Doc. No. 78-0917-09
March 28, 1994

CISCO SYSTEMS

Protocol Translator 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 *Protocol Translator Configuration and Reference* manual, 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

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 protocol translator software includes the following features:

- The protocol translator 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*

- 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 protocol translator software include the following:

- The Trivial File Transfer Protocol (TFTP) server now displays verbose messages during file transfer sessions to help you monitor TFTP sessions.
- Protocol translation is now available as an option on the M chassis terminal server. This configuration and the CPT both support the CSC/3 processor card for increased processing efficiency.

Protocol Translator Documentation Enhancements

The Release 9.0 *Protocol Translator Configuration and Reference* manual has undergone slight organizational changes to increase its usability. All user-related tasks and commands are now found in Chapter 3, "Protocol Translator 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 protocol translator.

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 protocol translator.

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]

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]

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]

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).

EXEC and Configuration Parser

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

Wide-Area Networking

- All ARPs over an SMDS link were being discarded preventing routing of IP traffic over SMDS. [CSCdi09781]

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 a protocol translator 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 cisco unit 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 protocol translators 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 protocol translators configuration memory. [CSCdi08957]

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]
- The **debug ?** command doesn't show serial options if only serial interface type is HSSI. [CSCdi07674]
- sysLocation is read-only. As a workaround, the location can be set with the **snmp-server location** configuration command. [CSCdi07909]
- The protocol translator 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]

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]

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. 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 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]

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 protocol translator 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 protocol translator after a reconfiguration that has invalidated the address the protocol translator was using to source syslog messages. [CSCdi04906]
- 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]
- The **setup** command does not allow CLNS station IDs containing a zero to be entered if an ID other than the default was desired. Possible workarounds include using the default station ID supplied, or using a station ID that does not contain a zero. [CSCdi06665]

- 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]

Wide-Area Networking

- When a switch is reconfigured to use a different DLCI to reach the same end address, the protocol translator 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 protocol translator 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 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]
- 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]
- Under some circumstances, primarily involving a non-zero hold queue on an Ethernet interface, the use of the HP probe feature may cause the protocol translator to lose memory. [CSCdi05186]
- If a user connected via Telnet to a protocol translator 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]

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. The **show interface** and **show X25 vc** commands have been modified to display this message "Window is closed" For the **show x25 vc** command the above message indicates the VC is packet is level flow controlled and the window is closed. For the **show interface** command the above message indicates the interface is frame level flow controlled and the window is 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 protocol translator may reload. [CSCdi05031]
- Attempting to issue a **clear x25-vc** command to remove idle X.25 SVCs may cause the protocol translator 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 protocol translator to reload. [CSCdi05219]
- When configured for ANSI ANNEX D frame relay, the protocol translator 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. The correct behavior is to check all VCs and not just the first one on the list. [CSCdi05374]

- The frame relay encapsulation code does not 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 protocol translator is misconfigured such that a mismatch exists between the protocol translators DLCI and those defined in the frame relay switch. The workaround is to configure the protocol translator 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 protocol translator 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 *Protocol Translator Configuration and Reference* publication.