will be implemented in a future release. [CSCdi07834]

## *Interfaces*

- The terminal server will reload if the interface subcommand bandwidth is set to zero. [CSCdi05964]
- The **test interfaces** command is not working. [CSCdi05977]
- The terminal server has problems netbooting when there are multiple paths to the remote TFTP server. [CSCdi06088]
- The terminal server software decrements the reset counter after some internally generated interface resets, e.g. after the “mac-address” command has been issued. There is no check to see if the reset counter is zero before decrementing it, thus it is possible to decrement the counter to a negative value. Because the value is always displayed as an unsigned positive number, it shows up as a number near 4294967295. [CSCdi06490]
- It is possible for the terminal server to reload in the **show controller token** command. This can only happen if a CSC-R16 or CSC-R16M token ring card is in the reset state. [CSCdi06681]
- When there is a single fiber break or the neighbor station sends constant halt line state(HLS), system CPU utilization will reach 100%. [CSCdi07682]
- When the Cisco terminal server receives a IEEE 802.2 TEST and XID frame that contains both a RIF field which indicates that the frame should traverse the Cisco terminal server, and a destination address which indicates the frame should terminate at the Cisco terminal server, the Cisco terminal server chooses to terminate the frame and reply to it, if needed. This is not in compliance with a strict definition of source-route bridging. This is a minor problem that has little, if any, actual functional impact in most source-bridged networks. This problem will be fixed in a future release. [CSCdi07722]

## *IP*

- The **service tcp-keepalive** command applies only to terminal ports and VTYS. [CSCdi05905]
- Issuing the command **show ip route** may cause a reload to occur. [CSCdi06011]

- In some cases we are sending tftp ACK responses after an out of order packet has been received by a client while netbooting. If the server is busy, this is quite a possible event. 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: [CSCdi06319]

```
!!!!!!O.....[timeout]
!!!!!!00000000!00000000!00000000!0000....[timeout]
!!!!!!O..... [timeout]
```

- **show traffic** will display certain fields as negative numbers once the values wrap into the sign bit. [CSCdi06979]
- The configuration command **no ip routing** only deletes the first of the defined static routes from the configuration, when in fact all of them should be deleted. [CSCdi07190]

## Wide-Area Networking

- When a switch is reconfigured to use a different DLCI to reach the same end address, the terminal server doesn't flush the "deleted" map entry and attempt to learn a new mapping. [CSCdi03757]
- TCP header compression over X.25 does not work in the initial release of 9.0(1). [CSCdi03839]
- An interface input queue may fill up and not recover if an X.25 provider in the RNR state receives and discards an I Frame and then violates the LAPB protocol by exiting from the RNR state with an RR instead of an REJ frame. The symptom is that the serial interface pauses indefinitely and ceases transmission. [CSCdi05957]
- The X.25 PAD code will return a list of ALL X.3 parameters if we received an x.29 "read request" message with more than one parameter requested. This is improper, and will cause some X.25 implementations to clear the connection. The X.25 PAD code will return a list of ALL X.3 parameters if we received an x.29 "read request" message with more than one parameter requested. This is improper, and will cause some X.25 implementations to clear the connection. [CSCdi06432]
- 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 terminal server and the X.25 protocol are not affected. If this message is produced, contact Cisco Systems; include the text and traceback of this message as well as the information from the **show version** command. [CSCdi07238]

- If a virtual circuit is established in order to forward a packet, the packet may not be forwarded immediately on receipt of the CALL CONFIRM. [CSCdi07560]

---

## 9.0(1) Caveats/9.0(2) Modifications

This section describes possibly unexpected behavior by release 9.0(1). Unless otherwise noted, these caveats apply to all 9.0 releases up to and including 9.0(1). For additional caveats applicable to release 9.0(1), please see the caveats sections for newer 9.0 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in release 9.0(2).

### Basic System Services

- Setting the SNMP `tsMsgInterval` 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]
- Setup does not exit automatically when modem disconnect is detected. At this point the user must type control c to exit from setup. [CSCdi04940]
- On very heavily loaded systems, the CPU utilization percentages given by the **show process**, and **show cpu** commands, and the interface utilization percentages given by the **show interface** command, may fail to decay properly, or may be displayed as impossible values. [CSCdi05168]
- Any “authenticated” extended tacacs request will change the users access class (if the field is set in the packet, the tacacs server supplied leaves it 0 for everything except login and slip address). This should only happen for responses to login requests. [CSCdi05175]
- The command **show flash** is not currently supported on terminal servers and protocol translators. The command **show flash** is not currently supported on communication servers and protocol translators. [CSCdi05506]
- If a user connected via TELNET to a terminal server leaves the **show process** display at the “--more--” prompt, and the virtual terminal session idle timer expires, a system reload may occur. [CSCdi05633]
- Under unusual circumstance when an SNMP packet is received some memory will be lost, over time this could use up all system memory. Two things must be true for this to happen; a bad community name is in the snmp request resulting in an authentication trap, and the snmp request must have over 14 variables in it. [CSCdi06309]

### Interfaces

- If the **frame relay map** command is issued before the **encapsulation frame relay** command, then 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]
- Very high average output rates can result in overflows in the computation of the five-minute data rates in the **show interface** display. This manifests itself as the appearance of nonsensically large values. [CSCdi04665]

- Older HP probe clients (notably old versions of OfficeShare) require support for the “where is gateway” packet. This feature is not supported. [CSCdi04667]
- 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]
- The **dialer fast-idle** command ignores parameters. [CSCdi05002]
- Under some circumstances, primarily involving a non-zero hold queue on an Ethernet interface, the use of the HP probe feature may cause the terminal server to lose memory. [CSCdi05186]
- Specifying **ring-speed 4** actually results in **ring-speed 16** and vice versa. [CSCdi05224]
- When issuing the command **show interface token 0** the bba is displayed as 0000.0000.0000. The correct behavior is for the actual burned in address of the board to be displayed. [CSCdi05404]

## IP

- ICMP Information requests do not cause entries to be made in the ARP table. Instead an ARP request is broadcast before sending the ICMP reply. This can cause problems with devices that need to learn the subnet portion of their IP address from the ICMP Reply. [CSCdi04328]
- If an IP address is removed from an interface using the **no ip address**, all routes using that interface are deleted from the IP routing table. This is sometimes unnecessary when there is an additional path to the target. [CSCdi04396]
- Attempts to create IP static interface routes through interfaces which do not have IP addresses assigned will fail. [CSCdi04898]
- If two interfaces have the same IP address and one of them is shut down, the other interface will not respond to an IP ping. [CSCdi04913]
- Under some obscure conditions (TCP connection receives a RST packet while the connection is closing and we 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 terminal server must be reloaded in order to clear up this condition. This problem is not so serious because the condition occurs infrequently. [CSCdi04957]
- If a network broadcast address and a default subnet are configured, the system will erroneously route a network broadcast to the default subnet. This can lead to routing table instabilities. A workaround is to specify the broadcast address of 255.255.255.255. [CSCdi05052]
- The **no ip routing** command does not stop IP routing processes. [CSCdi05157]
- 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]

- Under rare circumstances, it is believed to be possible for a proxy ARP reply to be processed incorrectly, resulting in incorrect entries in the ARP table. These entries will give valid MAC addresses for incorrect IP addresses. This behavior has never actually been observed in the field, and should occur only when the interface on which the original proxy ARP reply is received undergoes an up-to-down state transition immediately after the packet arrives. [CSCdi05169]
- Configuring **ip route 0.0.0.0 null 0** will result in the route showing up multiple times in the routing table. [CSCdi05754]

## *LAT*

- Enabling **debug lat-packet** may cause a system reload to occur. [CSCdi05100]
- Certain LAT error messages do not give sufficient data to actually tell what it wrong. In particular, the “% Reach limit of struct” message didn’t give any indication of which struct was involved. [CSCdi05178]

## *Terminal Service*

- Login strings do not work properly. If a connection is made to a host for which a login string has been defined, the login string is not sent, and a “bad login string” message is issued on the system console. There is no workaround. [CSCdi05791]

## *TN3270*

- 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 stuff, and a serial printing application called TPRINT. [CSCdi04645]
- For IBM hosts, 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]

## *Wide-Area Networking*

- 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]
- The **show interface** and **show X25 vc** commands did not indicate when the window at packet level(x25) and/or frame level(lapb) was closed. [CSCdi04981]
- With X25 TCP enabled, if data continues to be sent to a TCP connection in the CLOSEWAIT state after the X25 connection has been removed, then the terminal server may reload. [CSCdi05031]



- Attempting to issue a **clear x25-vc** command to remove idle X.25 SVCs may cause the terminal server to reload. [CSCdi05037]
- Issuing the command **no dialer fast-idle** incorrectly resets the **dialer idle-timeout** instead of the **dialer fast-idle timeout**. [CSCdi05041]
- 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]
- 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]
- The **no x25 facility throughput** command does not work. There is no way to remove this facility. [CSCdi05217]
- If more than one X25 facility is configured, and the **x25 rpoa wan** command is one of those facilities, then disabling the rpoa facility may cause the terminal server to reload. [CSCdi05219]
- When configured for ANSI ANNEX D frame relay, the terminal server incorrectly uses dlci 1023. This causes the line protocol to be declared down. The correct behavior is to use dlci 0. The workaround is to disable keepalives on a particular interface. [CSCdi05280]
- 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. [CSCdi05374]
- The frame relay encapsulation code doesn't correctly check the status of a DLCI. The result is that packets can be sent on a DLCI which the frame relay switch has indicated as deleted via the LMI messages. This problem shows up if a terminal server is misconfigured such that a mismatch exists between the terminal servers DLCI and those defined in the frame relay switch. The workaround is to configure the terminal server with the correct DLCIs. [CSCdi05481]
- 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 the interface and then reinitialize it. [CSCdi05483]
- If two **no dialer** commands are issued in a row, there is a high probability that the terminal server may reload. [CSCdi05594]

## *XRemote*

- 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]

---

## *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).

This document is to be used in conjunction with the *Terminal Server Configuration and Reference* publication.

Access Without Compromise, Catalyst, CiscoFusion, CiscoWorks, Internetwork Operating System, IOS, Netscape, SMARTnet, *The Packet*, UniverCD, Workgroup Director, and Workgroup Stack are trademarks, and Cisco Systems and the Cisco logo are registered trademarks of Cisco Systems, Inc. All other products or services mentioned in this document are the trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

Copyright © 1994, Cisco Systems, Inc.  
All rights reserved. Printed in USA