

Vanguard Managed Solutions

Vanguard Applications Ware
Basic Protocols

TCP/Telnet

Notice

©2003 Vanguard Managed Solutions, LLC
575 West Street
Mansfield, Massachusetts 02048
(508) 261-4000
All rights reserved
Printed in U.S.A.

Restricted Rights Notification for U.S. Government Users

The software (including firmware) addressed in this manual is provided to the U.S. Government under agreement which grants the government the minimum “restricted rights” in the software, as defined in the Federal Acquisition Regulation (FAR) or the Defense Federal Acquisition Regulation Supplement (DFARS), whichever is applicable.

If the software is procured for use by the Department of Defense, the following legend applies:

Restricted Rights Legend

Use, duplication, or disclosure by the Government
is subject to restrictions as set forth in
subparagraph (c)(1)(ii) of the
Rights in Technical Data and Computer Software
clause at DFARS 252.227-7013.

If the software is procured for use by any U.S. Government entity other than the Department of Defense, the following notice applies:

Notice

Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction, and disclosure are as set forth in FAR 52.227-19(C).

Unpublished - rights reserved under the copyright laws of the United States.

Notice (continued)

Proprietary Material

Information and software in this document are proprietary to Vanguard Managed Solutions (or its Suppliers) and without the express prior permission of an officer of Vanguard Managed Solutions, may not be copied, reproduced, disclosed to others, published, or used, in whole or in part, for any purpose other than that for which it is being made available. Use of software described in this document is subject to the terms and conditions of the Vanguard Managed Solutions Software License Agreement.

This document is for information purposes only and is subject to change without notice.

Part No. T0106-07, Rev H
Publication Code DS
First Printing November 1998

Manual is current for Release 6.3 of Vanguard Applications Ware.

To comment on this manual, please send e-mail to LGEN031@vanguardms.com

Overview

Introduction

The Telnet protocol uses the reliable services of Transmission Control Protocol (TCP) to provide remote terminal access. With Telnet, you can communicate with a remote Vanguard node across an IP network by connecting to its control terminal port (CTP). Telnet also provides a client through which you can log on to the CTP of another Vanguard node or any other server.

In This Manual

Topic	See Page
About TCP/Telnet	2
Telnet on a Vanguard Node	3
Configuring TCP	6
Starting a Telnet Session	8
Telnet Command Mode	12
AT Dialer	14
Statistics	23
Server and Client Support	27

About TCP/Telnet

Why Use Telnet?	Telnet lets you access a CTP on any host on the IP network without using a PAD port provided that Telnet software is installed on that host. The Telnet server residing in the node connects the CTP to the connection requests coming from the other hosts on the network.
TCP	<p>TCP is a connection-oriented, end-to-end reliable protocol which fits into a layered hierarchy of protocols that support multi-network applications. TCP sets up a connection allowing communication between pairs of processes in network nodes. The nodes are attached to distinct but interconnected computer communication networks.</p> <p>TCP interfaces on one side to user or application processes (client) and on the other side to a lower level network protocol such as Internet Protocol (IP).</p>
Telnet Protocol	<p>The Telnet protocol provides a standard method of interfacing terminal devices and terminal-oriented processes to each other. A Telnet connection is a TCP connection used to transmit data interspersed with Telnet control information.</p> <p>The Telnet protocol lets you access a remote host's terminal. Your local Telnet session is the client and the remote session is the server.</p>
RFCs Supported	<p>The following RFCs are supported in this implementation of Telnet:</p> <ul style="list-style-type: none">• RFC-854 Telnet Protocol Specification• RFC-858 Telnet Suppress Go Ahead Option• RFC 1091 Telnet Terminal Type Option

Telnet on a Vanguard Node

Introduction

This section describes how Telnet is implemented on Vanguard nodes.

Telnet Server

A Telnet server resides on the node. It provides the requested service to the client, which is any host on the IP network to which the node is connected. The server listens for incoming connection requests and connects the client to the CTP. You can perform any activity that is normally possible through a direct CTP access. However, if someone else has accessed the CTP, the request is rejected because multiple users cannot access the CTP at the same time.

Telnet Client

The Telnet client is responsible for establishing a connection over the network with the server that provides the desired service. It lets you set up a Telnet session with any other host or node that is connected to the same IP network and has a Telnet server.

Example Showing the Node Without the Telnet Feature

Figure 1 shows remote terminal access without Telnet. The only way to configure a Vanguard node is with a local asynchronous terminal. You can use the terminal to configure other Vanguard nodes in the network. However, you cannot access Vanguard nodes across the LAN from the workstation.

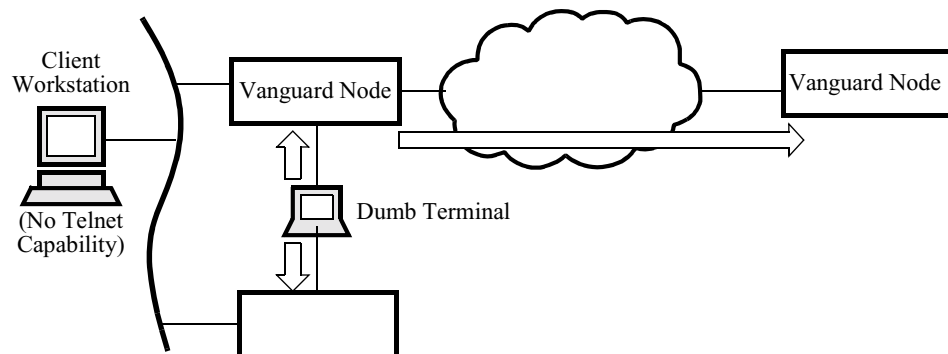


Figure 1. The Vanguard — Without Telnet

Example Showing the Telnet Feature

Figure 2 shows remote terminal access with the Telnet feature. You can access the CTP port on a Vanguard, from a workstation across the LAN using the IP interface on the Vanguard node. You can also access node (1) from a dumb terminal and then set up Telnet sessions with node (2) and node (3) in the network.

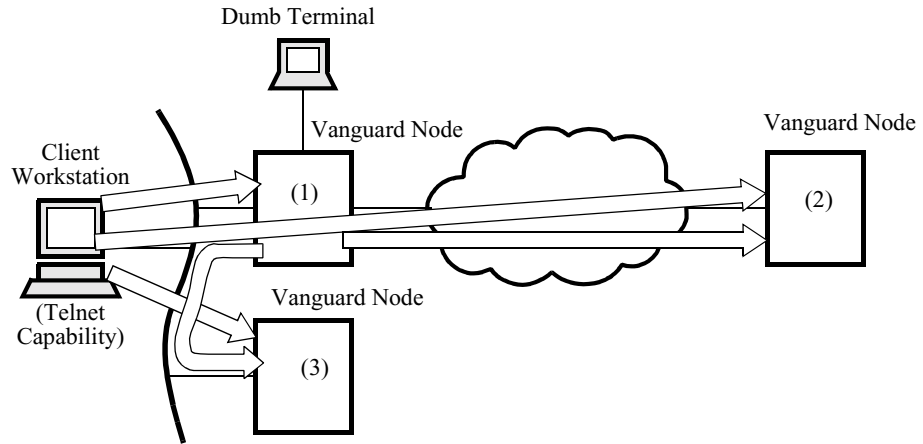


Figure 2. Telnet in Vanguard Nodes

Frame Relay Application Before Telnet

Figure 3 shows a Frame Relay application before the Vanguard supported the Telnet feature. Annex G was required to access a remote Vanguard node in a Frame Relay network.

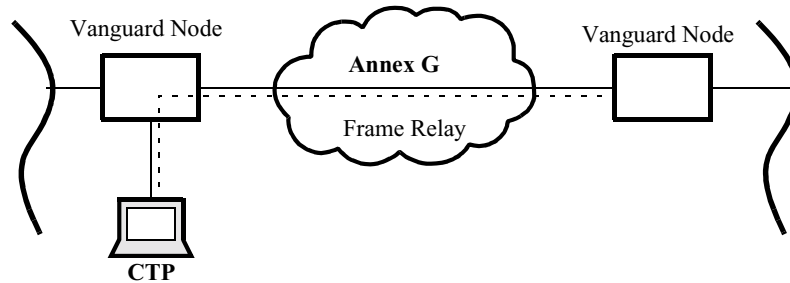


Figure 3. Frame Relay with Annex G

Frame Relay after Telnet

Figure 4 shows that with the Telnet support in the Vanguard nodes, you can use Bypass in a Frame Relay network at a substantial cost savings.

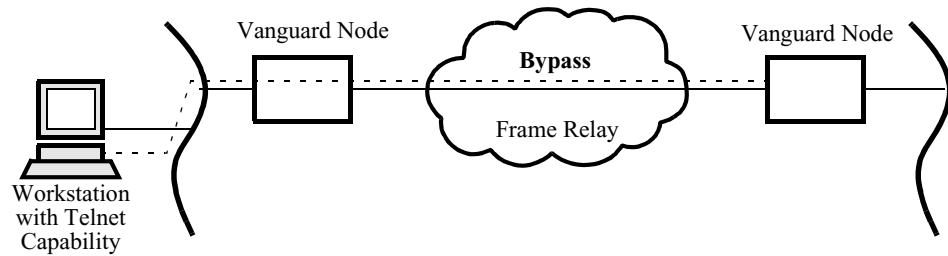


Figure 4. Frame Relay with Bypass

How to Start TCP

If you do not configure TCP in the Vanguard nodes (see the section, “Configuring TCP”), once the node is powered on, TCP automatically comes up with default values and is ready to accept connection requests.

How to Start Telnet

The Telnet server comes up automatically after powerup. You need to start the Telnet client. See “Starting a Telnet Session” for additional information.

Configuring TCP

Introduction

This section describes how to configure TCP. If you do not configure TCP, the node accepts the default values at startup.

Example of TCP Record

Figure 5 shows the Configure menu. You can access the TCP record from this menu.

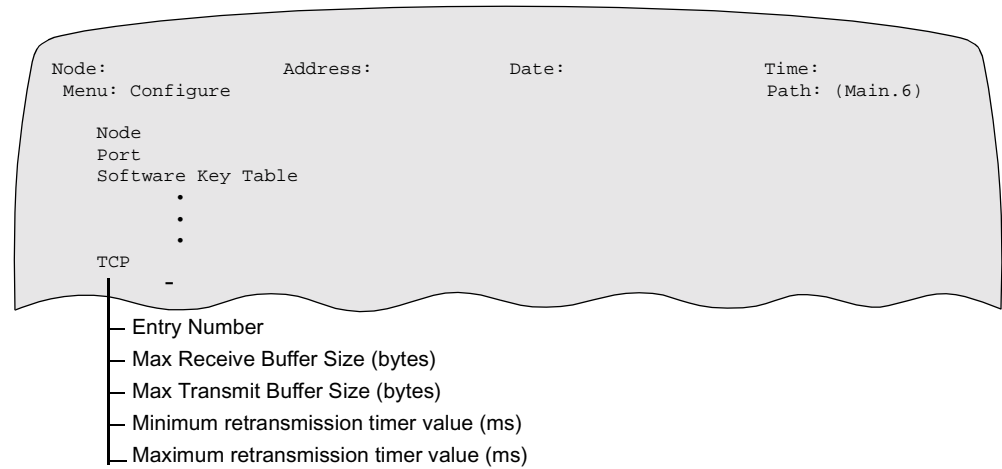


Figure 5. TCP Record

Parameters

These are the TCP parameters:

Note

Unless otherwise indicated, perform a TCP boot for parameter changes to take effect.

Entry Number

Range:	1
Default:	1
Description:	Entry number used to reference this table record.

Max Receive Buffer Size (bytes)

Range:	100 to 65000
Default:	100
Description:	Specifies the maximum size of the Receive buffer for all TCP connections.

Max Transmit Buffer Size (bytes)

Range:	100 to 65000
Default:	100
Description:	Specifies the maximum size of the Transmit buffer for all TCP connections.

Minimum retransmission timer value (ms)

Range:	100 to 5000
Default:	200
Description:	The minimum value, in milliseconds, of the retransmission timer for TCP. The retransmission timer value in TCP is calculated dynamically using a retransmission algorithm. The minimum retransmission timer value specified is the lower limit on this dynamic TCP retransmission timer value.

Maximum retransmission timer value (ms)

Range:	100 to 50000
Default:	5000
Description:	The maximum value, in milliseconds, of the retransmission timer for TCP. The retransmission timer value in TCP is calculated dynamically using a retransmission algorithm. The maximum retransmission timer value specified is the upper limit on this dynamic TCP retransmission timer value.

Starting a Telnet Session

Introduction

This section describes how to start a Telnet session.

Connecting to the CTP Through the Server

As you try to establish a Telnet session with the Vanguard control terminal port (CTP), the Telnet implementation on the host where you are working determines the types of messages that appear.

For example, if you are trying to set up a Telnet session from an HPUX host to the Vanguard nodes and another user has already activated a Telnet session with the specified node, this message appears:

Connection refused by foreign host.

If another user is connected to the specified node through the PAD port, the following message appears:

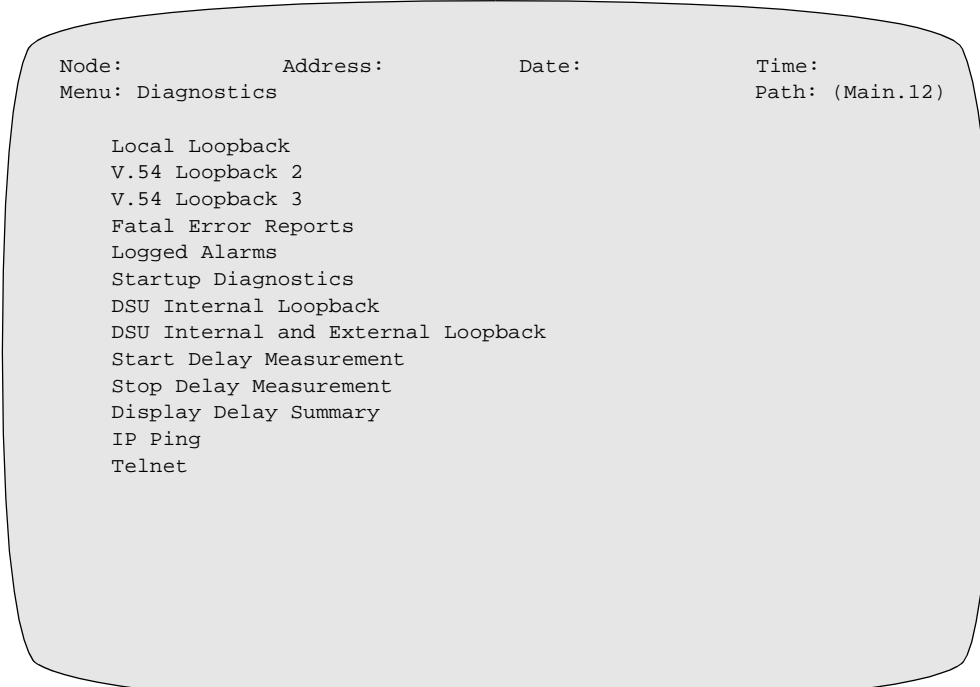
Connection closed by foreign host.

Other client implementations display different messages.

Once you are connected, the CTP screen appears.

Example of Diagnostics Menu

Figure 6 shows the Diagnostics menu. You can access the Telnet client from this menu.



```
Node:                Address:            Date:              Time:
Menu: Diagnostics    Path: (Main.12)

Local Loopback
V.54 Loopback 2
V.54 Loopback 3
Fatal Error Reports
Logged Alarms
Startup Diagnostics
DSU Internal Loopback
DSU Internal and External Loopback
Start Delay Measurement
Stop Delay Measurement
Display Delay Summary
IP Ping
Telnet
```

Figure 6. Diagnostics Menu

Configuration Procedure

Follow these steps:

Step	Action	Result/ Description
1	Select Diagnostics from the Main menu.	The Diagnostics menu appears.
2	Select Telnet .	<p>This prompt appears: IP Address <this terminal type> For help on the parameter, enter ? at the prompt.</p> <p>■ Note The terminal type parameter is optional. You need to indicate terminal type when you are logging into a server other than a Vanguard node. For example, if you are trying to access a UNIX server, enter the terminal type, such as xterm or vt100, on which the CTP is displayed.</p>
3	Enter the IP address in dotted notation. For example: 134.33.206.32	<p>This message appears: Trying...</p> <p>This message appears when the connection is established: Connected to <IP address> Escape character is '^J'. You are in data mode of a Telnet session on the remote node. You can perform any CTP function except for KERMIT Save Configuration and KERMIT Restore Configuration if the remote node is a 65xx or Vanguard device.</p>

Step	Action (continued)		Result/ Description
	If...	Then...	
<p>3 (Cont)</p>	<p>You enter an invalid address</p>	<p>This message appears: Bad address, try again. Press any key to continue...</p>	<p>The Telnet client quits and the Diagnostics menu appears if you press any other keys except for Ctrl/T. You can press Ctrl/T to display the Main menu.</p>
	<p>You enter an IP address that exceeds 15 characters</p>	<p>This message appears: Length exceeds expected, enter 0 to 15 characters. Press any key to continue...</p>	<p>The Telnet client quits and the Diagnostics menu appears if you press any other keys except for Ctrl/T. You can press Ctrl/T to display the Main menu.</p>
	<p>The remote server refuses the connection request or is unreachable</p>	<p>The client displays the message: Connection closed. Press any key to continue...</p>	<p>The client exits.</p>
	<p>The client cannot establish a connection due to a local TCP problem</p>	<p>This message appears: TCP open failed. Press any key to continue...</p>	<p>The client exits.</p>
<p>4</p>	<p>Enter Ctrl/] to enter command mode.</p>		<p>The telnet> prompt appears. See the “Telnet Command Mode” section, next, for additional information.</p>

Step	Action (continued)		Result/ Description
5	Close command mode using these methods: Enter either the close or quit commands. Press Return.		This message appears: Connection closed. Press any key to continue... You are in Telnet data mode. ■ Note The “send ayt” command or an unsupported command also closes the command mode.
	<i>If...</i>	<i>Then...</i>	
	The connection aborts because of a memory error	This message is displayed: Memory error: connection closed. Press any key to continue...	The client exits because it is not getting enough dynamic memory. Wait until the load on the node comes back to normal before you try again.

Telnet Command Mode

Introduction

This table describes the user commands supported by the Vanguard Telnet client when you are connected to the CTP using an asynchronous terminal.

Command	Description
close	Lets you close the Telnet connection.
quit	Lets you close the Telnet connection.
status	Provides the status of the connection. The following status message appears: Connected to <destination IP address> Operating in character-at-a-time mode Escape character is '^]'.
send	Lets you send a command to the server. The Telnet client supports these two commands: end ayt — Are you there? Telnet exits command mode when you enter this command. send ? — Displays the following message: ayt Send Telnet "Are You There" ? Display send options ■ Note If you only enter send (without the ?) , this message appears: need at least one argument for 'send' command. 'send?' for help.
?	Prints the help information. Telnet stays in command mode. The following help message appears: close current connection quit exit telnet status print status information send transmit special characters ('send?' for more) ? print this help information

Client Implementation

When you set up a Telnet client session from the Vanguard node, the client implementation on your workstation determines the commands that appear in the command mode session.

For example, set up a Telnet session from an HP workstation to a Vanguard node. The client on the HP workstation uses **Ctrl/J** to enter command mode just like the Vanguard Telnet client session. When you display the supported commands, you are actually in command mode of the first client, the HP workstation. Therefore, the commands that appear are the supported commands for the HP workstation and not for the Vanguard.

**If You Use Other
Commands**

If you enter commands other than those listed in the Telnet Commands table, this message appears:

Ambiguous command.

Telnet exits command mode.

**If You Press the
Return Key**

If you press Return at the **telnet>** prompt, Telnet exits command mode.

AT Dialer

Introduction

This feature allows you to establish a Telnet session to the Telnet Server in the Vanguard. This provides a means for you to enter ISDN dial information, or to access your local Vanguard CTP from a PC. This feature was first introduced in Release 4.55 for the Vanguard 310 Series.

AT Dialer Profile configuration shares many features with the ATPAD port.

Applications Using This Feature

The typical application that this feature has been designed for is connecting to the AT Dialer via Telnet to make an ISDN call or to call your local Vanguard control port (CTP). You can also connect to a remote node's CTP by connecting to the local node's Telnet Server, and making a Network SVC call from there to the remote node. The following diagrams show some of these example configurations.

- Dial-out from a LAN-connected PC (Figure 7).

In this scenario, you would open a Telnet session to the Telnet Server resident in the Vanguard. When the session is established you receive an AT "OK" prompt. You can then use an AT Dial Command to make an ISDN call, or to call the local CTP.

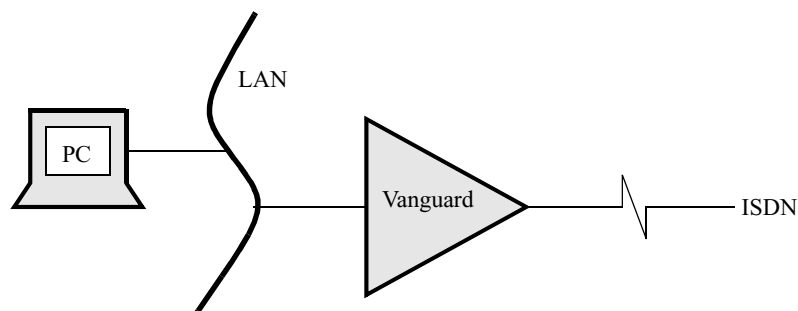


Figure 7. Dial-out from LAN-Connected PC

- Dial-out over IP-encapsulated async connection (Figure 8).

This application is identical to the previous one, except that PPP or SLIP is used in connecting the node. You would still establish a telnet session to make an ISDN call or to call the local CTP.

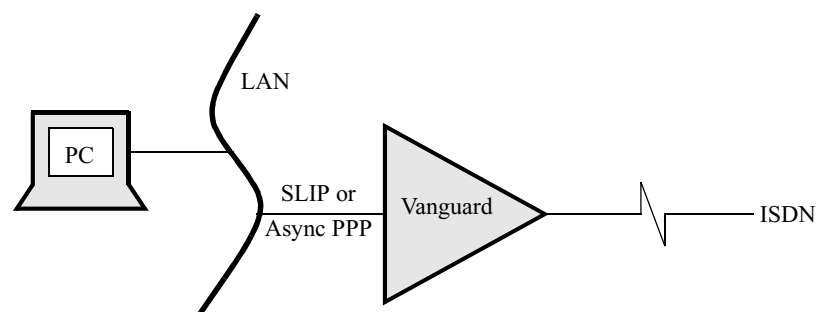


Figure 8. Dial-out over IP-Encapsulated Async Connection

- Remote CTP access from a PC on a Local LAN, over a non-IP network (Figure 9).

In this application, the remote CTP is accessed by connecting to the local node's Telnet server, and making a network SVC call into the remote node. You can then access the remote node's CTP for examination and/or configuration.

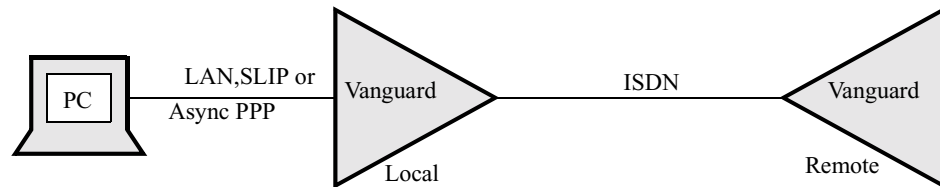


Figure 9. Remote CTP Access Vial an SVC Call

AT Dialer Operation When you connect to the AT Dialer by Telnetting into the node (either over a LAN or through the SLIP or PPP port), the **OK** prompt appears. You can then enter an AT Dial Command in the following format:

ATD555-1212 <CR>

See the “Called Number Format” section on page 17 for additional information about the options for the called number format.

The port will then respond with:

CONNECT

If the call is completed successfully, or:

NO CARRIER

If the call could not be completed.

Terminating the Call

If the call is an ISDN call made by Telnetting into the node, you can clear the call by typing:

ATH <CR>

If the call is an SVC network call from the Telnet server, you can clear the call by typing the AT escape sequence:

+++ <CR>

The port will then respond with:

OK

You then type:

ATO <CR>

to go back online, or:

ATH <CR>

to clear the call.

CTP Access Using AT Dialer

To access the CTP after you Telnet into the Telnet Server, type:

ATDS0 <CR>

Another way that you can access a local CTP or a remote CTP from any ATPAD port is to type:

ATD <nodeaddress+98> <CR>

You can terminate the call to the CTP by selecting menu item 1 from the Main menu, or by typing the AT escape sequence (**+++**) and **ATH** to end the call.

Supported Hayes AT Commands

This table describes the Hayes AT commands that you can use to make and clear X.25 calls from an ATPAD:

Command Name	Description	Use
ATD (ATDT, ATDP)	Call command	You can place a call by entering the address after the command name on the command line. All non-decimal digits, except &, or characters are discarded.
ATDS (ATDSn)	Call stored number	You can place a call using one of the stored addresses (stored in the AT Dialer Profile configuration record). If you specify “n” (where n=0-3), that stored number is used. If you do not specify a number, the address n=0 is used.
ATH	Clear call	You can clear a network call.
A/	Re-execute the last command	Do not enter a <CR> after the command. Use this command when redialing a busy number. You can type the command AT<CR> to clear the command buffer, which stores the last command.

Called Number Format

The Dial Command string format is as follows:

ATD 555-1212

You can add a dial modifier to the command to specify whether this is an ISDN call or an X.25 call:

- **P** means it is an X.25 Packet Call
- **T** means it is an ISDN Telephone Call

For example:

ATDT 555-1212

The second T indicates that this is an ISDN telephone call.

ATDP 70798

The P indicates that this is a packet call.

You can also specify the network port number that you wish to connect to by entering another dial modifier. For example, enter the port number and an ampersand (&) before the number to be called:

ATD 2&555-1212

You can enter both call type and port number in the same Dial Command:

ATDP 3&10098

Additional Notes

The following notes apply for this feature:

- There are two methods for specifying the calling method and the network port selection: in the dial string as discussed in the previous section, or using the AT Dialer Profile as discussed in the following section. (See the Preferred Calling Method and Preferred Network Port configuration parameters.) If you specify the dial modifier in the dial string, it will override any specification set in the Dialer Profile.
- When you are clearing a dial call, you must specify the port number of the call either using the AT Dialer Profile or in the Hang-Up command (i.e., **ATH 3**). If you do not specify the port number, the lowest-numbered ISDN port is cleared.
- The AT Dialer provides optional Account/Password authentication. If enabled, the password verification sequence must be successfully completed before you will be allowed to make an AT command. You will have three tries to successfully complete the password verification sequence. If the third attempt fails, the Telnet session is closed.

■ Note

To use this feature, you must configure an entry in the node's NUI table.

AT Dialer Profile Configuration

From the Configure Menu using your Vanguard CTP, you must establish an AT Dialer Profile. Up to four profiles can be configured using the following parameters, but profiles 2, 3, and 4 are currently not used.

When an AT Dialer Profile is not configured, then by default, the AT Dialer Preferred Calling Method is “Telephone”. To change this default, configure the AT Dialer Profile (number one), to use “Packet”. This can be overridden at the command line by entering “ATDT###”.

■ Note

The Telnet Server always uses parameter profile number one.

Profile Number

Range:	1-4
Default:	1
Description:	Specifies the AT Dialer profile number. This number is used during the port configuration. ■ Note The Telnet Server always uses parameter profile number 1.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Escape Character

Range:	0-127
Default:	43
Description:	Specifies the character used to escape to command mode.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Carriage Return Character

Range:	0-127
Default:	13
Description:	Specifies the character used to terminate commands.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Line Feed Character

Range:	0-127
Default:	10
Description:	Specifies the character used to move the cursor to a new line.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Back Space Character

Range:	0-127
Default:	8
Description:	Specifies the character used for a back space during character editing.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Data Forwarding Character

Range:	0-127
Default:	13
Description:	Specifies the character used to forward packets to the network. A value of 0 disables this function.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Escape Sequence Timer

Range:	1-51
Default:	10
Description:	Specifies the value of the escape sequence guard time in 100-millisecond increments. A value of 10 corresponds to 1 second.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Data Forwarding Timer

Range:	0-255
Default:	1
Description:	Specifies the value of the forwarding idle timer, in 1/20 seconds, that determines when data is packetized and sent to the network. A value of 0 disables the timer.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Packet Size

Range:	128, 256, 512, 1024
Default:	128
Description:	Specifies the maximum size of packets that can be formed when in PAD mode.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Echo

Range:	ON, OFF
Default:	ON
Description:	Specifies whether character echo is used during command mode.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Stored Addresses

Range:	4 sets of 0-64 alphanumeric characters
Default:	(blank)
Description:	Specifies the addresses to be used when making calls with the ATDSn Command.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Result Codes

Range:	ALPHA, NUM, NONE
Default:	ALPHA
Description:	Specifies if result codes are to be displayed in alpha or numeric format. If NONE is specified, this suppresses the result code display.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Password Protection

Range:	ON, OFF
Default:	OFF
Description:	Specifies if the AT Dialer is to prompt for user account and password before allowing access to command mode.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Same Destination

Range:	YES, NO
Default:	NO
Description:	Specifies if the AT Dialer is to allow two ISDN B channels to dial the same destination.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Preferred Calling Method

Range:	TELEPHONE, PACKET
Default:	TELEPHONE
Description:	Specifies the calling method used for the AT Dialer. ■ Note If the calling method is specified in the Call Command (using T or P), that value overrides the value specified by this parameter.
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Preferred Network Port

Range:	0-3
Default:	0
Description:	<p>Specifies the network port you wish to connect to. If the value is set to 0, the call is routed using the node's Route Selection Table.</p> <p>■ Note If the network port is specified in the Call Command (using &), that value overrides the value specified by this parameter.</p>
Boot Type:	Table boot loads information into the CMEM. Node boot activates the new configuration.

Exception Conditions

The following section describes potential exception conditions, and how they are handled:

- If you specify an incorrect port number (port other than the one on which you made the dial call) when hanging up an ISDN call, the call on the specified port will be cleared (if there is a call on that port).
- If you try to hang up an ISDN call while other calls are active on that port, the call will be cleared unless the network service's gentle clear option is active on that port.
- If a second person requests the same ISDN port to call the same destination, the "OK" prompt is displayed and no further action will be taken.
- If a second person requests the same ISDN port to call a different destination, the "NO CARRIER" prompt is displayed, and no further action will be taken.
- If a second person requests a different ISDN port to dial the same destination as the first active ISDN port, the result will depend on the value of the "Same Destination" parameter configured in the dialer's profile.
- If another person requests the same ISDN port, same destination, and all SVCs on that port are in use, the "OK" prompt will be displayed and the AT Command Interface will not take any further action. It would be up to the network port protocol to detect and correct this situation.
- If you request an invalid port number (not a dial port), the "ERROR" prompt is displayed.

Statistics

Introduction

This section describes the TCP statistics; there are no Telnet statistics.

Status/Statistics

Figure 10 shows the Status/Statistics menu. You can select TCP Statistics from this menu.

```

Node:          Address:          Date:          Time:
Menu: Status/statistics          Path: (Main.5)

Node Stat                      (reserved)
Detailed Port Stat             (reserved)
Network Services Stats         (reserved)
Detailed Link Stat             (reserved)
Flash to Flash Transfer Stat   (reserved)
Detailed Pad Stat              (reserved)
Bridge Statistics              (reserved)
Nest Inventory                 (reserved)
Lan Connection Statistics      (reserved)
Reset Port Stats               (reserved)
Reset All Stats                (reserved)
Software Option Statistics     SNMP Statistics
TFTP Stats
Router Stats
TCP Statistics
(reserved)
(reserved)
(reserved)

#Enter Selection:
    
```

Figure 10. Status/Statistics Menu

Example of TCP Statistics Menu

Figure 11 shows the TCP Statistics menu. You can display statistics or clear the statistics.

```

Node:          Address:          Date:          Time:
Menu: TCP Statistics          Path: (Main.5.15)

1. Display TCP Stats
2. Reset TCP Stats

Enter Selection: 1
    
```

Figure 11. TCP Statistics Menu

TCP Statistics

Figure 12 shows the first of two pages of statistics. It displays TCP-wide statistics or information about the TCP module.

```

Node:                Address:                Date:                Time:
TCP Statistics                               Page: 1 of 4

TCP state                                = Initialized
Number of connections made so far: 1      = 1
Number of packets not for my socket:      = 0
Number of packets with bad checksums:     = 0

tcpRtoAlgorithm      = VANJ
tcpRtoMin             = 200
tcpRtoMax             = 500

Press any key to continue ( ESC to exit ) ...
    
```

Figure 12. TCP Statistics — Screen 1

Description of Terms — First Screen

This table describes the terms found on the first screen.

Screen Term	Tells You...
TCP state	The state of TCP such as Initialized, Stalled, Boot, and so on.
Number of connections	The number of TCP connections established since the last node boot.
Number of packets not for my socket	The number of packets received that did not have a corresponding connection structure at the node.
Number of packets with bad checksums	The number of corrupted packets that arrived at the node.
tcpRtoAlgorithm	The retransmission algorithm being used.
tcpRtoMin	The minimum retransmission time.
tcpRtoMax	The maximum retransmission time.

TCP Statistics

Figure 13 shows the second screen of TCP statistics. It displays information about individual TCP connections.

```

Node:                Address:                Date:                Time:
TCP Statistics                               Page: 2 of 4

tcpConnLocalAddress      = 199.2.103.60
tcpConnLocalPort         = 23
tcpConnRemAddress       = 134.33.204.92
tcpConnRemPort          = 52049
Number of packets sent   = 37
Number of packets rcvd   = 86
Number of bytes sent     = 6332
Number of bytes rcvd    = 42
Number of resent packets = 3
Number of old packets rcvd = 0
    
```

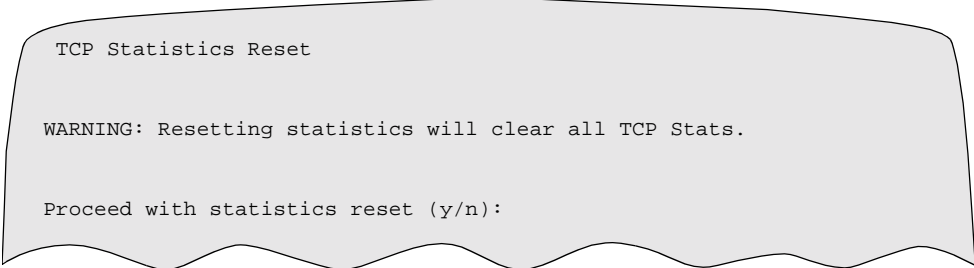
Figure 13. TCP Statistics — Screen 2

Description of Terms — Second Screen

This table describes the terms found on the second screen.

Screen Term	Tells You...
tcpConnLocalAddress	The IP address of the local host.
tcpConnLocalPort	The local port being used for the TCP connection.
tcpConnRemAddress	The IP address of the foreign host.
tcpConnRemPort	The remote port being used for the TCP connection.
Number of packets sent	The number of TCP packets sent over this particular TCP connection.
Number of packets rcvd	The number of TCP packets received over this particular TCP connection.
Number of bytes sent	The number of bytes sent over this particular TCP connection.
Number of bytes rcvd	The number of bytes received over this particular TCP connection.
Number of resent packets	The number of TCP packets retransmitted.
Number of old packets rcvd	The number of old TCP packets received.

Clearing Statistics Resetting the TCP Stats causes the TCP-wide statistics and TCP connection-wide statistics to clear. Figure 14 shows the warning that appears.



```
TCP Statistics Reset

WARNING: Resetting statistics will clear all TCP Stats.

Proceed with statistics reset (y/n):
```

Figure 14. Warning for Resetting TCP Statistics

Server and Client Support

Telnet Support

This section describes the Telnet commands supported by the server and client:

Server

- The server operates in remote-echo and Suppress-go-ahead mode. When the client is connected, the server sends WILL ECHO and WILL SGA to client. If the client negotiates for local-echo or no-suppress-go-ahead, the server aborts the connection.
- The server does not support any subnegotiation. When an SB or SE command is received, the server aborts the Telnet connection.
- In response to an AYT command, the server sends the bell (0x07) character to the client.
- The server does not send the WONT command to the client if a DO command other than ECHO or SGA is received.
- If the server receives the DONT ECHO or DONT SGA commands, the session is aborted. (The server can only operate in “echo” and “suppress go ahead” mode). Any other DONT commands are ignored.
- If the server receives a WILL command, the DONT command is sent back immediately for the same command.
- The server ignores all WONT commands.

Client

- Once the connection is established with the remote server, the client performs these negotiations:
 - DO SGA (suppress Go Ahead)
 - WILL TTY-TYPE (client will send terminal type if server requests)
 - DO ECHO (requesting server to do remote echo)
- The client responds to the TTY-TYPE SEND subnegotiation and aborts the session if any other subnegotiation command is issued.
- If the client receives an AYT command, it sends the Bell (0x07) character to the server.
- The client sends a WONT command to any DO command other than DO SGA and DO TTY-TYPE.
- If the client receives a DONT SGA command, it aborts the connection. It responds to any other DONT command with the WONT command.
- The client sends the DONT command to any WILL command other than WILL SGA and WILL ECHO.
- The client ignores all WONT commands.
- When the server asks for the terminal type, the client sends the terminal type back. You entered this string when prompted for it initially. If you did not enter a tty-name at the prompt, the terminal type will be null in the reply Subnegotiation.
- When you enter ‘^]’ (control-sq.bracket), Telnet goes into user command mode. The prompt **telnet>** is displayed. The supported commands are:

?	close	quit	status	send
---	-------	------	--------	------

A

- Application Examples
 - Frame Relay with Telnet 5
 - Frame Relay without Telnet 4
 - Without Telnet 3
- AT Dial/Telnet 14
 - accessing CTP 14
 - entering ISDN dial information 14
- AT Dialer 14
- AT Dialer Parameters 18
- AT Dialer profile 18

C

- Client
 - Telnet commands supported 27
- Command mode
 - Telnet 12
- Configuration
 - AT Dialer profile 18
 - TCP 6
- Configuration parameters
 - TCP 6
- CTP access
 - using AT dial over Telnet 14

D

- Diagnostics menu 8

I

- ISDN dial
 - using AT dial over Telnet 14

S

- Server
 - Telnet commands supported 27
- Starting Up Telnet 5
- Statistics
 - TCP 23

T

- TCP
 - clearing statistics 26
 - configuration parameters 6
 - definition 1
 - Parameters
 - Entry Number 6
 - Max Receive Buffer Size (bytes) 6
 - Minimum retransmission timer value (ms) 7
 - statistics 23
- Telnet
 - application example 4
 - application example without Telnet 3
 - client implementation 12
 - command mode 12
 - connecting to the CTP through the server 8
 - description 1, 2
 - Frame Relay example 5
 - Frame Relay example without Telnet 4
 - pressing the Return key 13
 - server 3
 - starting a session 8
 - starting up 5
 - steps to access the client 9
 - supported RFCs 2
 - TCP 2
 - Telnet client 3
 - using AT dial 14
 - using other commands 13
- Telnet client 3
- Telnet Command Mode 12
- Telnet commands
 - supported by the client and server 27
- Telnet server 3
- Transmission Control Protocol. See TCP

