Vanguard Managed Solutions

Vanguard Applications Ware
Basic Protocols

Vanguard Basic Configuration Manual

Notice

575 West Street
Mansfield, Massachusetts 02048
(508) 261-4000

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).

Proprietary Material

Part No. T0113, Rev M
Publication Code DS
First Printing: May 1996

Manual is current for Release 6.5 of Vanguard Applications Ware.

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

Contents

Contents (continued)

Chapter 1
Before You Begin...

What You Need to Do Before You Begin

Overview

This chapter describes some prerequisites you need to take care of before learning about configuring and maintaining a Vanguard:

- All the things you need to have before you can use this book.
- Loading software into your Vanguard.
- Everything else you need to know.

What Do I Need Before I Go Any Further?

If you want to use the tutorial in this manual, here is a list of hardware you need before you go any further in this document:

- Two operational Vanguard 320 devices loaded with software
- Two straight-thru cables or cross-over cables
- One DB-9 to DB-25 Control Terminal Port (CTP) cable
- One DB-25 to RJ45 cable
- Two personal computers running Windows 95/NT
- Two Ethernet LAN hubs and cables
- One copy of the Vanguide CD-ROM
- Access to X.25 or Frame Relay service

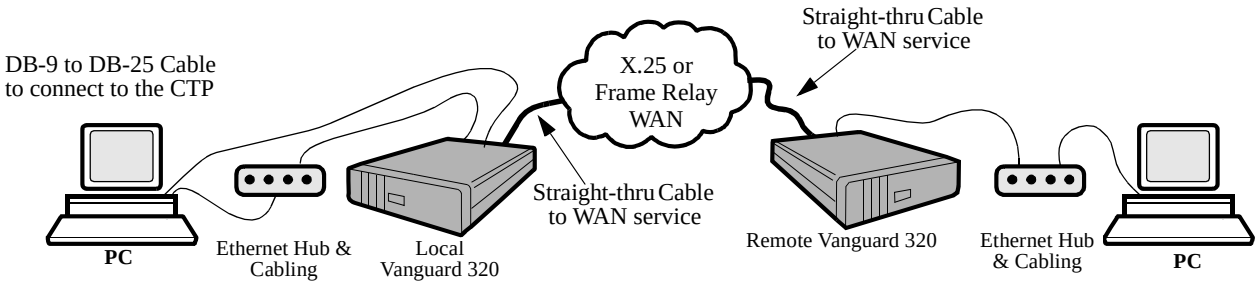
You need these things to perform the configuration tutorial in "Setting Up Vanguard for LAN/WAN Access" section in Chapter 3. You can substitute different Vanguard devices as long as you are comfortable with making some minor configuration adjustments as you follow along with the tutorial.

You can use a cable to connect the two Vanguard devices if you want to test the tutorial application without using your Frame Relay/X.25 service. Use a straight-thru cable for a DTE to DCE point-to-point network. Use a cross-over cable for a DTE to DTE or DCE to DCE point-to-point network.

If you do not use any Ethernet LAN equipment, you are not able to test your LAN connections. If, however, you want to perform all facets of the tutorial, you need gather all this equipment.

Sample Network

Basically, you want to set up a network like the one in Figure 1-1.



Note: You can also substitute a direct connection between the Vanguard nodes if you do not have access to a WAN service. Use a straight-thru cable or a cross-over cable depending on the DIM setting you use. This is covered in Chapter 3.

Figure 1-1. Basic Network Requirements

What About Loading Software?

Your Vanguard device should be loaded with Vanguard products operating software and operational before you try to connect to the Control Terminal Port.

Use your Vanguard Installation Manual to set up your Vanguard hardware.

Make sure that you have the proper software image options in your operating software to do the kind of network functions you want to perform. For the examples in this manual, the default image shipped with your Vanguard works fine. However, if you want to support a particular serial protocol such as SDLC or Bisync 3270, make sure the software option loaded in your unit supports these protocols. If you need to load new operating software, refer to the *Software Installation and Coldloading Manual* (Part Number T0028) for details.

You can use Vanguide Software Builder to develop your own operating software image option for your Vanguard. See the *Vanguide Software Builder Manual* (Part Number T0030) for more details.

Note

The Vanguard should be loaded with software and operational before you try to connect to the CTP port. Each Vanguard ships with default operating software so your unit should become operational shortly after you turn it on. See the *Software Download and Coldloading Manual* (Part Number T0028) for details on loading software if necessary.

Chapter 2
Accessing the Node

Cable the CTP and Bring Up The CTP Menu

Overview

Once you have a Vanguard cabled and powered on, you can connect to the Control Terminal Port (CTP) and view the Configuration Memory (CMEM) installed on the unit. The CMEM is different from the operating software. The CMEM provides the configuration memory that defines how your Vanguard node operates in a network. This chapter shows you how to connect a cable to the CTP on your Vanguard and how to use the Vanguide Terminal Emulator to bring up the CTP menus.

What Is the CTP Port?

The CTP is a port on the back panel of your Vanguard unit that enables access to the menu-driven user interface used to configure, monitor, and troubleshoot your unit. The location of the CTP port and the connection type varies depending on the type of Vanguard you have. On the Vanguard 320 port 4 is used for CTP access (see Figure 2-1). Check your Vanguard Installation Manual for details on the CTP port location and connection type requirements for your unit.

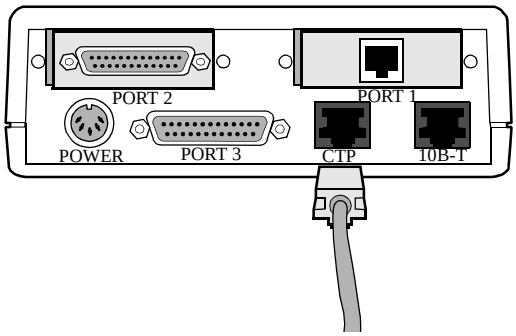


Figure 2-1. Sample Back panel of a Vanguard 320

Generally, the CTP port is defaulted to 9.6 kbps, 8 bits, no parity, 1 stop bit. Again, you can review your Vanguard Installation Manual for more details on default settings. For now, all you need to know is that the CTP provides you with access to the unit's user interface so you can download Applications Ware, configure, monitor, and troubleshoot the unit.

What Do You Need to Connect to the CTP?

You need a PC running Microsoft Windows 95 or Windows NT, running terminal emulation software such as Vanguide Terminal Emulator, or an asynchronous device such as a VT100 to access the CTP menus.

If you have a PC, you can use the Vanguide Application Set from the Vanguide CD-ROM that shipped with your unit to perform most of the operations described in this manual.

But before that, you need the proper cabling to connect your PC or asynchronous device to your local Vanguard, as shown in Figure 2-2.

You need a DB-9 (female) to DB-25 (male) cable to connect your PC to a Vanguard 320. The Vanguard 320 ships with a DB-25 (female) to RJ-45 cable for VT100 access, but if you want to use this cable you need to use the DB-9 to DB-25 adapter to connect the cable to your personal computer's serial port (COM Port). This adapter is not shipped with your Vanguard.

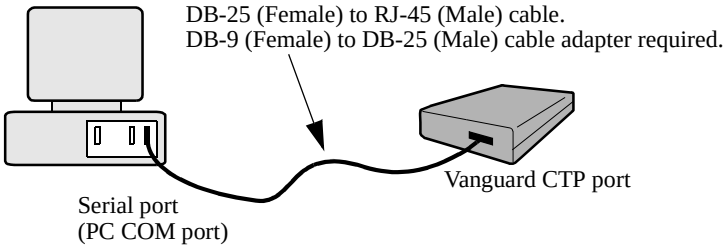


Figure 2-2. Connecting to the CTP of a Vanguard

See your Vanguard Installation Manual for more detailed information on CTP cabling and port connections.

Connecting to the User Interface

Introduction

You have seen how to cable a PC to the CTP on your Vanguard. Now, let us see how to access the CTP menu-driven user interface used to configure and maintain your Vanguard.

Connecting to the CTP

You can make only one PC or Async terminal session to a Vanguard unit's CTP at a time. Before you begin this procedure, make sure that you have loaded the Vanguide Application Set from the Vanguide CD-ROM. Follow these steps to connect from a local or remote personal computer:

Note

This manual uses the Vanguide Terminal Emulator for Windows 95/NT for the following screen examples. A different terminal emulation package or a different version of Windows may cause changes in screen display.

Step	*Action*	*Result/Description*
1	Cable a PC to the CTP port on the back panel of the Vanguard. Also, make sure that your PC's COM Port is enabled in the PC's Setup program. Note the COM Port number that you have connected to.	On a Vanguard 320, the CTP cable connects to Port 4 using the DB-25 to RJ-45 connector cable.
2	Open Vanguide Terminal Emulator by selecting **Start -> Program -> Vanguide -> Vanguide Terminal Emulator** from the Windows Start menu.	The Vanguide Terminal window appears, as shown in Figure 2-3.
3	From the COM Port menu, select **Connect**. Then, press ENTER. **Note** Make sure that you choose the COM Port that you connected to on your PC.	If connected, you should see an asterisk (*) or an OK prompt, as shown in Figure 2-4. This is the default CTP prompt.
4	If you see an asterisk (*****) type **.ctp.** Press ENTER to connect to the CTP. If you see **OK**, type **ATDS0**, then press ENTER.	The Password prompt appears.

Step	Action (continued)	Result/Description
5	Press ENTER.	By default, ENTER is the initial password. Unless someone set a password, the Main menu appears as shown in Figure 2-5. You are now logged on to the CTP and your terminal is acting as a control terminal. If someone set a password on the unit, see Chapter 5, How Do I Set Up Security on My Node? for details.

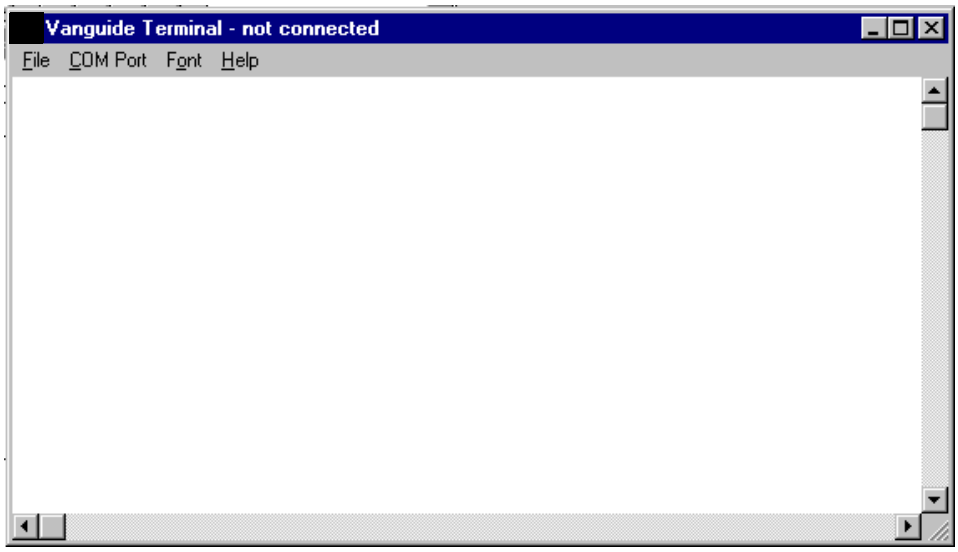


Figure 2-3. Example of Vanguide Terminal Emulator

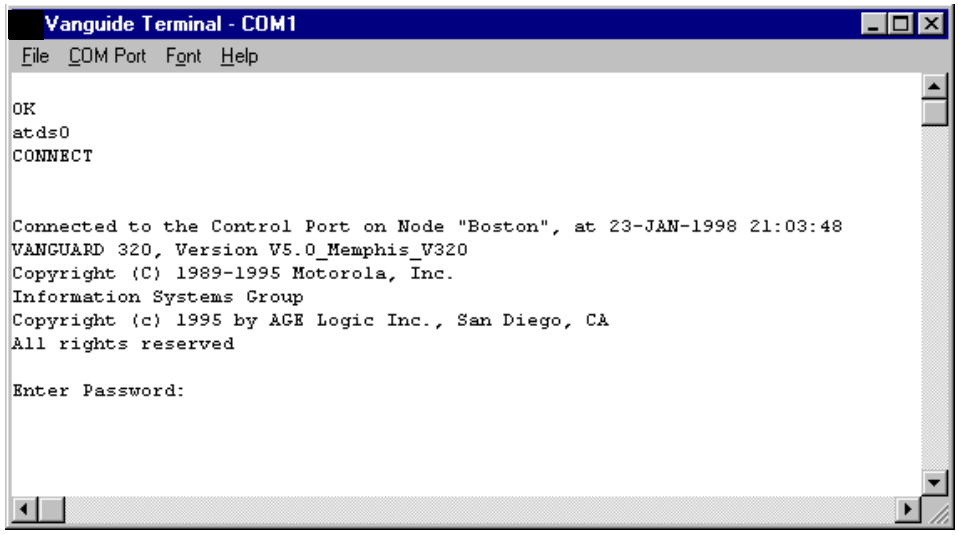


Figure 2-4. Example of CTP Opening Screen

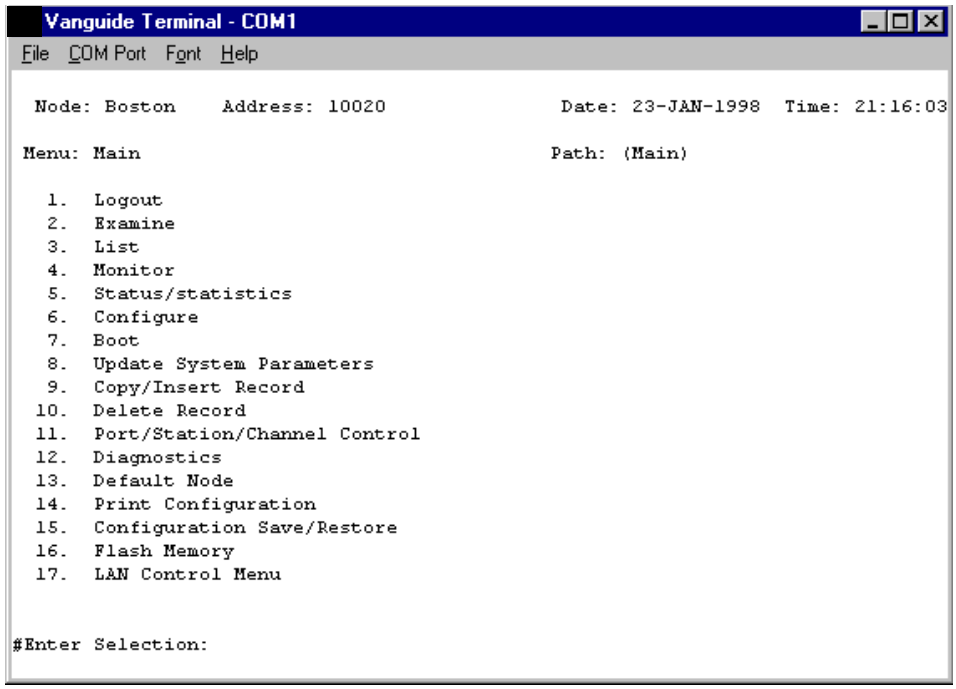


Figure 2-5. Example CTP Main Menu

Logging Off the CTP

From the CTP Main menu, select **Logout**.

The system prompt appears, with either an **OK** or an ***** (asterisk).

Automatic Logout

The Vanguard Applications Ware operating software automatically logs out if you have not entered any data on the control terminal for ten minutes.

You can change the logout time with the Control Port Idle Disconnect Time parameter in the Node record.

Using the Menus and Making Selections

Introduction

As described earlier, you configure the Applications Ware operating software for the Vanguard using a series of hierarchical menus and prompts. The CTP main menu shown in Figure 2-6 is the first menu in the menu hierarchy. The Main menu leads to other menus that contain submenus, configurable parameters, or screen displays. Depending on the options and protocols installed in your unit, some of your menus may appear different.

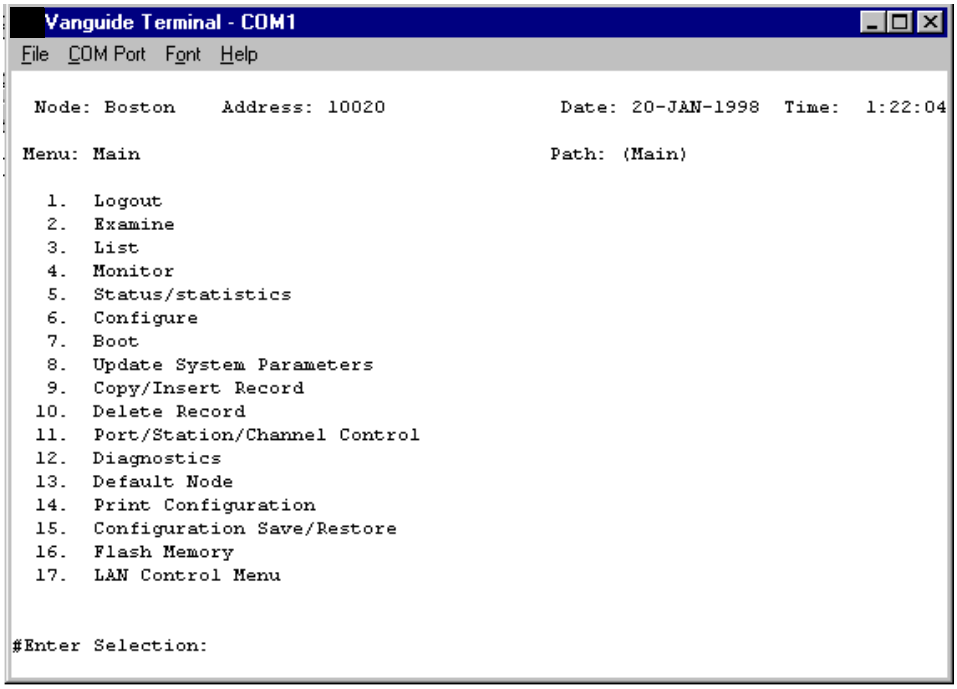


Figure 2-6. The Main Menu

Selecting Menus

Follow these steps to select menus:

Step	Action	Result/Description
1	At the CTP Main menu, type the number of the menu you want to access at the **#Enter Selection:** prompt, **6** for example, and press ENTER.	The Main menu disappears and the selected menu appears.
2	From the next menu, select submenus to perform specific configuration, control, or monitoring tasks.	Selected submenu appears.
3	Press ESC to exit a menu or CTRL + T to return to the Main menu.	This returns you to the previous menu or higher.

Note

You can type in a series of menu option numbers (separated by a period) to jump to an option on a submenu. For example, on most Vanguards typing 6.1 and pressing ENTER displays the Node record for the Configure menu.

Menu Header Elements

Several different elements appear at the head of the menus. Figure 2-7 identifies these elements.

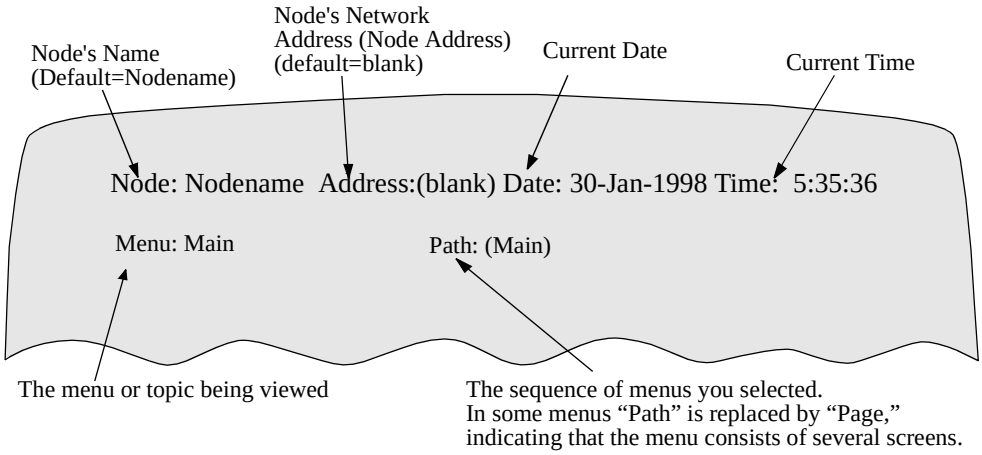


Figure 2-7. Menu Header Elements

Help Screens

If you are uncertain about the possible entries that can be made at a particular point, or if you have a question about the meaning of a prompt, enter any of the following at the system prompt and then press ENTER:

?

H

help

A Help screen appears containing descriptions and explanations. For example, if you press **?** and ENTER at the Main menu, you see the Help screen that appears in Figure 2-8. It displays all the key commands you can enter at the Main menu.

Scrolling

To stop the Help screen from scrolling, press CTRL + S**.** To resume scrolling, press CTRL + Q.

Help Screen for Main Menu

Figure 2-8 shows the help screen for the Main menu. By typing **?** at the **Enter Selection:** prompt and pressing ENTER the screen shown in Figure 2-8 appears. You can use these keystroke combinations to navigate through the Applications Ware software user interface:

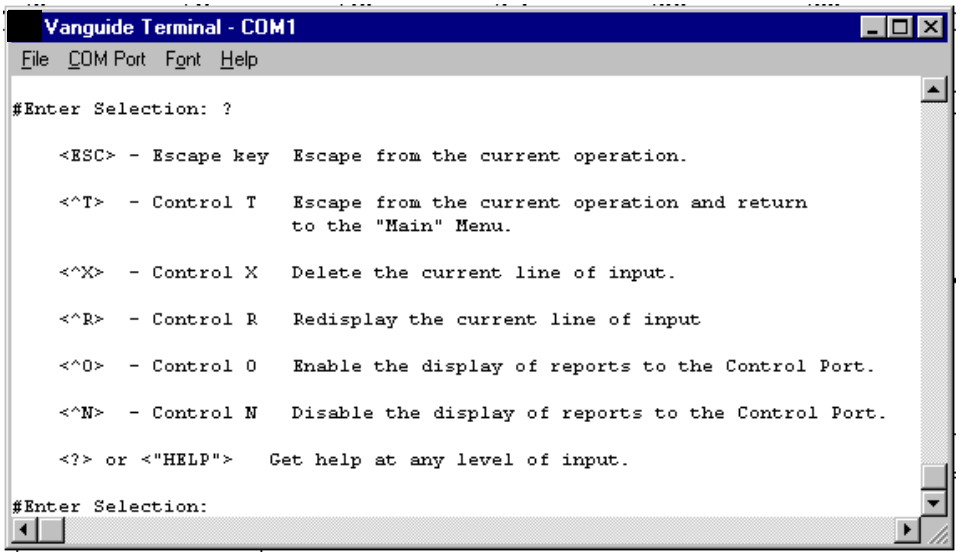


Figure 2-8. Main Menu Help Screen

Note

During initial configuration of a Vanguard node, you should type CTRL + N at the Main menu. This shuts off alarm reporting to the CTP screen.

Chapter 3
It's All Cabled Up, Now What Do You Do With It?

Setting Up Vanguard for LAN/WAN Access

Introduction

This chapter uses a tutorial approach to show you how to set up your Vanguard for basic LAN/WAN operation. It uses a point-to-point application of IP traffic from an Ethernet LAN over X.25 or Frame Relay to show you how to configure your Vanguard for LAN/WAN operation. To do this:

- First, the tutorial explains how to configure the WAN side of your Vanguard device. This lets you make a call from one side of the WAN to the other. It does not matter if you want to pass data over an X.25 or Frame Relay WAN, this tutorial covers both methods.
- Then, the tutorial explains how to configure the LAN side. Setting up the LAN side lets you pass LAN traffic through your Vanguard and out onto the WAN to another remote Vanguard.

What is in the Tutorial?

The tutorial focuses on the records and tables you need to configure to make a basic connection. The tutorial's example emphasizes setting the required parameters for a basic point-to-point LAN/WAN application. This should give you a baseline understanding to work from when you start to configure your own Vanguard network applications. For more information on routing basics and terminology, refer to the *Vanguard Router Basics Manual* (Part Number T0100-01).

How Are we Going to Do This?

On the local node, you connected a PC COM Port to the CTP of the local Vanguard 320. This provides CTP access to both Vanguard 320s from the PC on the local side of this network. Also, connect the PC's Ethernet port through an Ethernet port to the Vanguard 320 Ethernet port.

Once you establish a WAN connection, use the local PC to configure both Vanguard 320s' LAN interfaces, locally and remotely, by calling the CTP address of each Vanguard 320. The PC on the remote side of the network is connected to the remote Vanguard 320 by an Ethernet connection through an Ethernet hub. This provides a LAN on the remote side as well. When you are finished with this tutorial, you should be able to perform Ping operations from one side of the network to the other to test your connectivity.

Note

Ping is a protocol used by TCP/IP to test whether a node or remote device is communicating on a LAN or WAN. A Ping operation tries to receive an echo response from a network device such as a PC or a Vanguard or a gateway identified by an IP address. Ping sends datagrams to the target IP address and displays any responses. Use Ping for locating bad connections or software configuration problems in your CMEM.

Sample Network Configuration

Use the network example in Figure 3-1 as an example of how to configure your Vanguard for LAN/WAN operation. You can choose to follow along with the examples in this tutorial, or you can make modifications according to the requirements of your nodes or network.

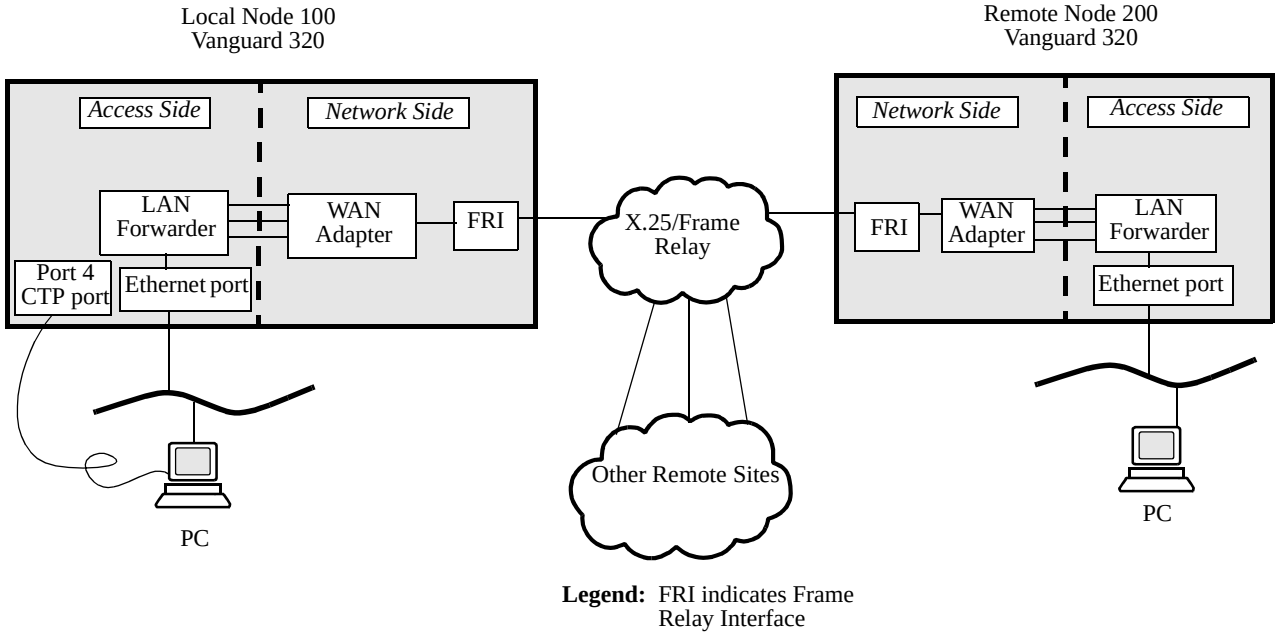


Figure 3-1. Sample Network

How Will We Do This?

This tutorial uses two sets of procedures to show you how to make a LAN/WAN connection between the local and remote nodes shown in Figure 3-1:

1) Configure the local and remote nodes for X.25 or Frame Relay WAN operation. First, configure the local Vanguard. Then, repeat the procedures for the remote Vanguard.

2) Then follow a similar set of procedures to configure the local and remote nodes for LAN operation.

Figure 3-2 maps out the sequence of procedures for the tutorial.

When you are configuring parameters to build a Vanguard CMEM, the default parameter values for the Vanguard node are usually suitable for basic LAN/WAN operation. The tutorial does not take you through the process of configuring every parameter in the CTP menus. It shows you only the critical parameters you need to configure to get the Vanguard up and running using a Switched Virtual Circuit (SVC) call in a point-to-point application.

Note

A SVC is a temporary connection between two end points or nodes in a packet-switched network. You make an SVC connection between nodes when you make a call from one node to the other.

Figure 3-2 shows the sequence of the procedures for the tutorial:

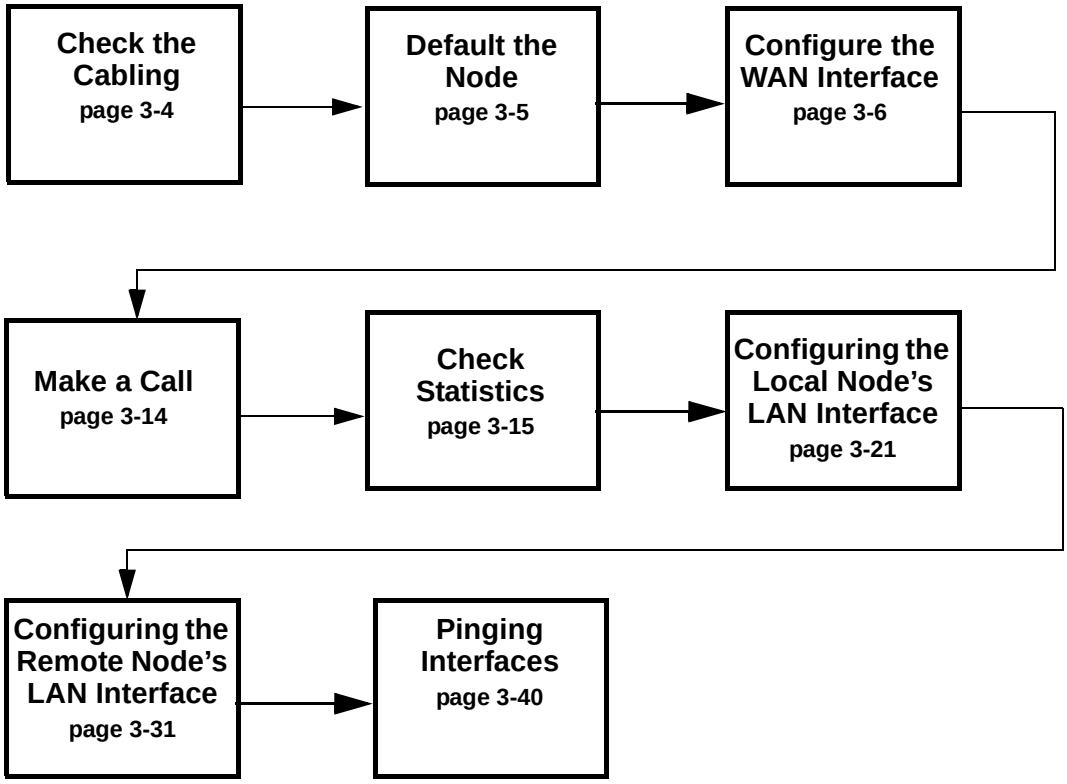
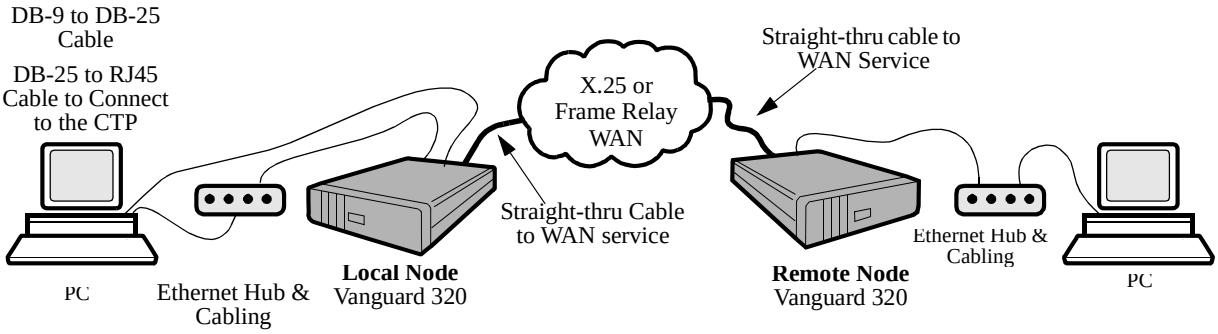


Figure 3-2. Main Procedures for the Tutorial

Check the Cabling

Reviewing the Network Example

This tutorial uses two Vanguard 320s connected by a straight-thru cable to a X.25/Frame Relay service provider. Figure 3-3 shows the network example that appears in Chapter 1 for your reference before you begin setting up the Vanguards for LAN/WAN access. You can also use whichever Vanguard devices you have and modify these procedures for your particular hardware.



Note: You can also use a cross-over cable to connect the Vanguard nodes if you do not have access to a WAN service. Cross-over cables connect DCE to DCE or DTE to DTE interfaces. Whatever cable you use, make sure physical DIM settings are correct for both nodes to make a connection. Typically, carrier devices are set to DCE and Vanguards are set to DTE.

Figure 3-3. Vanguard 320 Network Example

Note

Cross-over cables and straight-thru cables are common networking cables used to connect network access devices to WAN service provider equipment or other networking devices. At first glance, their differences are almost indistinguishable, but they differ subtly. Use a cross-over cable to connect two networking devices if the network ports are set to DTE in one device and DTE in the other or DCE in one and DCE in the other. Use a straight-thru cable if the networks ports are set to DTE in one and DCE in the other.

Default the Node

Procedure

If the Vanguard devices you are using for this tutorial have been previously configured, you can reset the nodes, so they return to their factory-installed default configurations. It is best to start out with a default configuration, so the parameter values you see in your nodes match the default values discussed in this tutorial.

To default a Vanguard:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Default Node**.	The **Proceed (Y/N):** prompt appears.
2	Type **Y** to reset the node.	This erases the configuration memory in your Vanguard node.
3	Go back to the CTP Main menu and select **Boot -> Boot (Warm)**.	This executes a warm boot on your node and implements the default CMEM. This lets you begin this tutorial with a default configuration in your node.

Configure the WAN Interface

Overview

This section shows you how to configure local and remote Vanguard WAN interfaces. Set up the WAN interfaces for the local and remote nodes as shown in Figure 3-3.

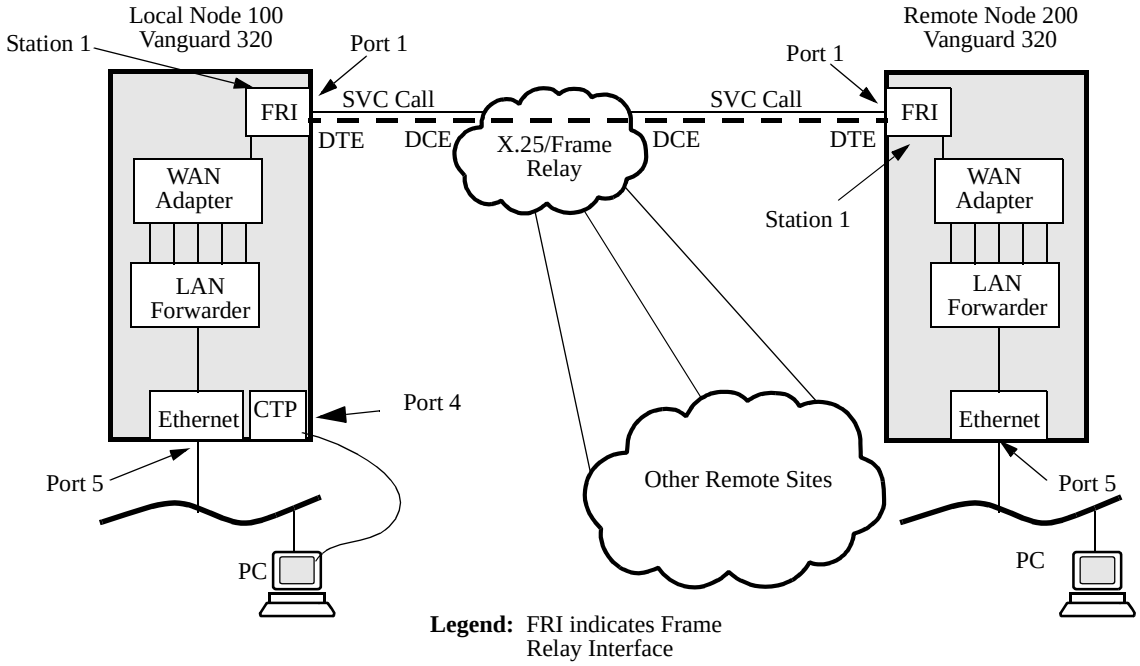


Figure 3-4. Sample of WAN Interface Setup

What You Have To Do

Follow these steps to make a WAN connection between the local and remote nodes. See the following sections for detailed discussions on these steps.

Step	Follow These Steps	Description
1	Configure the Node record.	This gives your node a name and an address. Do this for the local and remote node.
2	Configure a Port record.	This tells the node which WAN protocol (X.25 or Frame Relay) you want to use to pass traffic across the WAN. If you are setting up for X.25 operation, you only have to set up the port record. If you are using Frame Relay, you must configure a Frame Relay Station record, too. You do this later. Do this for the local and remote node.
3	Configure Network Services.	This means you need to configure a Route Selection Table. This tells the node which port to use to pass data traffic, and it gives your node an address to route traffic to across the WAN. Do this in the local and remote node.
4	Boot the node.	This implements the changes you made to the node's configuration memory. Do this in the local and remote node.

Note

When one node makes a call to another node, the node receiving the call sometimes needs a Route Selection Table entry set up to route the call to its LAN Forwarder. This is the case in FRA, SDLC, or LAN connection applications. If the receiving node is connected to a PAD port, no entry is required in the routing table because the remote node knows it has a direct connection.

Begin by configuring the local node first. Then, configure the remote node by repeating the same set of procedures.

Configure the Node Record

Procedure

First, configure the Node record for your local or remote Vanguard.

Use the CTP to access the Node record and enter values for the required parameters. See Chapter 2, Accessing the Node, for details on making a CTP connection to a Vanguard node.

Configuring The Node Record

For a basic point-to-point connection, you do not have to configure much. Fill out the node name and the node address and you have completed the tasks necessary to configure a node record for this example. See Appendix A, Configuring a Node, for a detailed description of the Node record and its parameters.

To configure the Node record:

Step	*Action*	*Result/Description*
1	From the CTP, select **Configure -> Node**.	The Node record appears.
2	In the Node Name parameter: • For the local node, type **Local**. • For the remote node, type **Remote.**	In a typical application, this can be any name you want as long as you do not exceed the limit of eight alphanumeric characters. You should always follow any naming convention established for your network, if there is a naming convention. If you do not have one, you should establish one.
3	In the Node Address parameter: • For the local node, type **100**. • For the remote node, type **200**.	This can be any number up to a 13-digit limit. Again, you should follow the addressing scheme set up for your network. **Note** Configuring a value in the Node Address parameter of the Node record is required for LAN and Voice applications. This value lets the node keep track of hop counts to neighboring nodes. Voice links require a node address configured in the Node record.
4	You can use the default values for the rest of the parameters. Type a semicolon (**;**) after the last value and press ENTER.	This saves the record.

Configure a Port Record

Procedure

The next thing you need to do is configure your WAN port on the Vanguard. Usually you configure Port 1 as the WAN port because it is the high speed port.

For this example you just need to make a point-to-point WAN connection. In other applications, you may need to configure additional WAN ports as backups depending on how many ports your device has and your network requirements.

Configuring a X.25 or Frame Relay Port

Or you may want to configure additional WAN ports because you are routing more than one circuit through your device, such as in the case of a Vanguard 6520 or a Vanguard 6560. It does not matter how many WAN connections you want to set up because you configure one WAN port the same as any other. The only difference is whether you are running X.25 or Frame Relay. This example covers both X.25 and Frame Relay.

To configure a X.25 or a Frame Relay port:

Step	*Action*	*Result/Description*
1	From the Control Terminal Port Main menu, select **Configure -> Port**.	The Port record appears.
2	In the Port Number parameter, type **1** (if it is not already displayed), then press ENTER.	This defines Port 1 as the WAN access port. Usually you use Port 1 for your WAN access because it is the high speed port on a Vanguard.
3	In the Port Type parameter: • For an X.25 connection, type **X25**, then press ENTER. • For a Frame Relay connection, type **FRI**.	**Note** You must also configure a station record for Frame Relay. You do that later in this example
4	In the Connection Type parameter, type **SIMP**.	This means no control signals are required
5	In the Clock Source parameter, type **EXT** for both the local and remote Vanguard 320 nodes.	You are using the clock from your WAN service provider's node. **Note** If you are making a direct connection between the Vanguard 320s using a straight-thru cable, you need to set one Vanguard 320 to INT and the other to EXT, so one node is providing the clocking and the other one is receiving it.

Step	Action (continued)	Result/Description
6	In the Link Address parameter: • For the local node, type **DCE**, then press ENTER. • For the remote node, type **DTE**, then press ENTER.	This appears in the port record for X.25 only. For Frame Relay, you must configure the Link Address in the FRI station record. This is an important parameter because it provides a logical connection between your node and the remote node. **Note** It is important to remember to set the link address of your Vanguard node to the opposite value of the node you are connecting to. For instance, if you are making a direct connection (as in a bench test) between two Vanguard nodes, you would set one node to DTE and the other to DCE, and use a straight-thru cable to connect them. The Link Address parameter in the X.25 port record or the Frame Relay Station record lets you set up a logical connection for control signals between your node and the remote node. Control Signals establish and maintain an electrical connection between networking devices. Networking devices like Vanguard are either Data Communications Equipment (DCE) or Data Terminal Equipment (DTE). If you are making a direct connection, use a cross-over cable to connect the two Vanguards using the DTE DIM settings in both nodes, or use a straight-thru cable and set one node to DTE and the other node to DCE.
7	Use default values for the rest of the parameters. Type a semicolon (;) after the last value, then press ENTER.	This saves the record.

Configure Frame Relay Station Record

Procedure

If you are configuring a node for Frame Relay operation, you must configure a station record after you configure the port record. The Station Record sets up the logical connection between the nodes.

Configuring Frame Relay Station Record

To configure a station record:

Step	Action	Result/Description
1	From the Control Terminal Port Main menu, select **Configure -> FRI Stations.**	The Frame Relay Interface Station record appears.
2	In the Port Number parameter, type **1** (if it is not already displayed), then press ENTER.	This is the Frame Relay port associated with the Frame Relay station.
3	In the Station Number parameter, type **1** (if it is not already displayed), then press ENTER.	
4	In the Station Type parameter, type **Annex-G** (if it is not already displayed), then press ENTER.	The default is **Annex-G**. This should work for most operations.
5	In the DLCI parameter, type **16**. If you are using a cable for a direct connection between the two nodes, type any value but **0** (zero).	This is the Data Link Connection Identifier (DLCI). It is critical for establishing a connection across the WAN. The DLCI defines the number that identifies the logical connection multiplexed into the channel provided by your Frame Relay services carrier. For Vanguard, you can use the DLCI Autolearn feature instead of typing in DLCIs for all your nodes. DLCI Autolearn automatically learns the assigned DLCI for a node when the node comes online and a WAN connection is made as long as your Frame Relay network is functioning properly. See the *Frame Relay Interface/Access Manual* (Part Number T0106-02) for more details on this.
6	Use the default values for the rest of the parameters. Type a semicolon (;) after the last value, then press ENTER.	This saves the record.

Configure Network Services

Overview

Next you must set up network services for the WAN connection. Network Services handles how traffic is routed out of your Vanguard to the WAN.

You need to configure a Route Selection Table to set up the node address of the remote node you are connecting to and the destination port in the local node. The destination is a little confusing because you might assume that it refers to the remote node. However, the destination is the WAN port in the node you are configuring at the moment. The destination tells your Vanguard network services which port to use to pass traffic through to the WAN and what type of WAN carrier service is in use (Frame Relay or X.25), as shown in Figure 3-5.

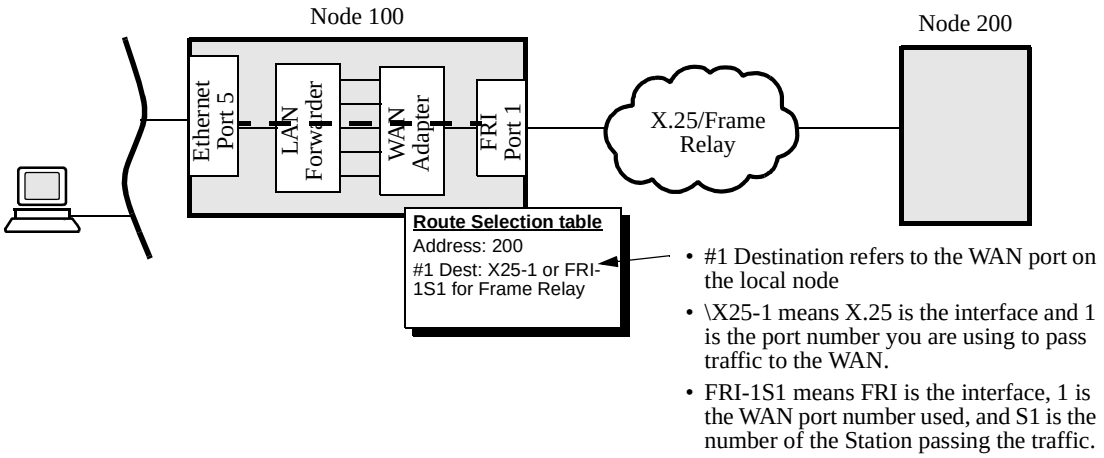


Figure 3-5. Example of Node Address and Destination in Network Services

Procedure

To configure the Network Services:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Network Services -> Route Selection Table**.	The Route Selection Table appears.
2	In the Entry Number parameter, type **1** (if it is not already displayed).	This defines this record as entry 1.
3	In the Address parameter, type **200**, then press ENTER. When you configure the remote node, type **100** here to connect to the local node 100.	This identifies the address of the remote node you want to connect to across the WAN.

Step	Action (continued)	Result/Description
4	In the #1 Destination parameter: • For Frame Relay, type **FRI-1S1**. • For an X.25 connection, type **X25-1**.	This tells your node that you want to use port 1, station 1 for a Frame Relay WAN or port 1 over an X.25 WAN to pass data from this Vanguard to the remote node.
5	Type a semicolon (**;**) after the last value, then press ENTER.	This saves the record.

Boot the Node

Procedure

Now, you should boot the node to implement your changes. Booting the node implements the changes you made to the node's CMEM.

To boot the node:

Step	Action
1	From the CTP Main menu, select **Boot -> Node (warm)**.
2	Type **Y** at the prompt. The node resets itself. Check your Vanguard Installation Manual for start-up diagnostics if you have any problems.

Make a Call

Procedure

Once the node resets itself, you have a WAN connection. To make sure that you have WAN access, you should call the other node's CTP.

To make a call you must know:

- the node address (set when you configured the Node Record).
- the WAN adapter address (always 98 for a Vanguard).

To make a call:

Step	*Action*	
1	From the CTP main menu, select **Logout**.	The asterisk (*****) prompt or the **OK** prompt appears on the CTP.
2	If the asterisk (*****) prompt appears on the CTP: • If you are calling the remote node, type **Call 20098**. • If you are calling the local node, type **10098**. If the **OK** prompt appears on the CTP: • If you are calling the remote node, type **ATD20098**. • If you are calling the local node, type **ATD10098**.	The called node's CTP screen appears.

If there is a problem, see the "Potential Problems" section on page 3-16 for details on how to troubleshoot your connection. Remember, you can make only one connection to a CTP port at a time.

Check Statistics

Procedure

Once you have both nodes configured, you can also check the Statistics screens to make sure everything is running correctly.

To make sure you have a WAN connection:

Step	*Action*	
1	From the Control Terminal Port Main menu, select **Statistics -> Detailed Links Stat**.	The detailed Links Statistics screen appears.
2	Check the link state for port 1 on the first page of the screen.	The Link State should read **up** for a Frame Relay connection, as shown in Figure 3-6. (If you configured an X.25 connection at port 1, that should read **up** as well.) If you configured a Frame Relay connection you should also see that the FRI Station is **up** as well.
3	If your link is not up, refer to "Potential Problems" section on page 3-16 for details on troubleshooting.	

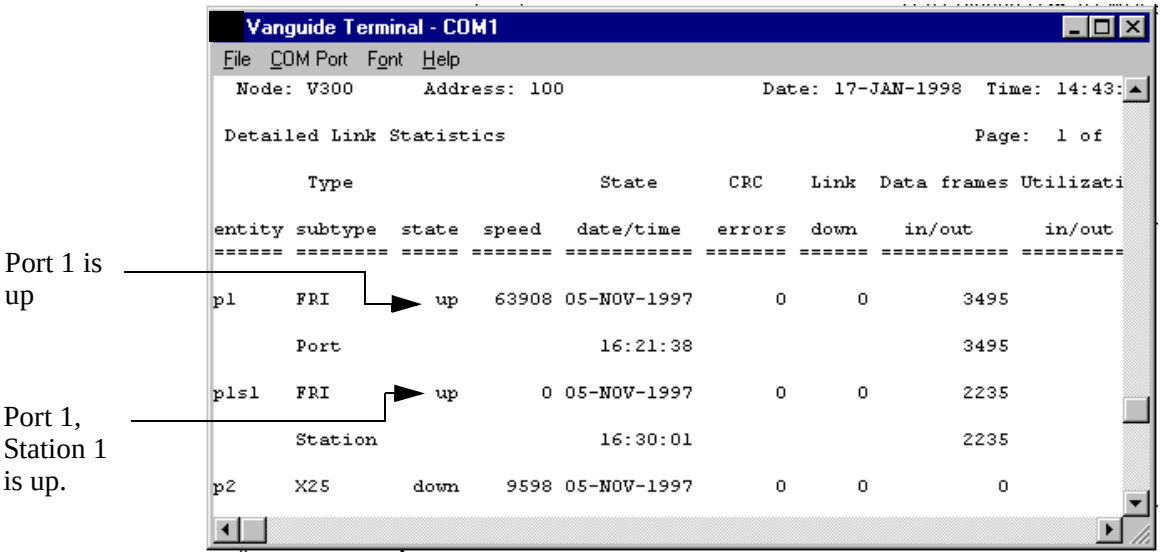


Figure 3-6. Detailed Link State Statistics

Potential Problems

Troubleshooting The WAN Connections

If you were unable to make a call between the nodes, here is a list of potential problems you can troubleshoot:

- Cabling – make sure the cables are connected to the correct ports as configured in CMEM. In other words, make sure you connected your WAN cable to port 1 on the Vanguard 320, so your Port 1 configuration in CMEM is valid.
- FRI station statistics – Check the FRI station statistics for FRI link setup status. If the status is Link Setup it probably means the Link Address is incorrectly configured. Refer to the "Problem with a Frame Relay Port" section on page 8-5 for Frame Relay configuration or the "Problem with an X.25 Port" section on page 8-10 for X.25 configuration.
- Link Addresses – make sure the link addresses in the Vanguard 320 nodes are correct. They should be DTE if you are connecting to a WAN service. If you are making a direct connection (as in a bench test), they should be DTE-DCE with a straight-thru cable or DTE-DTE or DCE-DCE using a cross-over cable. You can examine the Port record for the link address in an X.25 WAN configuration or you can check the Station record for a Frame Relay WAN connection. Also check the alarms log. If you see the alarm, BAD FRAME, this probably means your link addresses are incorrect. See "How to Display Event Log" section on page 8-2.
- DIM Location – The DIM may be physically located in a DTE or DCE position. Check Node statistics to verify the physical location of the DIM. If there is a problem with physical DIM setting, check your Vanguard Installation Manual for details on how to change the DIM setting.
- Route Selection Table – Verify that the called addresses and destinations in the Route Selection tables are configured correctly. You may be calling the wrong node or misconfigured the WAN port in your destination.
- Bad Port – If the port you are currently using does not seem to work, try a different port. You could have a hardware problem. If you have more than two nodes available, try configuring a different node for WAN operation.
- Port Status – Check the Detailed Port Statistics on the X.25 port to make sure a call is going out of the node. Check Last Outbound Call parameter. The port must be in an Up state for a call to go out.

For more details see the Chapter 7, Making Sure Everything Is Running Correctly.

Configuring the LAN Interface

Overview

This section describes how to configure the LAN interface on your Vanguard device. Now that you have configured the WAN interfaces for the local and remote nodes, you can set up your LAN interfaces.

This manual cannot cover every possible scenario, so it shows you how to run IP traffic from an Ethernet LAN into your LAN port. This is a common application, and it gives you a basic idea of how Vanguard handles LAN traffic.

If you want to learn how to configure your LAN interface for Token Ring traffic or one of the many serial protocols supported by the Vanguard family, refer to the appropriate option guide for details. See the "Documentation Map" section on page -xii for a complete list of Vanguard user documentation.

What Will We Cover?

First, configure the LAN interface for local node 100. Then, because the configuration procedure for the remote node is slightly different, set up the LAN side for node 200.

Once again, use the example of configuring local and remote Vanguard nodes for LAN/WAN operation. Using the nodes from the previous example, nodes 100 and 200, it explains how to enable the LAN interfaces for LAN/WAN operation, as shown in Figure 3-7.

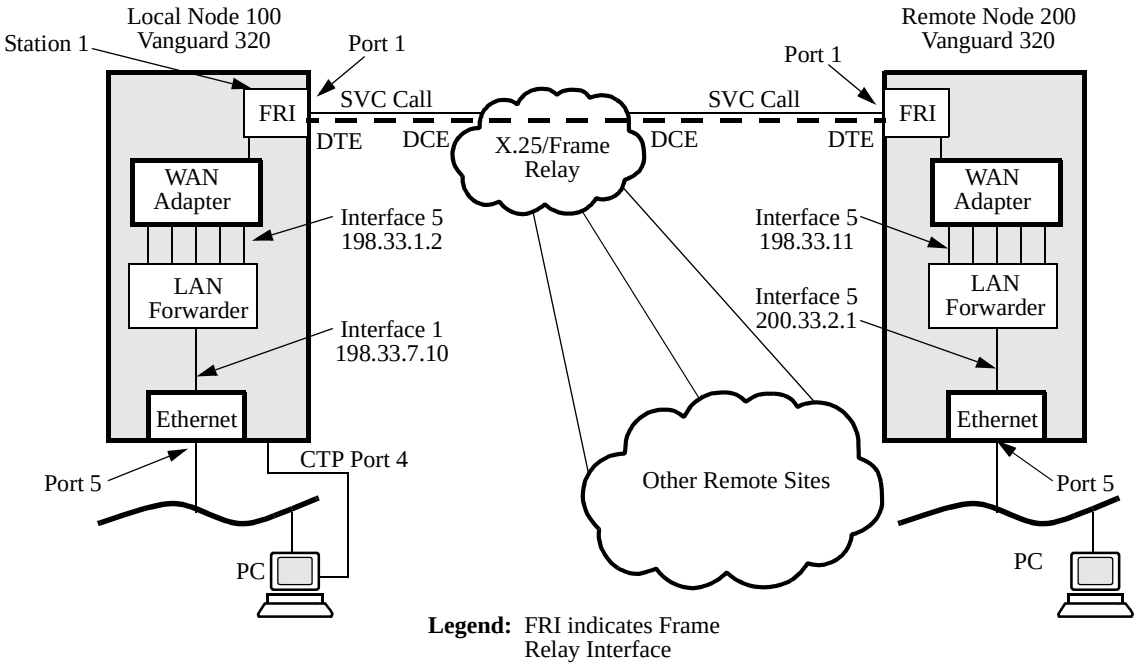


Figure 3-7. Sample of the LAN Interface Setup

A Few Words About Configuring the LAN Interface

Overview

Because the Vanguard architecture is based on X.25 packet switching technology, setting up your LAN interface is not as simple as configuring a LAN port and passing traffic out of the WAN side of your node.

You have to set up X.25 SVC calls within the node and define how the LAN interface and the WAN interface pass traffic internally. This means you must configure a few tables and records to control how LAN traffic is passed from the LAN port to WAN interface before it travels out to the X.25 or Frame Relay network.

Now, the LAN Forwarder and the WAN Adapter components of the Vanguard architecture come into play. They guide data traffic through the node from LAN to WAN. As shown in Figure 3-8, these components handle the routing of traffic inside Vanguard devices. Without properly configuring these components the LAN interface cannot pass data to the WAN port in a Vanguard device.

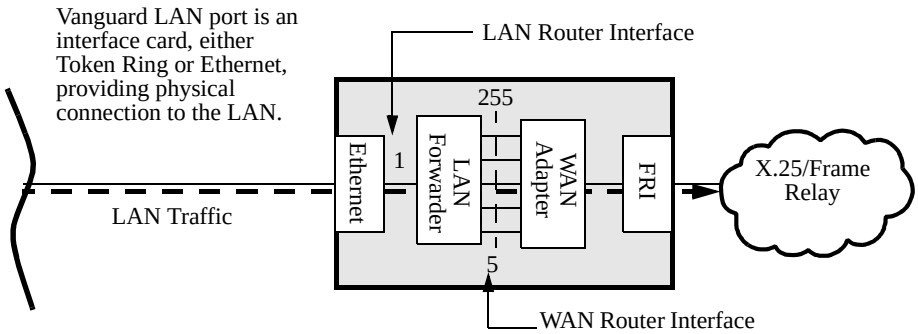


Figure 3-8. Example LAN Forwarder and WAN Adapter

LAN Forwarder

The LAN Forwarder makes forwarding decisions for both bridged and routed data traffic. In other words, the LAN Forwarder makes the decision to bridge or route LAN data traffic to the WAN within the Vanguard node. As shown in Figure 3-8, there is one virtual connection between the Forwarder and the physical LAN port. Starting with interface 5, because the LAN interface uses interfaces 1 through 4, you can configure up to 250 virtual connections between the LAN Forwarder and the WAN adapter. You can configure each of these virtual connections to pass bridged, routed, or brout (bridged/routed) traffic from the local LAN to the WAN.

WAN Adapter

The WAN Adapter is a software module that connects the LAN Forwarder to the WAN ports on the local Vanguard and the remote node. When it is making a call to another node, the WAN Adapter is responsible for establishing a SVC or PVC connection between the local and remote node. To do so, the WAN Adapter provides the following functionality:

- Performs WAN encapsulation.
- Establishes remote connections using autocall SVCs and or PVCs configured in the PVC setup table.
- Controls data traffic flow using traffic priority and the “on demand” option.
- Makes connections across the WAN using Frame Relay, X.25, ISDN, or Sync PPP.

When it receives a call from another node, the WAN Adapter provides the node subaddress for the remote node to connect to in order to reach the LAN interface for the remote node. The node subaddress for a Vanguard is always 94.

What You Have to Do

List of Records To Configure

The following table lists the parameter records you need to configure to set up the LAN interface for the local node shown in Figure 3-7:

Records	*Description*
Port Record	This record tells the node the type of LAN protocol (Ethernet, Token Ring) that is to pass traffic through the LAN port. You need to do this in both the local and remote node.
LAN Connection Parameters	This table lets you set up the number of LAN connections you need.
LAN Connection Table	This table lets you create the entries that setup connections between the LAN interface and the WAN interface in the node.
Mnemonic Table	This table provides a short-form name to make a call to the other node. You only have to configure the Mnemonic table in the node making the call.
Configure Router Interfaces	This record enables router interfaces for the LAN/WAN interfaces.
IP Parameters record	This record allows you set up the maximum number of IP interfaces.
IP Interfaces record	This record allows you to assign IP addresses to your LAN/WAN interfaces.
Route Selection Table ■ **Note** Configure this table for the remote node only as it is for the node receiving the call.	This table lets the remote node receive a mnemonic call from the local node. You only have to set this up in the node receiving the call.
Boot record	This record boots the node and implements the changes you made.

The following sections show you how to configure these records in detail.

Configuring the Local Node's LAN Interface

Overview

When you set up a node's LAN interface, you have to configure the records and tables that allow LAN traffic to pass from the LAN port to the WAN port. The LAN traffic then passes over the WAN to the remote node. The following sections describe how to configure the records and tables for the local node's LAN interface.

Configuring the Port Record

Procedure

Recall that ports 1 through 4 are typically used for the WAN interfaces on Vanguard devices. Likewise, ports 5 and up to the maximum number of ports supported on your node are used for LAN ports or serial interfaces. On the Vanguard 320, port 5 is the LAN port, and you are about to configure it as an Ethernet port for this example.

To configure the Port record for the local node.

Step	Action	Results/Description
1	From the CTP Main menu, select **Configure -> Port**.	The Port record appears.
2	In the Port Number parameter, type **5**, then press ENTER to identify the physical location of the LAN port for node 100. **Note** For most Vanguards, you can determine the port number for the LAN port by looking at the back panel. However, if you are configuring a Vanguard 6520 or a Vanguard 6560, you can determine the port number for a LAN card in the device by multiplying the slot number the card is installed in by 6 and adding 1. For example, a LAN card installed in slot 2 is port 13. You can also determine the LAN port number by checking statistics for the nest configuration in your device. From the CTP Main menu select **Statistics -> Nest Inventory** for a list of configured cards and options.	Port Number represents the physical port on the back panel of the device. It is also the reference number of the port record.
3	In the Port Type parameter, type **ETH**, then press ENTER.	This identifies the port type for the LAN port. In this case, it is an Ethernet LAN.
4	You can use the default values for the rest of the parameters at this time. Type a semicolon (;) after the last value, then press ENTER.	This saves the record.

Configure the LAN Connection

Procedure

Next, you need to configure the LAN Connection. The LAN Connection is made up of two records:

- LAN Connection Parameters
- LAN Connection Table

Configuring LAN Connection Parameters

The LAN Connection Parameters record lets you configure up to 250 LAN connections. The default is 32. Other applications may require more or less LAN connections. However, for this example, you need to configure only one LAN connection. Because the default values for the LAN Connection Table are sufficient for this example, you must access the table and save it. If you do not save it, the connections are not made because you have not saved your changes to CMEM.

To configure the LAN Connection for this example:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Configure LAN Connection -> LAN Connection Parameters**.	The LAN Connection Parameters record appears.
2	In the Maximum Number of LAN Connections parameter, type **32**, if does not already appear.	This identifies the maximum number of LAN connections you want to configure for your node. For this example, you need only one LAN connection, so the default value of 32 works for this example.
3	Type a semicolon (**;**), then press ENTER.	

Configuring the LAN Connection Table Record

After you define the number of maximum LAN connections you want, you need to set up the actual LAN connections. This means you need to connect LAN connection entries to actual interfaces inside the Vanguard so the node knows where to route traffic internally to the WAN Adapter.

To configure the LAN Connection Table Record:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Configure LAN Connections -> LAN Connection Table**.	The LAN Connection Table appears.
2	In the Entry Number parameter, Type **1** (if it is not already displayed), then press ENTER.	This is the entry number used to reference this record. This entry is mapped to a particular LAN interface.
3	In the Interface # parameter, type **5**, then press ENTER.	This means the LAN Forwarder uses interface #5 to send LAN traffic to the WAN Adapter.
4	In the LAN Forwarder Type parameter, type **ROUT** (if it is not already displayed).	This tells the LAN Forwarder how to pass traffic to the WAN Adapter. Since you are routing traffic, use the default value ROUT for this example.
5	In the Autocall Mnemonic parameter, type **200LAN**, then press ENTER. Do not put any value in this parameter for the remote node.	This sets up a SVC call between the LAN interface in the local node and the WAN interface in the remote node. You have to set up a SVC call in one of the nodes, local or remote. For this example, set up the local node to do the calling. This means you need to configure an autocall name here.
6	In the Maximum Number of Autocall Attempts parameter, set this parameter to zero (**0**) because you want the local node to continuously make SVC calls to give the link enough time to come up.	When you set this parameter to zero, it overrides the Maximum Number of Autocall Attempts parameter. Once you know your configuration works, you can set this back to another value.

Step	***Action*** *(continued)*	***Result/Description***
7	In the Remote Connection ID parameter, type **1** (if it is not already displayed).	This specifies where the LAN Connection SVC call in the local node connects to the WAN Adapter in the remote node. It points to an entry number configured in the LAN Connection table of the remote node containing the router interface number for the remote node's WAN Adapter. In other words, use this to connect your LCON entry in the local node to the WAN adapter interface in the remote node.
8	Everything else in the record can be set to the default values, so type a semicolon (;) after the last value, then press ENTER.	This saves the record.

Note

The rule for setting a value in the Maximum Number of Autocall Attempts parameter is that you should determine how long it takes your network to come up and become operational, and then set the parameters accordingly.

Configure the Mnemonic Table

Procedure

Since you configured a Mnemonic name in the LAN Connection Table for the local node, you must fill out a Mnemonic Table. The Mnemonic Table lets you configure short-form names and destinations used by the Vanguard to make calls to another node. You can configure up to 64 Mnemonic names, but for this example, you need only one Mnemonic name.

To fill out the Mnemonic Table:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Configure Network Services -> Mnemonic Table**.	The Mnemonic Table appears.
2	In the Entry Number parameter, type **1** (if it is not displayed already).	This identifies the Mnemonic Table entry. The default value is 1.
3	In the Mnemonic Name parameter, type **200LAN**.	This defines the alphanumeric name used for calling or autocalling. The Mnemonic name can be up to eight alphanumeric characters. It must be the same Mnemonic used in the LAN Connection Table.
4	In the Call Parameters parameter, type **20094** to call node 200 and connect to the WAN Adapter.	The default address for a Vanguard WAN adapter is always 94. This defines the call string including the node address and the subaddress of the node you are calling. These values are the network address of the remote node and the subaddress of the node's WAN Adapter.You are defining the LAN Connection of one node to the WAN Adapter of a remote node.
5	Everything else in the record can be set to the default values, so type a semicolon (**;**) after the last value, then press ENTER.	This saves the record.

Enable the Router Interface

Procedure

Before you can make a call to the remote node, you need to enable the interfaces for interface 1 and interface 5.

To configure the router interface:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Configure Router -> Configure Interface States**.	The Configure Interface States record appears.
2	In the Interface #1 State parameter, type **Enable**, then press ENTER.	This enables interface 1, the LAN interface.
3	In the Interface #5 State parameter, type **Enable**, then press ENTER.	This enables interface 5, the WAN interface.
4	Everything else in the record can be set to the default values, so type a semicolon (;) after the last value, then press ENTER.	This saves the record.

Configure IP

Procedure

Next, you need to configure IP parameters and IP interfaces. This is where you set the maximum number of IP interfaces for your node. You can have up to 36 interfaces, but since you need only two IP interfaces for this node, use the default value of 36 for this example. After that, you assign IP addresses to your interfaces in the Interfaces record.

Configuring IP Parameters

Although you do not need to change anything in the IP parameters record for this example, you must access the record and save it. Your changes are not in CMEM until they are saved.

To access and save the IP Parameters record:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Configure Router -> Configure IP -> Parameters**.	The Configure Interface States record appears.
2	In the Maximum Number of IP Interfaces parameter, type **36** (if it is not already displayed), then a semicolon (;), then press ENTER.	This sets the maximum number of IP interfaces, and it saves the record.

Configuring IP Interfaces

Now you need to configure the IP interfaces. Here, you assign an entry number to each one of your router interfaces in the local node and you assign IP addresses to the interfaces. You can ping these interfaces later to make sure you configured them properly.

You are going to configure two IP Interface entries: one for interface number 1 which is your LAN port, and one for interface number 5 which is your WAN port.

To configure the IP interfaces for the local node:

Step	Action	Result/Description
1	From the CTP Main menu, select **Configure->Configure Router-> Configure IP->Interface**.	The Configure IP Interfaces record appears.
2	In the Interface Number parameter, type **1** (if it is not displayed already), then press ENTER.	This is for the LAN port.
3	In the Interface Number parameter, type **1** (if it is not displayed already), then press ENTER.	
4	In the IP Address parameter, type **198.33.7.10** for this LAN port.	**Note** You should use the IP address assigned by your network administrator.
5	Type a semicolon (**;**) after the last value.	This saves the record, and entry Number 2 appears.
6	In the Entry Number parameter, type **2** (if it is not displayed already), then press ENTER.	This is for the WAN interface.
7	In the Interface Number parameter, type **5** and press ENTER.	You can use interface number 5 up to the maximum for virtual circuits over the WAN to other routers.
8	In the IP Address parameter, type **199.33.1.2** for the WAN interface for the local node.	**Note** You should check with your network administrator to determine a valid IP address to connect your WAN service provider.
9	Type a semicolon (**;**) after the last value and press ENTER.	This saves the record.

Boot the Node

Procedure

Now you should boot the node to implement your changes.

To boot the node:

Step	*Action*
1	From the CTP Main menu, select **Boot -> Node (warm)**.
2	Type **Y** at the prompt. The node resets itself. Check your Vanguard Installation Manual for start-up diagnostics if you have any problems.

Configuring the Remote Node's LAN Interface

Overview

Now that you have configured the LAN interface for the local node, you need to configure the LAN interface for the remote node.

The remote node is configured the same way you configured the local node, except that you do not have to configure a Mnemonic table because the local node is making the call. But you have to configure a Route Selection Table to receive the call.

The following sections show you how to configure the remote Vanguard 320's LAN interface.

Connect Remotely

As long as the WAN connection is up and running, you can configure the remote node by making a call to the node's CTP just as you did earlier to check your WAN connection.

You can do this because you have already set up the WAN interfaces for the nodes, and you have either an X.25 connection or a Frame Relay WAN connection running between the nodes.

To make a call you must know:

- the node address (set when you configured the Node Record)
- the WAN adapter address (always 98 for a Vanguard)

To connect to remote node 200's CTP:

Step	*Action*
1	From node 100's CTP Main menu, select **Logout**.
2	At the asterisk (*****) prompt, type **Call 20098**. Or: At the **OK** prompt, type **ATD20098**.
3	This should place a call to node 200. You should see node 200's CTP screen appear.

If you cannot connect to node 200's CTP remotely, check your WAN setup again and make sure everything is configured correctly. See "Potential Problems" section on page 3-16 for details.

Configuring the Port Record

Procedure

To configure the Port record for the remote node:

Step	Action	Result/Description
1	From the CTP Main menu, select **Configure -> Port**.	The Port record appears.
2	In the Port Number parameter, type **5,** then press ENTER.	This sets the LAN port for node 200. **Note** Port Number represents the physical port on the back panel of the device. It is also the reference number of the port record.
3	In the Port Type parameter, type **ETH**, then press ENTER.	This identifies the port type for the LAN port. In this case, it is an Ethernet LAN.
4	Use the default values for the rest of the parameters at this time. Type a semicolon (**;**) after the last value, then press ENTER.	This saves the record.

Configure the LAN Connection

Procedure

Next, you need to configure the LAN Connection. The LAN Connection is made up of two records:

- LAN Connection Parameters
- LAN Connection Table

Configuring LAN Connection Parameters

Since you need only one LAN connection, use for this example the default value of 32. So, when you access the parameter record, save the default value.

To configure the LAN Connection Parameters:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Configure LAN Connection -> LAN Connection Parameters**.	The LAN Connection Parameters record appears.
2	In the Maximum Number of LAN Connections parameter, type **32**.	This identifies the maximum number of LAN connections you want to configure for your node. For this example, you need only one LAN connection, so the default value of 32 works well.
3	Type a semicolon (**;**), then press ENTER.	This saves the record.

Configuring the LAN Connection Table Record

After you define the number of maximum LAN connections that you can have, you must setup the actual LAN/WAN connections.

To connect LAN connection entries to interfaces:

Step	Action	Result/Description
1	From the CTP Main menu, select **Configure -> Configure LAN Connections -> LAN Connection Table**.	The LAN Connection Table appears.
2	In the Entry Number parameter, Type **1**, then press ENTER.	This is the entry number used to reference this record. This entry is mapped to the WAN interface specified in the Router Interface Number parameter that follows.
3	In the LAN Forwarder Type parameter, type **ROUT**, then press ENTER.	
4	In the Router Interface Number parameter, type **5**, then press ENTER.	This is the default and the WAN interface.
5	In the Autocall Mnemonic parameter, leave it blank.	The default is Blank. Leave it blank in the node receiving the call. Because this node is receiving the call, you do not have to configure a Remote Connection ID in this node.
6	Use the default values for the rest of the parameters at this time. Type a semicolon (**;**) after the last value, then press ENTER.	This saves the record.

Configure Router Interface

Procedure

Before the local node can call the remote node, you must establish a virtual circuit between the nodes. This means you need to configure the router interfaces. First, enable the interfaces for interface 1 and interface 5.

To enable the interfaces for interfaces 1 and 5:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Configure Router -> Configure Interface States**.	The Configure Interface States record appears.
2	In the Interface #1 State parameter, type **Enable**, then press ENTER.	This enables interface 1, the LAN interface.
3	In the Interface #5 State parameter, type **Enable**, then press ENTER.	This enables interface 5, the WAN interface.
4	Use the default values for the rest of the parameters at this time. Type a semicolon (**;**) after the last value, then press ENTER.	This saves the record.

Configure IP

Procedure

Next, you must configure IP parameters and IP interfaces.

IP Parameters

Although you do not need to change anything in the IP parameters record for this example, you must access the record and save it.Your changes are not in CMEM until they are saved.

To access and save the IP Parameters record:

Step	Action	Result/Description
1	From the CTP Main menu, select **Configure -> Configure Router -> Configure IP -> Parameters**.	The Configure Interface States record appears.
2	In the Maximum Number of IP Interfaces, type **36**, then press ENTER.	
3	Type a semicolon (**;**), then press ENTER.	This saves the record.

IP Interfaces

Now you need to configure the IP interfaces. You are going to configure two IP Interface entries: one for interface number 1 which is your LAN port and one for interface number 5 which is your WAN port.

To configure the IP interfaces for the remote node:

Step	Action	Result/Description
1	From the CTP Main menu, select **Configure -> Configure Router -> Configure IP -> Interfaces**.	The Configure IP Interfaces record appears.
2	In the Entry Number parameter, type **1** (if it is not displayed already), then press ENTER.	
3	In the Interface Number parameter, type **1** (if it is not displayed already), then press ENTER.	This is for the LAN port.
4	In the IP Address parameter, type **200.33.2.1** for this example.	You may want to use the IP address assigned by your network administrator.
5	Type a semicolon (;) after the last value.	This saves the record and entry Number 2 appears.
6	In the Entry Number parameter, type **2** (if it is not displayed already), then press ENTER.	
7	In the Interface Number parameter, type **5**, then press ENTER.	

Step	***Action*** *(continued)*	***Result/Description***
8	In the IP Address parameter, type **199.33.1.1** for this example.	This assigns an IP address to the WAN interface for the local node for this example. Again, you should check with your network administrator to determine a valid IP address to connect your WAN service provider.
9	Type a semicolon (;) after the last value and press ENTER.	This saves the record.

Configure Route Selection Table

Procedure

Since the local node is doing the calling, you must set up the Route Selection Table to receive the call in the remote node. The Route Selection Table routes the call from the WAN adapter at 20094 to the LCON in the remote node.

To configure the Route Selection table:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Configure Network services -> Route Selection Table**.	The Configure Interface States record appears.
2	In the Entry parameter, type **2**, then press ENTER.	You already defined Entry 1 as the route selection for your WAN access, so you cannot use that entry. This entry contains the route selection that enables incoming calls to route to the WAN adapter of node 200.
3	In the Address parameter, type **20094**, then press ENTER.	This is the address of node 200's WAN Adapter.
4	In the #1 Destination parameter, type **LCON,** then press ENTER.	This routes incoming calls from the WAN Adapter to node 200's LAN connection. **Note** If you access Help at the #1 Destination parameter, notice that **LCON** is not listed as a choice. It is a valid value, however, and it is the only value that routes incoming calls between the remote node's WAN Adapter and LAN Forwarder.
5	Type a semicolon (;) after the last value, then press ENTER.	This saves the record.

Boot The Node

Procedure

Now, you should boot the node to implement your changes.

To boot the node:

Step	*Action*
1	From the CTP Main menu, select **Boot -> Node (warm)**.
2	Type **Y** at the prompt. The node resets itself. Check your Vanguard Installation Manual for start-up diagnostics if you have any problems.

Pinging Interfaces

Overview

In an IP network, “ping” sends a single packet and listens for a single packet in reply. Ping is implemented using the required ICMP Echo function, documented in RFC 792. Ping places a unique sequence number on each packet it transmits and reports which sequence numbers it receives back. This allows you to determine if packets have been dropped, duplicated, or reordered.

When to Use Ping

The ping function can be used to confirm the operation of IP interfaces in your network. Begin by pinging the LAN interface first and then proceed to other interfaces in your network.

Follow these steps to preform a Ping operation on each interface:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Diagnostics -> IP Ping**.	The Target IP Address prompt appears. This parameter is entered in dotted notation and defines the 32-bit IP host address associated with the node to be pinged. For example, type the IP address of the LAN interface for the local node first.
2	Type the IP address of the destination node to be pinged, then press ENTER.	The Source IP Address prompt appears. This parameter allows you to change the source IP address field in the ICMP packet. It also allows an ICMP packet to respond to an address other than the default. A valid value is one of the node's operational interfaces or the internal IP address. The default value (0.0.0.0) allows the router to calculate the source IP address in the regular way.
3	At the Source IP Address parameter, use the default value (0.0.0.0) or type the address of one of the node’s operational interfaces or the node’s internal IP address, then press ENTER.	The Number of Packets prompt appears.
4	At the Number of Packets parameter, type the number of ICMP packets you want to transmit, and then press ENTER.	The Packet Size prompt appears. The Packet Size parameter requires an integer from 56 to 1124. The Packet Size parameter typically matches your network.

Step	Action	Result/Description
5	At the Packet Size parameter, type the number for the packet size you require, and then press ENTER.	The Response Window parameter appears. This parameter allows for the inherent delay in your network. The Response Window parameter specifies the number of seconds that ICMP waits for a response before deciding that PING failed.
6	At Response Window parameter type the number of seconds that ICMP waits for a response before deciding that PING failed, and then press ENTER.	The PING is executed. Refer to Figure 3-9 for an example of a PING.
7	Source IP address Parameter	

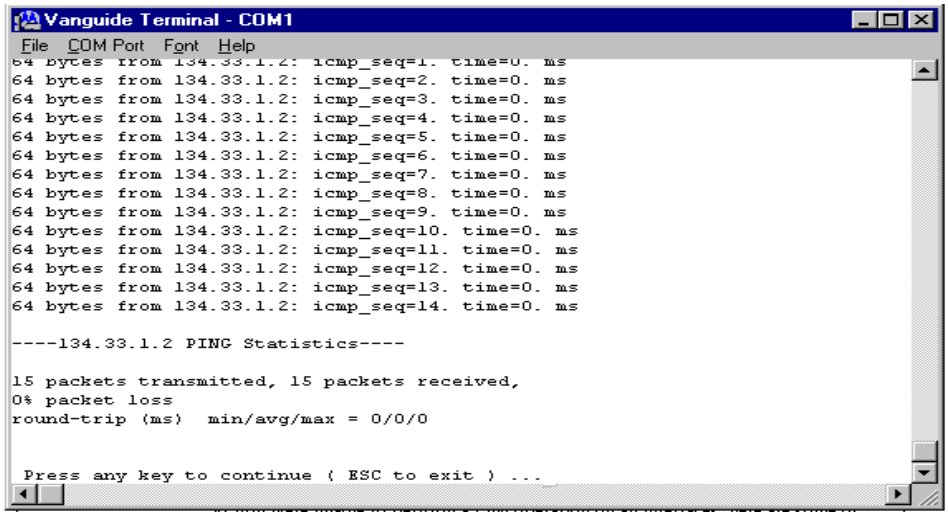


Figure 3-9. Example of PING Information

The number of packets received should equal the number of packets transmitted. Sometimes the first ping operation may fail, so retry if the first one does not succeed.

If zero (0) packets are returned, the Ping operation was unsuccessful, and you have a problem with the configuration of your interfaces.

See “Potential Problems With LAN Interfaces” section on page 3-47 for details on troubleshooting your LAN interfaces.

Multiple IP Ping (Remote Ping)

Creation

Multiple IP Ping allows you to create a maximum of ten ping entries using these parameters:

- Source IP address
- Remote IP address
- Number of packets
- Packet size
- Ping response window

The created ping record are stored in CMEM.

Activation

A user can make a specific ping entry active among all the ping entries. Once the ping entry is activated, this ping entry sends out the predefined parameters. Once the ping transaction is finished, it can be made active again if the ping is reset.

Deactivation

The user can make a specific ping entry deactivate among the ping entries (while that ping entry is sending the packet). When an entry is deactivated, the sending packet is stopped and result statistics are gathered.

Deletion

The user can delete a specific ping entry after the response has been received. A configured and not activated ping entry should be deleted automatically after five minutes have passed since it's creation. A ping entry can also be deleted manually by CTP delete menu under the Network Services menu.

Multiple IP PING

From the CTP Main menu, select **Diagnostics->IP Ping->Multiple IP Ping:**

```
Node: Nodename Address: (blank)
Menu: Multiple IP Ping

1. Ping Parameters
2. Ping Controls
```

Figure 3-10. Multiple IP Ping Menu

Multiple IP Ping Parameters

These parameters must be set in order to configure multiple IP Ping:

Multiple IP Ping -> Ping Parameters

Ping Instance Number

Range:	1 to 2147483647
Default:	1
Description:	Specifies the instance number of the Ping Entry.

Ping Protocol

Range:	TCP/IP, NOV
Default:	TCP/IP
Description:	This is the protocol for the ping.

Source IP Address

Range:	Any valid IP address in dotted notation
Default:	0.0.0.0
Description:	This parameter is entered in decimal dotted notation, and defines the 32-bit IP host address associated with the source node. This must be a valid address corresponding to one of the nodes operational interfaces or the internal IP Address. If no value is specified by the user (default case), it is selected by the router in this order: the internal IP address (if configured) or the IP address of the lowest interface that is up.

Remote IP Address

Range:	Any valid IP address in dotted notation
Default:	0.0.0.0
Description:	Specifies an IP address that becomes the default target IP address for the ping.

Packet Number

Range:	1 to 65000
Default:	10
Description:	Specifies the packet number for the ping.

Packet Size

Range:	56 to 1124
Default:	56
Description:	Specifies the packet size for the ping.

Response Window

Range:	1 to 60
Default:	1
Description:	Specifies the response window for the ping.

Packet Priority

Range:	0 to 255
Default:	1
Description:	Specifies the priority of the packet for the ping.

Ping Control

These parameters must be set in order to configure Ping Control:

Multiple IP Ping -> Ping Control

Ping Instance Number

Range:	1 to 2147483647
Default:	1
Description:	Specifies the instance number of the Ping Entry.

Ping Admin

Range:	DEACT, ACT, RESET
Default:	ACT
Description:	These parameters control the pin transaction: **DEACT:** Used to make a ping entry deactivate **ACT:** Sends a ping request **RESET:** Resets a ping entry

Trace Route

Overview

Trace Route is a troubleshooting tool that allows you to study the route that an IP datagram takes to a certain destination. It displays a complete list of routers that a datagram crosses in order to reach its destination. Trace Route also provides the Round Trip Time (RTT) between the Vanguard where the Trace Route program resides and each of the routers that the datagram crosses.

When to Use Trace Route

Typically Trace Route is used when ICMP packets are lost or the Return Trip Time (RTT) is very high after a ping. Trace Route allows the user to examine the path of an ICMP packet and determine where problems lie.

Follow these steps to use Trace Route:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Diagnostics -> Traceroute**	The Target IP Address prompt appears. This parameter is entered in dotted notation and defines the 32-bit IP host address associated with the destination node to be traced.
2	Type the IP address of the destination node to be traced, then press ENTER.	The Source IP Address prompt appears. This parameter is entered in decimal dotted notation and defines the 32-bit IP host address associated with the source node. This must be a valid IP address corresponding to one of the nodes's operational interfaces or the internal IP address. The default of 0.0.0.0 means not configured, in which case it is selected by the router in this order: the internal IP address if configured, or the IP address of the lowest interface which is up.
3	Type the desired Source IP Address or use the default of 0.0.0.0, then press ENTER.	The Timeout prompt appears. The Timeout parameter defines the number of seconds a node waits for a response to a datagram probe. This parameter is entered in numeric form and must be a number from 1-255. The default is 3.
4	Type the desired value for the Timeout parameter and press ENTER.	The Probe Count prompt appears. This parameter defines the number of probes to be sent at each Time to Live (TTL) level. This parameter is entered in numeric form and must be a number from 1-30. The default is 3.

Step	Action	Result/Description
5	Type the desired value for the Probe Count and press ENTER.	The TTL prompt appears. The Trace command terminates when the destination is reached or this value expires. This parameter is entered in numeric form and must be a number from 1-255. The default is 30.
6	Type the desired value for the Time to Live parameter and press ENTER.	The Port Number prompt appears. The destination port number is used by UDP probes. This parameter is entered in numeric form and must be a number from 0-65535. The default value is 0, which means that UDP is not used, and ICMP probes are sent instead. If UDP datagrams are to be sent, the recommended value is 33434.
7	Type a value other then 0 if UDP is used and then press ENTER.	The Trace Route program is executed. The following is an example of what appears: Tracing the route to 15.15.15.2 1 10.10.10.1 4ms 2ms 2ms 2 12.12.12.1 8ms 9ms 8ms 3 15.15.15.1 5ms 8ms 7ms 4 15.15.15.2 6ms 5ms 5ms

Not all IP datagrams follow the same route. The Trace Route program sends out several consecutive datagrams at each TTL level. The default setting uses 3 probes for each TTL. You may want to increase the number of probes to increase the accuracy of the test. Some older routers do not send back a ICMP port unreachable message. As a result, the end destination of the datagram does not show up in the list.

Potential Problems With LAN Interfaces

What To Look For

If you were unable to perform a Ping or use Trace Route on all interfaces, here are some of potential problems you can troubleshoot:

- Make sure the Remote ID parameter in the local node's LAN Connection Table is set to a value of 1. The remote Connection ID should be pointing to LAN Connection Table entry 1 in the remote node.
- Make sure the WAN links are up. If the SVC is not in an UP state, make sure you are calling the correct node. Check the Frame Relay Statistics.
- Check the FRI Station State. Look to see if your local node is generating outbound calls, and make sure the calls are going to the correct location.

For more details, see Chapter 8, What To Do If Something Goes Wrong, in this manual.

Chapter 4
Don’t Forget About This

Some Other Things You Should Know How To Do

Overview

This chapter describes the various system maintenance activities that you should know about:

- Setting the Date and Time on your Vanguard
- Printing a hardcopy of your node’s current configuration
- How to Copy/Insert Records
- Deleting a Record
- Examining Records
- Listing Records
- Saving and Restoring Configuration (CMEM) Files
- Accessing a node with misconfigured ports
- Booting a node to implement configuration changes.
- Resetting your node to its default parameter values
- Specifying the Control Terminal Port calling address

Setting the Date and Time

Overview

The Date and Time function is a basic function that lets you set the time and date on your Vanguard. When the Time and Date are set, the statistics screens on the node are time and date stamped. You should set the correct date and time so the time stamps for alarms correlate with the date and time of occurrence.

Under certain circumstances, you can use another function, the Simple Network Time Protocol (SNTP), to provide date and time synchronization on the network for accurate billing, packet stamping, and alarm information. Refer to Appendix B, Implementing SNTP, for more information about SNTP.

How To Set the Date and Time

Follow these steps:

Step	*Action*	*Result*
1	From the CTP Main menu, select **Update System Parameters -> Date and Time**.	The Date/Time Update screen appears as shown in Figure 4-1.
2	Enter the four digits to represent the year.	This field sets the year.
3	Enter the first three letters of the month.	This field sets the month.
4	Enter the day of the month. Range = 01 to 031.	This field sets the day of month.
5	Enter the hour. Range = 00 to 23.	This field sets the hour of the day by 24-hour clock.
6	Enter the minute. Range = 00 to 59.	This field sets the minute.
7	Enter the second. Range = 00 to 59.	This field sets the second.

Date/Time Parameters Example

Figure 4-1 shows an example of the Date/Time update screen. This screen allows you to set the node's time and date. Press ENTER to move through the parameters and set new values. Make sure you use a semicolon (;) to save your changes after the last value.

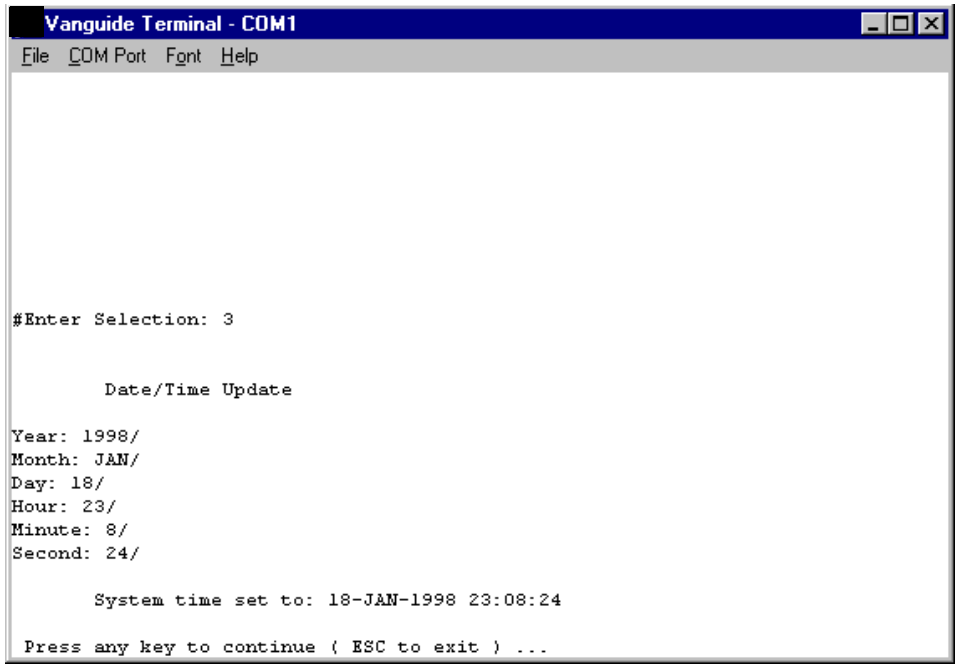


Figure 4-1. Date/Time Update Screen

Note

A boot is *not* required to activate the Time and Date function.

Printing Configurations

Introduction

The Print Configuration menu option is available from the CTP main menu. This function allows you print a node's configuration so that you can examine it and determine how to configure other nodes in your network.

Note

This utility may not be available with all Vanguard Application Ware software releases.

Procedure

Follow these steps to print your node's configuration:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Print Configuration**.	The screen appears as shown in Figure 4-2.
2	Select the **Change Print Characteristics** option and enter the necessary information to satisfy these parameters: • Printer Address: (For example enter 10001 if your printer is connected to node 100, port 1.) • Echo to CTP: (Set this to NO if you do not want the data to echo back to the node.) • Lines per Page: (The setting you use here is dependent on the size of paper you want to print on.) • Clear Time Out: (Set this to a large number - less than 255 seconds - to ensure that all configuration data makes to your printer.	The screen appears as shown in Figure 4-3. This configures your node to print to the desired printer.
3	Select the **Select Record Types** option.	The Print Characteristics screen appears as shown in Figure 4-4.
4	Enter the numbers corresponding to the characteristics you would like to print.	This selects the configuration information to be printed. To select all parameters, enter all numbers separated by a (**+**) sign.
5	Select the **Print Selected Records** option.	The aspects of your nodes configuration that you have selected are printed.

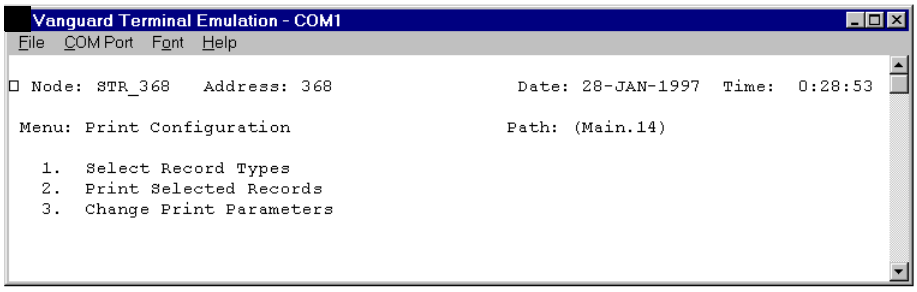


Figure 4-2. Print Configuration Menu

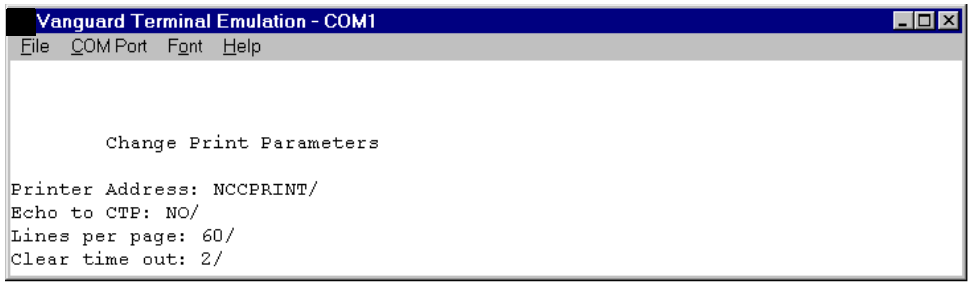


Figure 4-3. Changing Print Parameters

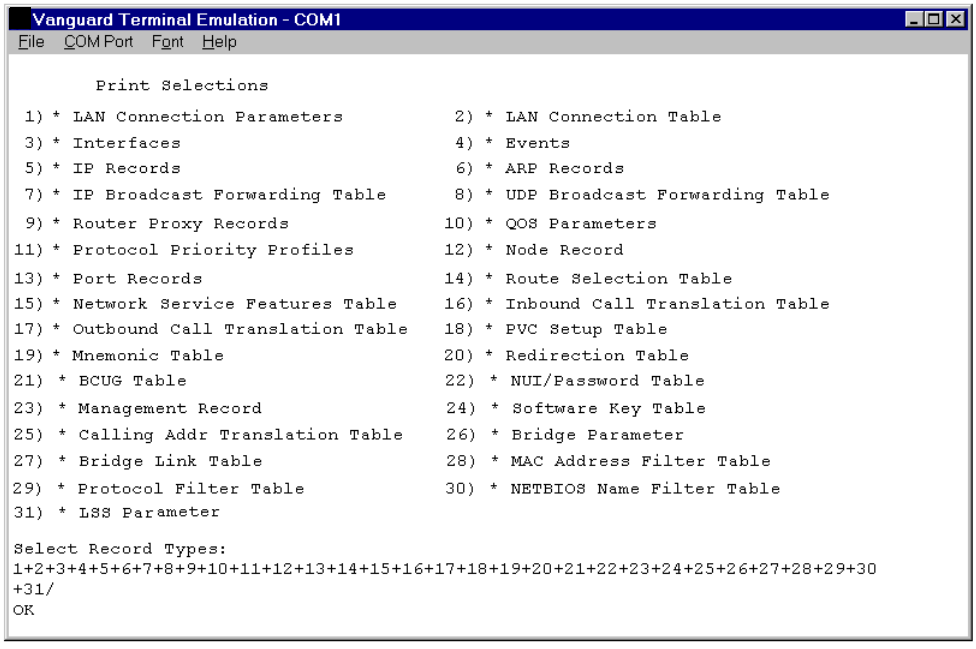


Figure 4-4. Print Characteristics Screen

Limit CTP Calling Addresses

Introduction

The CTP Calling Address function lets you specify which calling addresses can access your node's Control Terminal Port. In other words, a calling address must be listed or it is denied access to the Control Terminal Port.

Leave all the entries blank to allow any node to call the Control Terminal Port on this Vanguard.

Procedure

Follow these steps to implement the Valid CTP Calling Address:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Update System Parameters -> Valid CTP Calling Address**.	The Valid CTP Calling Address screen appears as shown in Figure 4-5.
2	In the Entry parameter, type in an entry number or accept the default value.	
3	In the Address parameter, type in the address of the node(s) allowed to call this node's CTP.	
4	Type a semicolon (;) after the last value.	This saves the record.

Note

Enter a wildcard character (*) to let a series of nodes access the CTP. For example, enter 200* to let all node addresses beginning with 200 access the CTP.

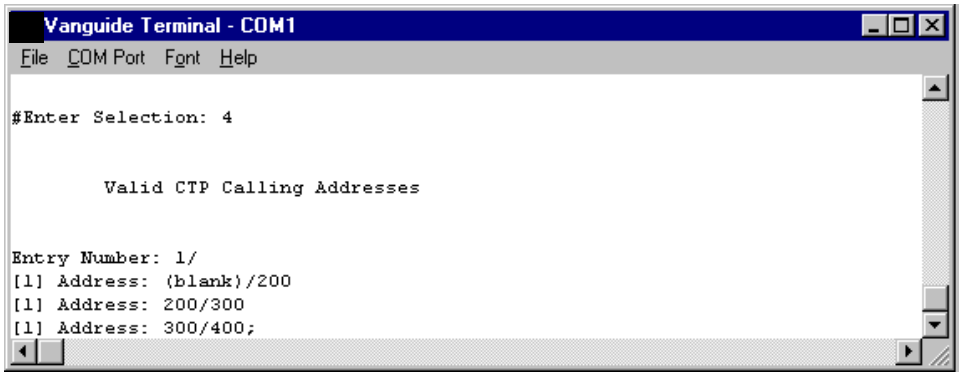


Figure 4-5. Valid CTP Calling Address Example

Copy/Insert Records

Introduction

The Copy/Insert command is available from the Main menu. It lets you copy or insert the parameter values from one record to another within the same node.

Note

You cannot use the Copy/Insert command from one node in the network to another node in the network.

When to Use The Copy Function

You should use the copy function when:

- You are configuring many ports which are the same, or nearly the same. In the latter case, edit small changes as required after the copy has been made.
- You are configuring identical records. The copy command removes the chance of error in repeatedly entered data.

Copy/Insert Record

When you select Copy/Insert Record from the Main menu, the Copy Insert Record appears as shown in shown in Figure 4-6. Select an option from the menu and follow the system prompts to copy or insert records.

Note

If you have purchased and activated options for this node, additional entries may appear in this menu.

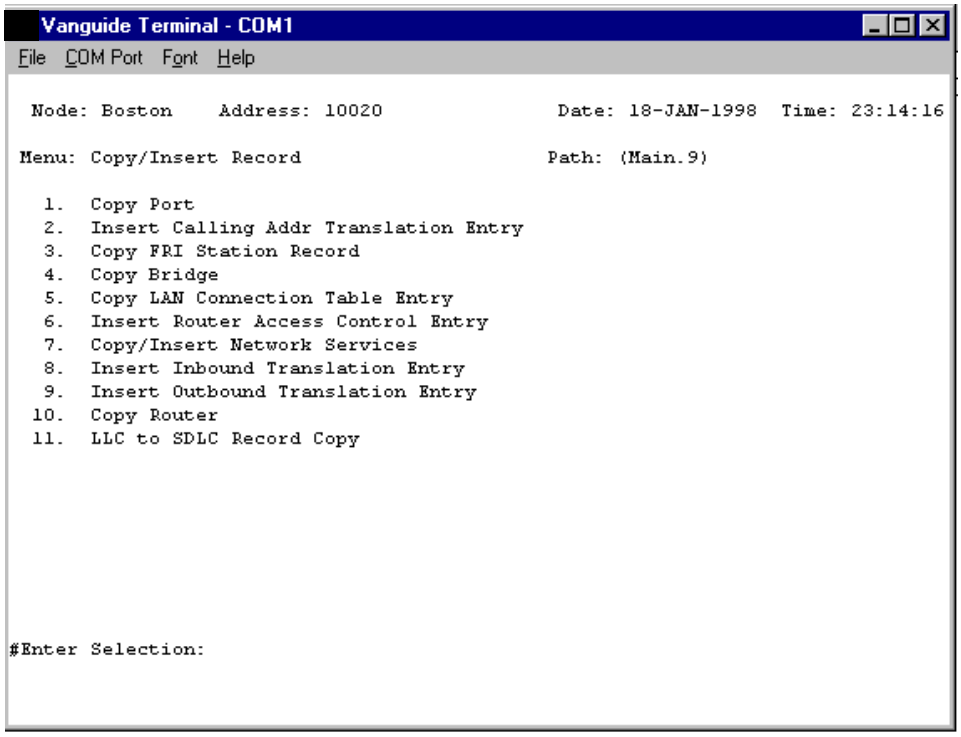


Figure 4-6. Copy/Insert Record

Examining a Record

Overview

The Examine command, available from the Main menu, lets you examine the parameter settings for each entry in a record. You can use this command with the Users, UserPlus, or the Manager Passwords covered in Chapter 5, How Do I Set Up Security on My Node?.

Note

The settings shown by the Examine command are currently configured in CMEM. Changes made in CMEM during this session do not appear until after a boot operation.

Examine Menu

Figure 4-7 shows the Examine menu.

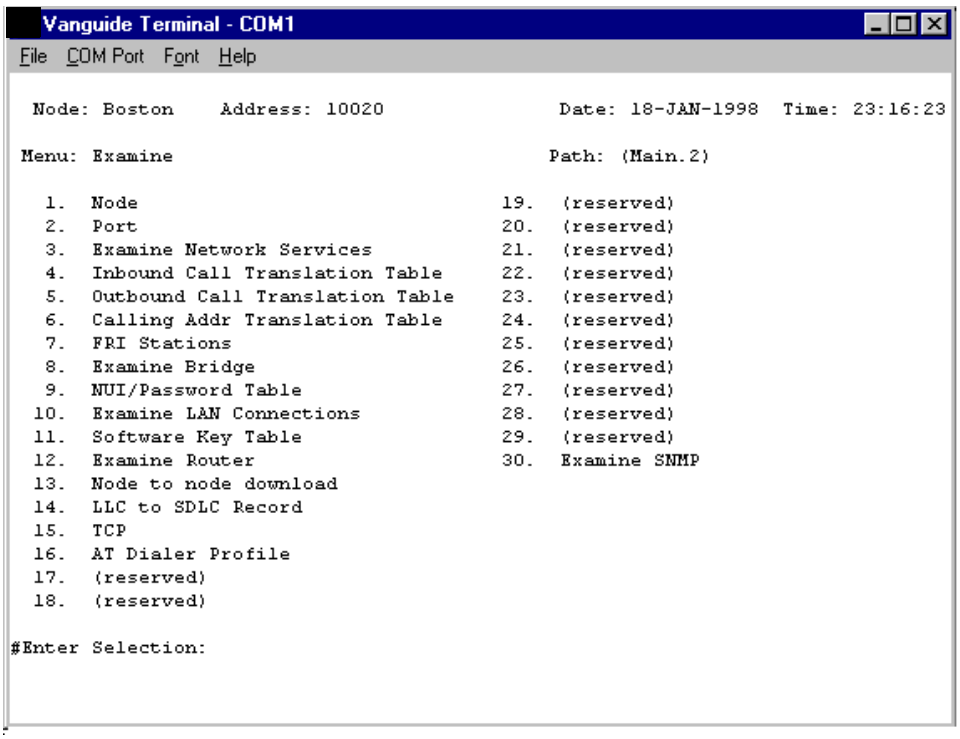


Figure 4-7. Examine Menu

Using the Examine Command

Select the record and press ENTER. Depending on the record selected, the prompts vary. In some cases, a record has so many parameters that several screens are needed. In these cases, you are prompted to press a key to display subsequent screens.

Examine Port Record Menu Example

Figure 4-8 is a sample of the Examine Port Record menu for Port 1.

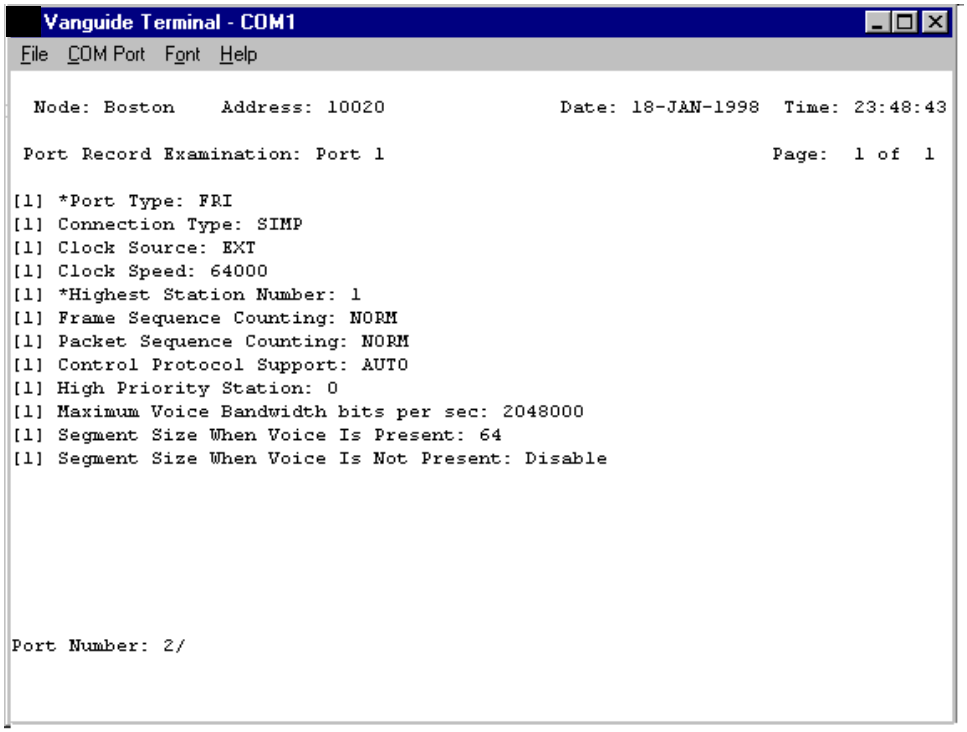


Figure 4-8. Examine Port Record Menu Example

Listing Records

Overview

The List command lets you see all the parameter settings for all the entries in a record. It is a little different from the Examine menu because it shows only the values for the parameters in a particular record, instead of the parameter and values as shown by the Examine option.

The List command is available on the Main menu.

You need the Users, UserPlus, or the Managers Password to use the List command.

Accessing Records with the List Command

To list the parameter values for a record, select the record and press ENTER. The screen displays parameter settings for all the configured entries in that record.

Figure 4-9 shows the List menu.

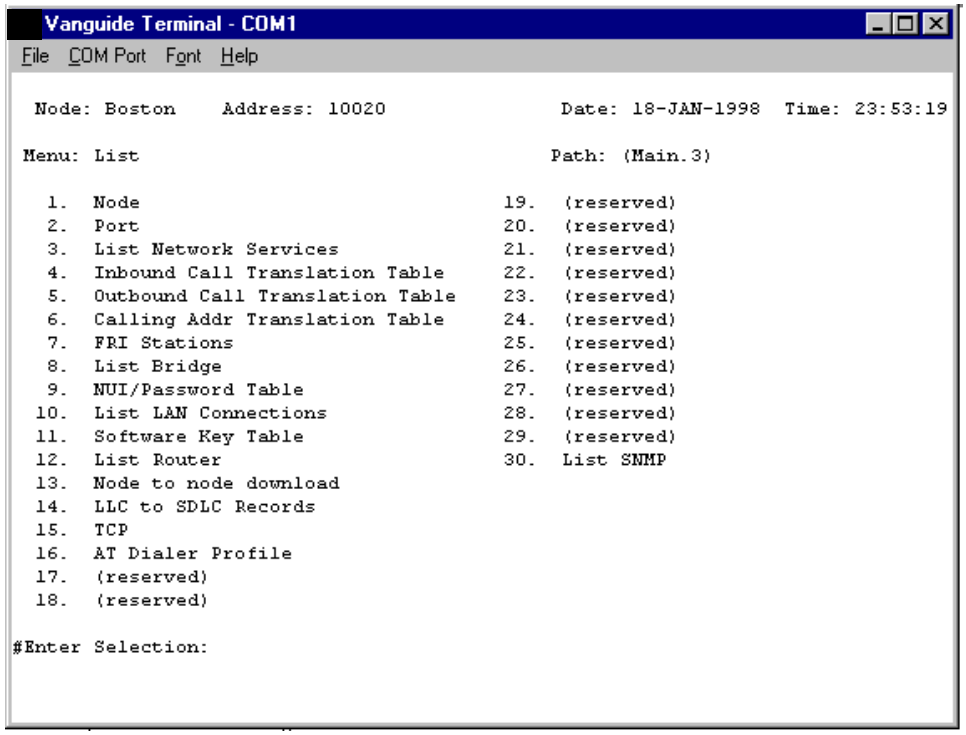


Figure 4-9. List Menu

Example of Port Record List Menu

Figure 4-10 is an example of a Port Record List menu. Notice that the parameter names do not appear, just their settings, in sequence. This format lets you use the data in a database program on a PC. The PC must accept ASCII files with a data communications software set for terminal emulation.

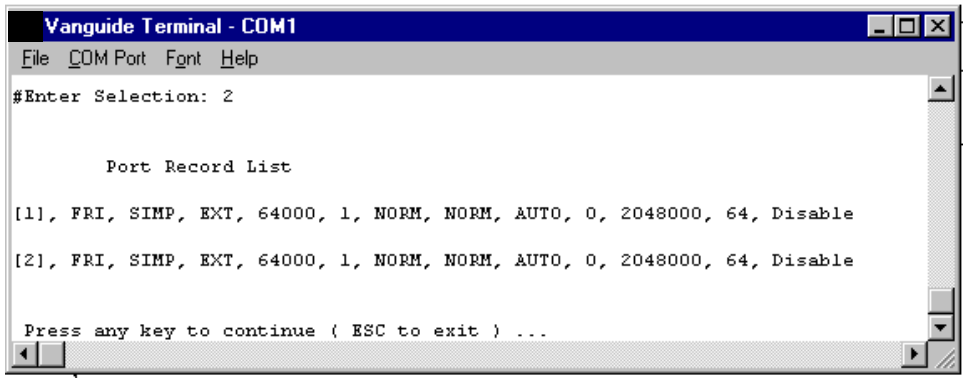


Figure 4-10. Port Record List Menu Example

Deleting a Record

Overview

The Delete command is available from the Main menu and lets you delete a specified record.

Procedure

To delete a port record entry:

Step	Action	Result/Description
1	Select an option from the Delete Record menu.	Depending on the selection, prompts may vary.
2	Before you delete a record, you are prompted **Proceed (y or n)?** If you type: • **Y** • **N** **Caution** There is no restore command. If you delete a record, it cannot be restored.	The port record is immediately deleted, and this message appears: • **Record deleted.** The record is not deleted, and this message appears: • **Record not deleted.**

Figure 4-11 shows the Delete Record Menu.

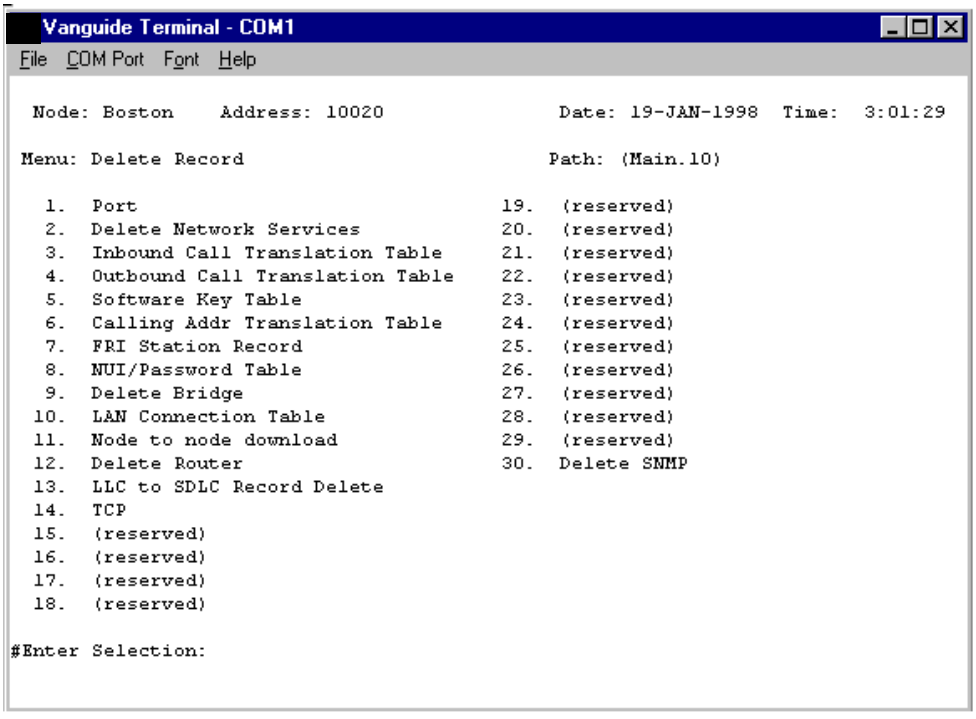


Figure 4-11. Delete Record Menu

Booting a Node

Overview

There are two ways to implement a new configuration in your Vanguard:

- Boot command
- Reset button

Boot Command

Boot Menu Options

The Boot command is available on the Main menu. The Boot menu, shown in Figure 4-12, lets you implement operating parameters that have been stored in the configuration memory. The selections in the Boot menu let you boot the entire node or just a part of it.

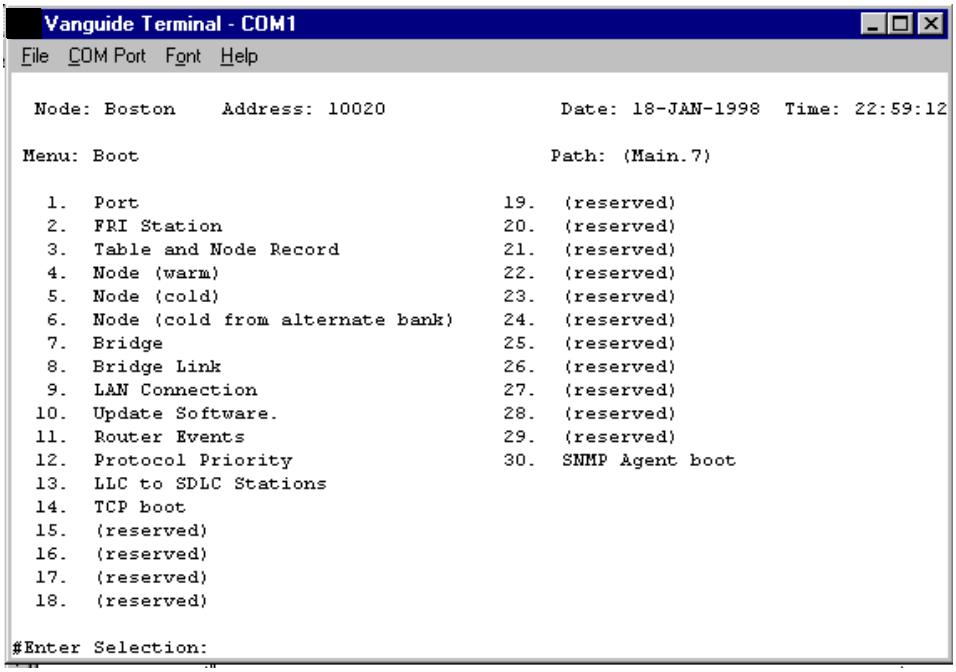


Figure 4-12. Boot Menu Options

Rules for the Boot Command

The following rules apply to the Boot command:

- A boot always disrupts communications on the section of the node being booted. For example, a Port Boot clears all calls on that port.
- A boot is required to implement changes to operational parameters.
- A Node Boot is required to implement changes that effect the organization of memory (for example, altering the number of logical channels on an X.25 link or the number of ports in a node).

Warm/Cold Boots

In most cases, when you change a record's parameter setting, you must boot the record for the change to be implemented. However, some parameters require that the entire node be booted (warm or cold) for a change to take effect. These parameters are identified by an asterisk (*) when they are displayed on the control terminal. A warm node boot and a cold node boot differ:

- Warm Node Boot – the node reloads the configuration and restarts the node.
- Cold Node Boot – runs the diagnostic tests, reloads the operating software which may require a software download, and then reloads the configuration.

Release 5.1 and later of the Applications Ware lets you isolate boot operations to some ports and tables rather than perform a Node boot.

Procedure

Follow these steps to boot a node:

Step	*Action*	*Result*
1	From the CTP Main menu, select **Boot**.	The Boot menu appears, as shown in Figure 4-12.
2	Select the type of boot operation you want to perform.	The **Proceed (y/n):** prompt appears.
3	Type **Y** to boot the node. Or:	The nodes resets itself and implements the changes you made to CMEM.
	Type **N** to stop the boot operation.	The Boot menu appears.

Ease of Configuration

Ease of Configuration is a system enhancement that allows you to implement specific changes to your configuration without the need to reboot the node.

Previously, you had to boot the node to implement changes to certain parameters (those with an asterisk in their name). For example, changes to the Port Record parameter Port Type would only take effect after the node was booted. This disrupted data until the node came back up. However, with Ease of Configuration you only have to boot that port. Data continues to pass through the node's other ports without disruption.

Ease of Configuration is supported on the Vanguard 64xx, 6520, and 6560.

Default Node Command

Introduction

The Default Node command, available from the Main menu, lets you change the current configuration of the entire node back to the factory default settings.

How the Default Node Command Works

This table describes how the Default Node command works:

Step	Action	Result/Description
1	From the CTP Main menu, select **Default Node**.	The Default Node prompt appears, as shown in Figure 4-13.
2	Type **Y** for yes to return the node to its default settings.	The node reboots. When the STATUS light stops blinking and remains on, you can connect to the node.

This table describes how the Default Node command works:Default Node Message

Step	Action	Result/Description
1	From the CTP Main menu, select **Default Node**.	The Default Node prompt appears, as shown in Figure 4-13.
2	Type **Y** for yes to return the node to its default settings.	The node reboots. When the STATUS light stops blinking and remains on, you can connect to the node.

Figure 4-13 shows the Default Node Message.

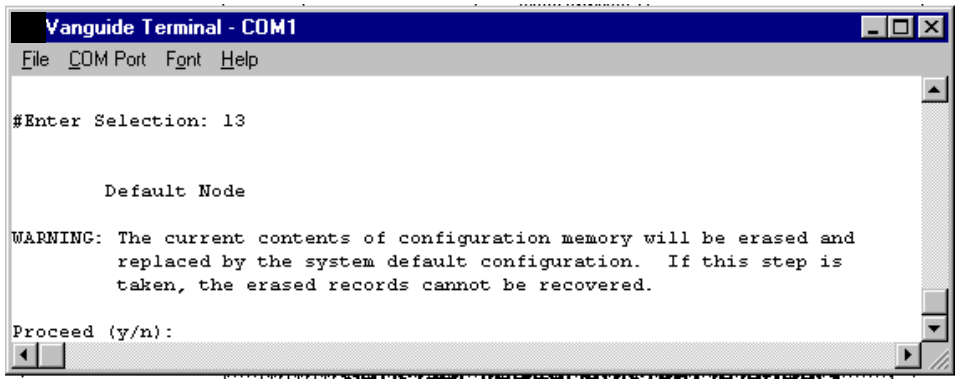


Figure 4-13. Default Node Message

Accessing a Node in an Emergency

Introduction

In some cases, you may be unable to access your node because the ports have been misconfigured as NULL or as a port type you cannot call.

Before You Begin

If you cannot access a node, perform the following procedure:

Caution

This procedure interrupts communications. Be sure that the node can be disabled without disrupting the network.

Step	*Action*	*Result/Description*
1	At the node's front panel, set the default CTP pin switch to ON position. Refer to the Vanguard operator's guide for details on the default CTP port.	The port defaults to an asynchronous PAD Port. For example, on a Vanguard 320, this is port 4. **Note** In a multi-processor node such as the 65xx, the CTP>PT 6 switch only works on the primary processor card.
2	Connect an ASCII asynchronous terminal to the CTP port. Make sure the terminal is set to 9600 bps, 8 data bits, 1 stop bit, no parity.	
3	Press the RESET button or power the node off and on.	The node reboots, and then the CTP prompt (*) or OK appears on the terminal.
4	Type **.ctp** at the * prompt or **ATDS0** at the OK prompt to call the CTP.	The prompt Enter Password appears.
5	Type the appropriate (Users or Managers) password.	The CTP Main menu appears.
6	Correct the configuration or type a new password.	
7	Log off the Control Terminal Port.	
8	Disconnect the terminal.	
9	At the front panel, set the CTP pin to the OFF position.	This turns off default CTP port.
10	Reboot the node.	You are now able to connect to the Vanguard normally.

Chapter 5
How Do I Set Up Security on My Node?

What's the Password?

Introduction

Setting up password security on your Vanguard node is important in order to prevent unauthorized access to your node's operating system and configuration memory.

What Kind of Passwords can I Set?

You can set four different levels of password protection on your Vanguard device:

- Manager's Password
- User's Password
- UsersPlus Password
- Diagnostic Password (Release 6.3 and greater software)

This type of password protection prevents unauthorized users from logging into the CTP menus on your Vanguard and changing system configuration parameters.

If this is the first time you accessed the CTP, or if you have not configured a password, just press ENTER at the Password prompt to access the CTP menus.

Manager's Password

The Manager's Password lets you perform all actions supported by the CTP. You can also view all passwords and define valid users.

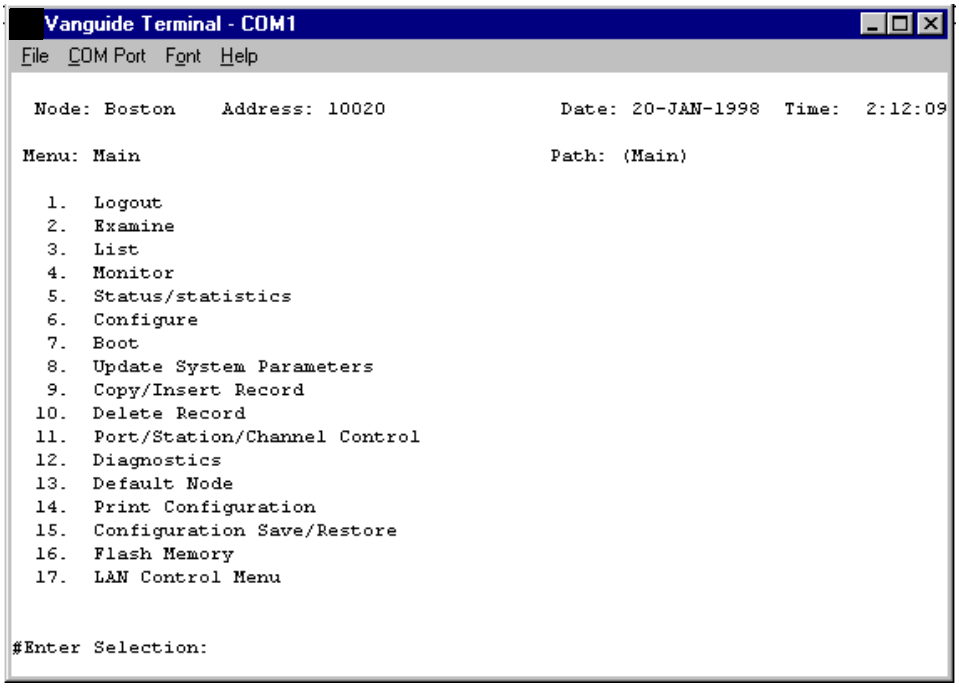


Figure 5-1. Example of Manager Password CTP Access

User's Password

The User's Password lets you examine the node parameter settings, statistics, and node status. It prohibits you from changing the configuration or disrupting any node operations. Figure 5-2 shows the Main menu that appears with the User's Password.

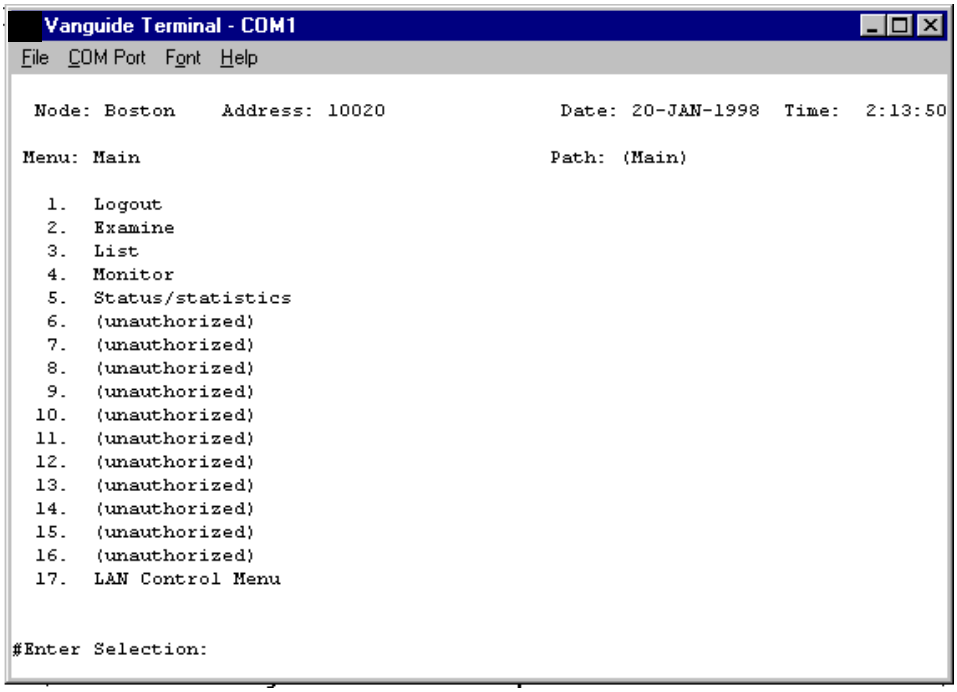


Figure 5-2. Main Menu Example—User's Password

UserPlus Password

The UserPlus Password lets you perform all CTP supported actions that the User Password does and these:

- Node Boot a node
- Port/Station/Channel Control
- Access to the Diagnostics menu

Note

For Vanguard Applications Ware Release 5.1 and earlier, the UserPlus Password requires a Customer Security Key (CSK). At Release 5.1M, the User Plus CSK became part of Applications Ware.

Diagnostic Password

Release 6.3 and greater introduces the Diagnostic Password menu selection. Users will continue to have access to the Logout, Examine, List, Monitor and Status/ statistics menu. Access the Diagnostic Password menu by selecting the Update System Parameter menu shown in Figure 5-3.

Main->Update System Parameters->Diagnostic Password

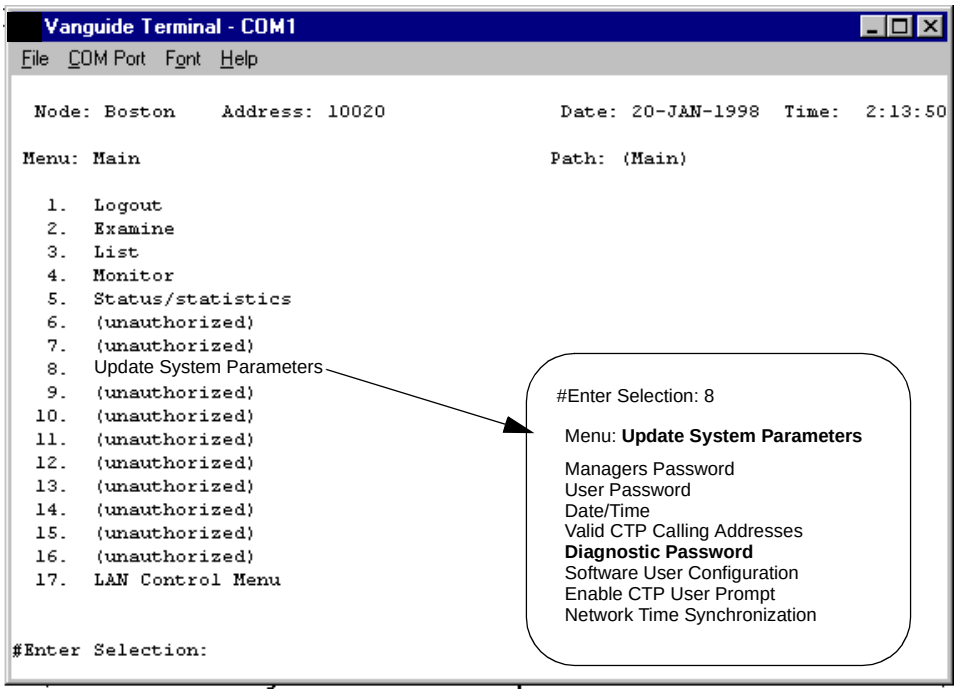


Figure 5-3. Diagnostic Password Menu

Blank Username

The CTP authentication example (listed below) is used when a username prompt option is enabled. In this example, username and password are required for authentication/authorization purpose. An (empty) blank username is allowed for backward compatibility.

CTP authentication example:

When a blank username is used, the node reverts back to the previous way to do the authentication. The user enters a manager password to logon as a manager user (internal username "~oservice_user" will be used in the user profile), and user password is used to logon as a basic user ("~obasic_user" internal username is used).

Enable CTP User Prompt

The CTP user prompt configuration parameter can be enabled or disabled. More information regarding this parameter can be found in the IP Routing Manual, Part Number T0100-03.

Chapter 6
How Do I Set Up Software Keys?

Don’t Forget Your Keys!

Introduction

A Software Access Key (SAK) is a license to use a particular software option for the Vanguard. Each SAK is unique to a specific Vanguard device’s processor card and to a specific software option. This means you may have to purchase and enable individual SAKs for each Vanguard before you can use certain software options.

Note

Effective with Applications Ware Release 5.2, the required use of SAKs has essentially been discontinued. However, there are a relatively small number of SAKs that remain for specific applications. You may still require a SAK if you are using pre-Release 5.2 software. Contact your Vanguard Managed Solutions representative for more information.

Additionally, there is also something called a Customer Software Key (CSK). You install a CSK to enable a particular function or option on a specific node, too. The difference is that CSKs are generally universal across all Vanguard devices, meaning you can use the same key across all your devices in a network.

Another difference between the two is that you generally have to purchase a SAK, while a CSK is usually free.

How to Obtain a SAK

This is how you obtain a SAK or CSK for your Vanguard:

If	*Then*
You purchased/obtained a SAK/CSK with a Vanguard.	The SAK/CSK is shipped with the product.
You purchased/obtained a SAK/CSK for a Vanguard already installed in your network. or: You lost the SAK sheet for the product.	Provide your Vanguard Managed Solutions representative with the CPU serial number of your node and the name of the software option you want to use. You can get the serial number from the Detailed Node Statistics from the Statistics menu. See “Node Statistics” section on page 7-4.

Entering a Key in the Software Key Table Record

Overview

After you get a SAK or a CSK, you can enter it into the Software Key Table on the node. The Software Key Table Record contains all the SAKs enabled on your Vanguard. You can get to this table from the CTP Configure menu.

What You See In This Record

Figure 6-1 shows the Software Key Table record and parameters.

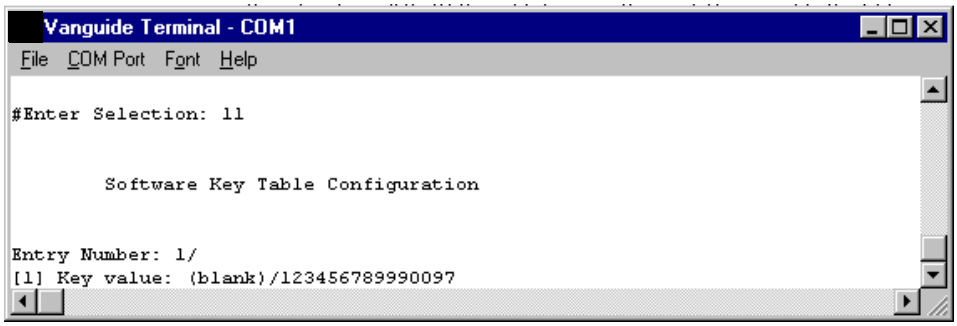


Figure 6-1. Software Key Table Record

Configuration Guidelines for SAKs and CSKs

When you configure the Software Key Table record, use the following guidelines:

- You must configure this record before the node can access optional features purchased after the initial installation.
- Each SAK or CSK option requires a separate entry in the Software Key Table record in each node.
- To implement an option, you must boot the node.

Accessing the Software Key Table Record

Follow these steps to access the Software Key Table Record:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Software Key Table.**	The Software Key Table and its parameters appear. A prompt appears asking you to configure the next parameter.
2	Enter the new SAK or CSK number follow by a semicolon (**;**) to save it, and press ENTER.	The message, **Storing updated record in configuration memory** appears.
3	Press CTRL+T to return to the Main menu.	The Main menu appears.
4	Select **Boot -> Table and Node Record** from the Boot menu to implement your changes.	The following prompt appears: **Boot Configuration Table and Node Records** **Proceed (Y/N):**
5	Type **Y** to boot the node.	The new option is available.

Parameter Descriptions

Here is some detailed information on the Software Key Table record parameters:

Entry Number

Range:	1 to 20
Default:	1
Description:	Specifies the reference number for the individual option that is being enabled. **Note** You must configure a separate entry for each software option enabled for the node. A node can have up to 20 options enabled at one time.

Key Value

Range:	0 to 20 alphanumeric characters
Default:	(blank)
Description:	The key number supplied by VanguardMS for the node. Entering keys in this table activates specialized functionality. If you change the key number or enter the wrong one, the option is disabled. **Note** Enter semicolon (;) to save the entry. **Note** Use the space bar to blank the parameter value.

For More Details

For a complete list of all the CSKs available for your Vanguard, contact your Vanguard Managed Solutions representative.

Chapter 7
Making Sure Everything Is Running Correctly

Monitoring Statistics

Overview

This chapter shows you how to use the Statistics menu from the CTP to monitor your Vanguard node. It is important to understand how to read basic statistics to determine if your node is operating properly. You can also use statistics to troubleshoot connectivity problems.

Only basic statistics such as Node Statistics and Port Statistics are shown here. Refer to the appropriate feature protocol manual for specific statistics (such as X.25, Frame Relay, IP, SDLC, Ethernet and Token Ring LAN, or others).

How Do I Display Statistics?

Follow these steps to view statistics:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select the **Status/Statistics**.	The Status/Statistics menu appears as shown in Figure 7-1.
2	Enter a selection number.	The requested screen appears.

What You See in This Menu

Figure 7-1 shows the Status/Statistics screen. The selections on your screen may differ depending on your Vanguard platform and the installed software image and options.

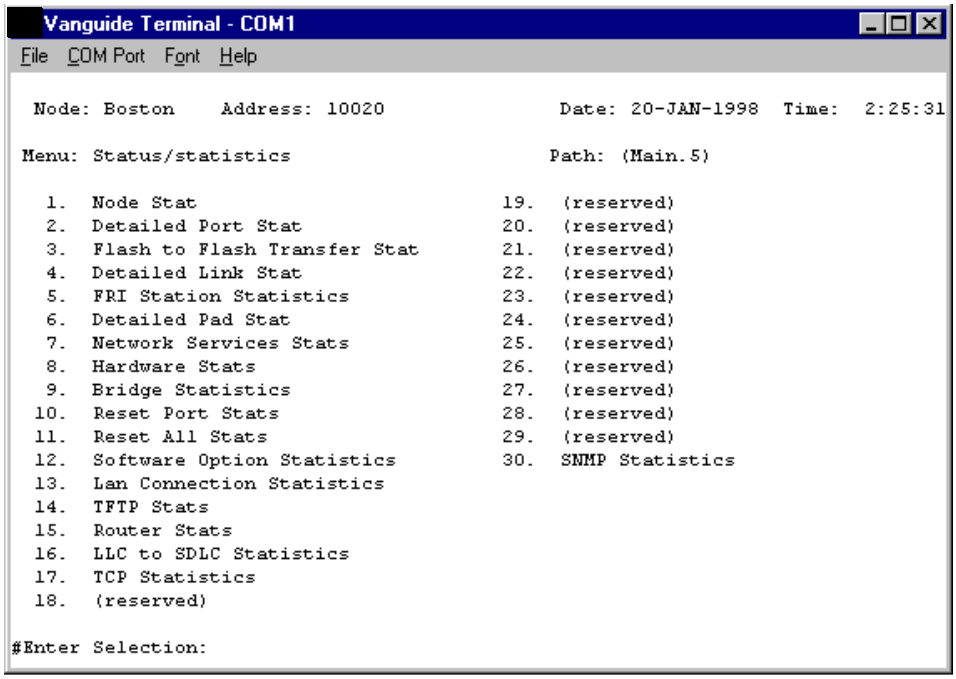


Figure 7-1. Status/Statistics Menu

How To Find Information in Statistics

Here is a partial list of the statistics available to monitor your Vanguard. The statistics available from your CTP menus may differ from what appears here, depending on what options and protocols are configured in your Vanguard. For details on statistics not covered in this manual, refer to the appropriate option or protocol manual.

Use Selection	*For Information Concerning*
Node Stat	Hardware platform, software revision, node serial number, PROM revision, powerup and configuration changes time stamp, calling statistics, node throughput, memory configuration, and port configurations.
Detailed Port Stat	Port type, port status, port speed, control protocol, data traffic summary, error checking summary, port state, DIM interface summary, frame summary, packet summary, and inbound/outbound calling summaries.
Flash to Flash Transfer Stat	The state of any Flash-to-Flash transfer in progress.

Use Selection	For Information Concerning (continued)
Detailed Link Stat	Link state, link speed, timestamp, CRC errors, Link down, data frames in/out, utilization in out.
Detailed Pad Stat	Port number, type and state for PAD device, parity errors, overrun errors, framing errors, data in/out, and utilization in/out.
FRI and FRA Statistics	Statistics on Frame Relay Interface attributes, including station status, station state, congestion detection, call, data, packet, and frame summaries.
Network Services Stats	SVC call summary, including calling channel, called channel, facilities and connection time. PVC connection summary, including source channel, destination channel and connection time. Data compression statistics.
Router Stats	IP statistics, including interfaces states, IP addressing, interface types and numbers, and masks.
Bridge Statistics	Spanning tree statistics, detailed bridge link statistics, bridge link filter status, Transparent Bridge forwarding statistics, and reset.
Reset Port Stats	Clear and reset specified statistics.
LAN Connection Statistics	LAN connection type, connection state, forwarder connection, remote address, autocall attempts, last clear codes, packet summary, last reset, transmit data summary, and discard summary.
Software Option Statistics	Optional software that has been purchased and enabled, which triggers additional selections.

Navigating a Statistics Screen

These keyboard commands let you navigate through the statistics screens and menus.

If You Want To	Press
Update a Statistics screen	CTRL+R
View a previous Statistics screen or prompt	ESC
Return to the Main menu	CTRL+T
Pause a scrolling menu screen	CTRL+S
Resume scrolling	CTRL+Q
Backup a screen	CTRL+B

For More Details

The following sections describe the types of basic statistics reports you can generate, in detail. For details on protocols statistics not covered in this chapter, refer to the appropriate Vanguard Applications Ware Feature Protocols Manual.

Node Statistics

Function

Selecting Node Statistics from the CTP Statistics menu displays a set of Detailed Node Statistics screens as shown in Figures 7-2 to 7-5.

These screens provide details about the selected node. You can use Node Statistics to find out information about node name, node number, the serial number for your node, software installed in the node, motherboard information, and CPU utilization.

The number of screens that appear here depend on the number of daughtercards or option cards installed in your Vanguard.

Example - Page 1

Figure 7-2 shows an example of the first Detailed Node Statistics screen for a Vanguard 320.

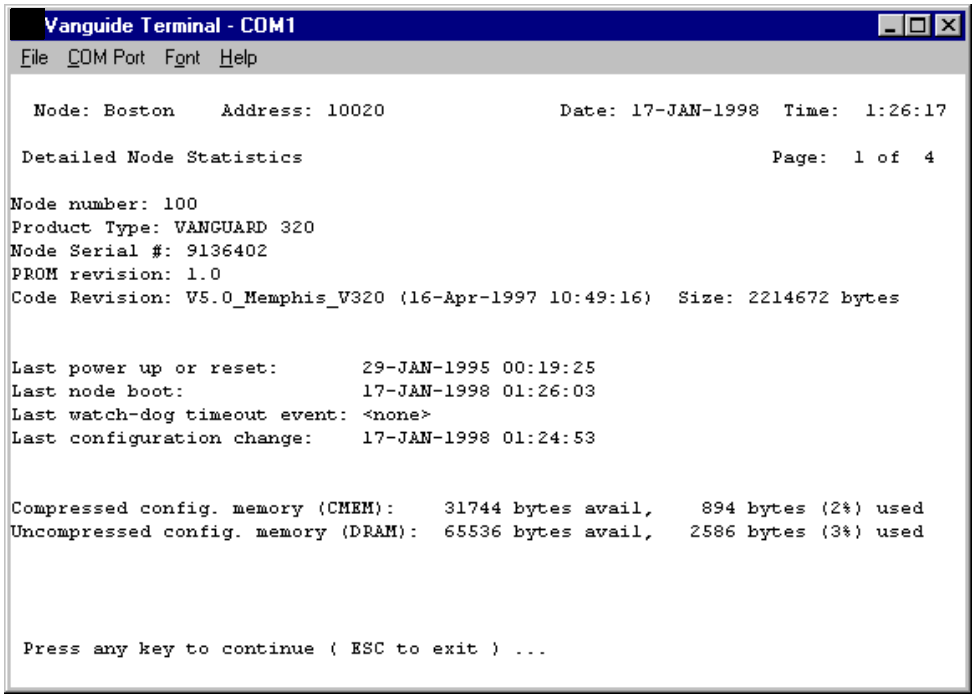


Figure 7-2. Node Statistics - Page 1

Description — Page 1

Depending on the Vanguard unit, the first Detailed Node Statistics screen contains the following information:

Screen Term	Tells You
Node Number	Number of the node
Product Type	Type of Vanguard product
Software Source	Source of the Software: • PROM • Disk • FLASH • Remote
Software PROM Revision	Version of the PROM
Node Agent Revision	Version of the patch PROM
Download Code Source	Source of downloaded software
Size	Size of downloaded software
Flash Software	Status of FLASH
Software ID	• ID of the downloaded software • Revision of downloaded software • Revision of Agent software (if present)
Last Power on Event	The last time that the node was turned on.
Last Reset Button Event	The last time that the node's reset button was pressed.
Last Node Boot	The last time that the node was booted.
Last Watchdog Timeout Event	The last time that the Watchdog timer timed-out.
Last Configuration Change	The last time that the configuration was changed.
Running Power Supplies	Status of power supplies running in the nest (if monitored).
Compressed Configuration Memory	The size of the compressed configuration records in CMEM.
Decompressed Configuration Memory	The size of the configuration records that were uncompressed and are now in RAM. **Note** When the configuration is changed, the size of the Compressed configuration memory and Decompressed configuration memory change.

Example - Page 2

Figure 7-3 shows an example of the second Detailed Node Statistics screen.

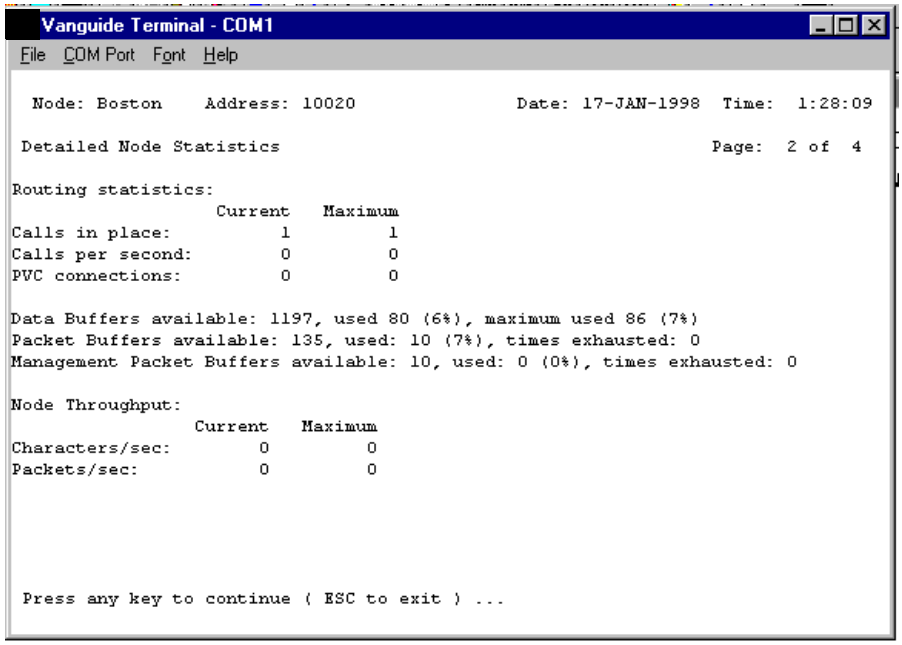


Figure 7-3. Detailed Node Statistics - Page 2

Description — Page 2

The second Detailed Node Statistics screen contains the following information:

Screen Term	*Tells You*
Routing Statistics	Calls in Place: • Number of calls currently in place • Maximum number of calls since the last node or statistics reset Calls per Second: • Rate at which the calls are being processed • Maximum rate of calls processed since the last node or statistics reset PVC Connections • Number of PVCs currently in place • Maximum number of PVCs since the last node or statistics reset

Screen Term	Tells You (continued)
Buffer Pool Statistics	Buffers available: • Number of available buffers • Percentage in use • Maximum percentage of buffers used since the last node or statistics reset
Node Throughput	Characters/sec: • Number of current characters per second • Maximum number of characters per second since the last reset Packets/sec: • Number of current packets per second • Maximum number of packets per second since the last reset **Note** Throughput is calculated by this formula: Number of bytes counted in the previous sec/Link Speed/8

Example - Pages 3 & 4

Figures 7-4 and 7-5 show examples of the third and fourth pages of Node Statistics.

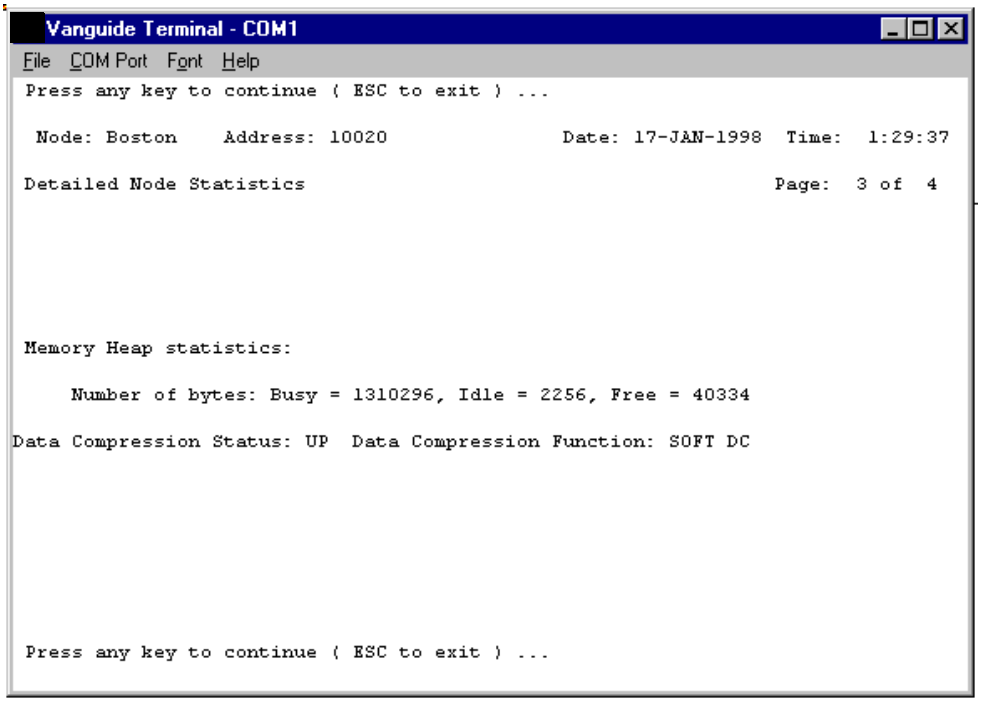


Figure 7-4. Example of Detailed Node Statistics - Page 3

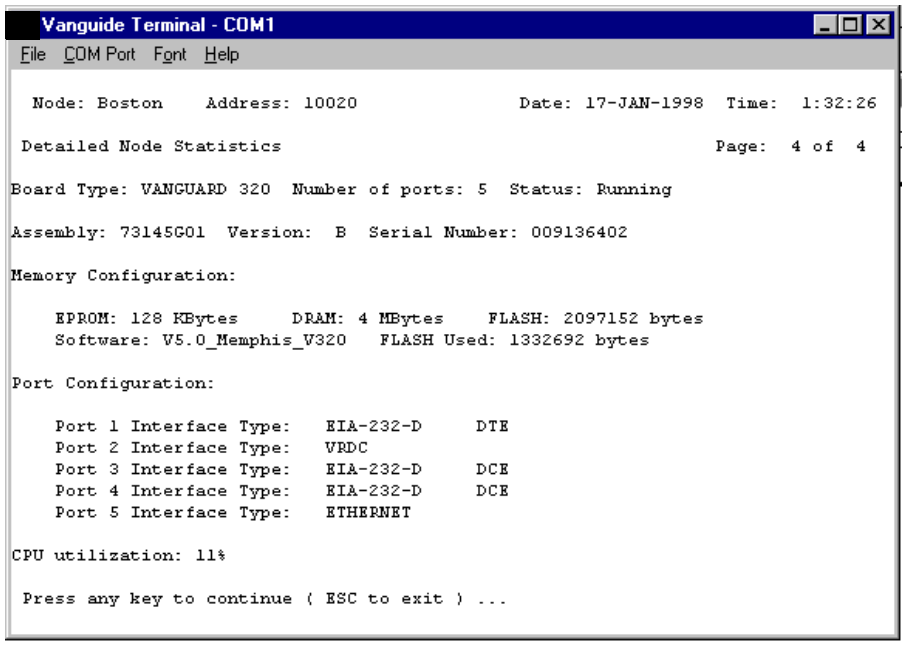


Figure 7-5. Detailed Node Statistics - Page 4

Description — Pages 3 & 4

Detailed Node Statistics pages 3 and 4 contains the following information. Some of these attributes may not be applicable to your Vanguard unit:

Screen Term	*Tells You*
Memory Heap Statistics	Shows allocation of existing memory, including amount of memory in use, idle, and free.
Data Compression Status	Shows data compression option as UP and enabled or DOWN and disabled.
Data Compression Function	Shows the data compression option in operation.
Board Type	Shows type of Vanguard unit motherboard.
Number of Ports	Shows number of ports on motherboard for selected device.
Status	Device or node is either Running: Passed power-up diagnostics, or Failed: Failed power-up diagnostics.
Assembly	Shows motherboard assembly number.
Version	Shows the alphabetical version of the node's motherboard.
Serial #	If you are using Vanguard with a Token Ring card installed, the TRIM's (Token Ring Interface Module) serial number value as read by the software appears here.

Screen Term	Tells You (continued)
Memory Configuration	Shows the following: • EPROM: Memory size available on the processor card • DRAM: Memory size available for data buffers • FLASH: Memory size available on the Flash Module • Software: the installed software image and version number in FLASH. • FLASH Used: Size of software in FLASH.
Port Configuration	Shows the port configuration for selected node including port number and interface type, and DIM setting (DTE/DCE).
CPU Utilization	CPU Utilization: Percentage of time the CPU processed data in the last 64 seconds.
Characters/sec	Number of current characters per second and maximum number since the last node or statistics reset.
Packets/sec	Number of current packets per second and maximum number since the last node or statistics reset.
Board Type	TRIM: Token Ring Interface Module (the daughter card on CPU+ hardware).
Buffer Usage	Percentage of current buffer usage and the maximum percentage since the last node or statistics reset.
Available	Amount of total buffer space in bytes.

Detailed Port Statistics

Function

The Detailed Port Statistics option provides detailed information about a selected port. You can display port statistics on X.25 and Frame Relay WAN ports or any other types of ports configured on your Vanguard.

Since this document focuses on Vanguard basics, it does not examine protocol port statistics here. You can get that information from the Vanguard Applications Ware Feature for the protocol you are interested in. Instead, let us examine the information available when examining the CTP port of a Vanguard 320.

Accessing the Detailed Port Statistics

Follow these steps to access Detailed Port Statistics:

Step	*Action*	*Result*
1	From the CTP Main menu, select **Status/Statistics**.	The Status/Statistics menu appears.
2	Select **Detailed Port Stats**.	The **Port Number** prompt appears.
3	Enter a port number.	Screens appear specific to the type of port configured (for example, APAD, PAD, Frame Relay or X.25).
4	Scroll through the screens for the selected port.	Port statistics appear, as shown in Figures 7-6 and 7-7.

Example - Page 1 ATPAD Stats

Figure 7-6 shows the first screen of the Detailed Port Statistics. Depending on the protocol configured for the selected port, different attributes appear on screen. This port is configured for ATPAD, so attributes specific to ATPAD appear.

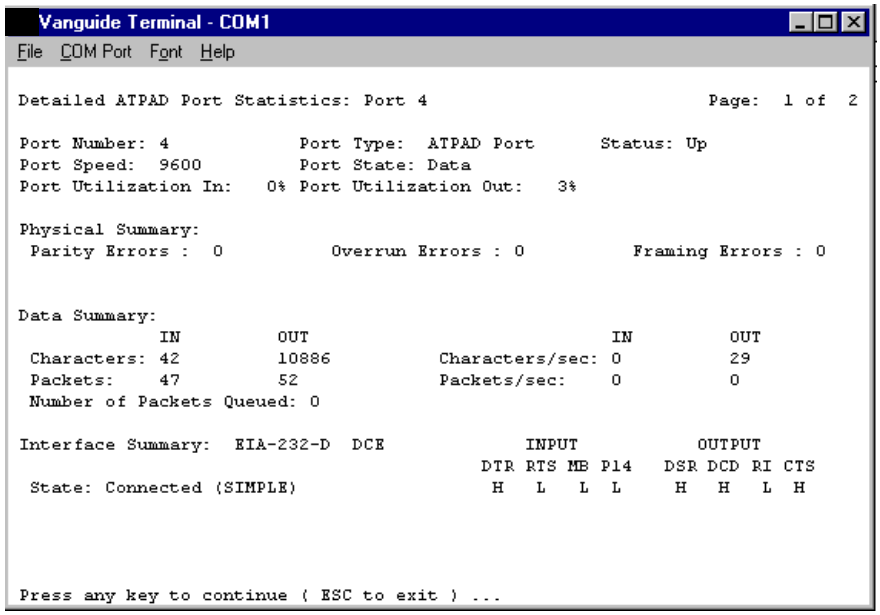


Figure 7-6. Example of Detailed Port Statistics - Page 1

Description for ATPAD Stats Page 1

The first Detailed Port Statistics screen contains the following information:

Screen Term	*Tells You*
Port Number	Number of the port
Port Type	Type of port
Status	Status of the port: • Up: Port is active. • Down: Port is inactive.
Port Speed	Speed of the port if Clock=Int Detected clock speed if Clock=Ext If Port Speed is 0, Clock=Ext, but clocking is not being received from attached device. A CTP port is usually set at 9600 bps.

Screen Term	Tells You (continued)
Port State	Possible states are: • Disabled: An operator has disabled the port. • Busy Out: An operator has busied-out the port. • Remote Busy: The port is receiving RNR frames. • Send_rej: The port is sending REJ frames. • Normal: The link is able to pass data. • Link Setup: The port is sending SABM frames and waiting for a UA response. • Data: passing data.
Port Utilization: In/Out	Percentage of port bandwidth in use. High percentages in these values may indicate network congestion on WAN/LAN ports.
Physical Summary	Number of Overrun, Underrun, Parity, Framing, or CRC errors since the last node or statistics reset. • Overrun Errors: Received data was lost because it could not be processed by the CPU. • Underrun Errors: Transmission of a frame could not be completed because all the data had not been sent to X.25 port. • CRC Errors: Cyclical Redundancy failure because of noise on the line. Depending on your port's configuration, you may see different attributes here.
Data Summary: In/Out	Characters/Packets/Frames: • Number of characters, packets, and frames sent and received by the port since the last node, port, or statistics reset Number of Packets Queued: • Number of packets currently queued • Characters/sec; Packets/sec; Frames/sec • Summary of the characters, packets, and frames being sent and received over the port
Interface Summary	Shows DIM interface and setting for configured ports.
State	Shows physical link connection state with High/Low pin settings.

Screen Term	Tells You (continued)
EIA Summary	Possible states are: • NULL • Connected (SIMPLE) • Idle, Connected (DTR), Wait For Clear (DTR), Wait for DTR (DTR) • Idle, (DTRP), Call Detected (DTRP), Connected (DTRP) • Idle, Call Detected (DIMO), Incoming Call Detected (DIMO), Connected (DIMO), Clear Confirm (DIMO) • Idle, RI On (EMRI), RI Off (EMRI), Wait for RTS (EMRI), Connected (EMRI), Wait for DTR (EMRI) INPUT/OUTPUT: Summary of EIA control signals being sent and received over the port.

Example - ATPAD Stats Page 2

Figure 7-7 shows the second screen of the Detailed Port Statistics.

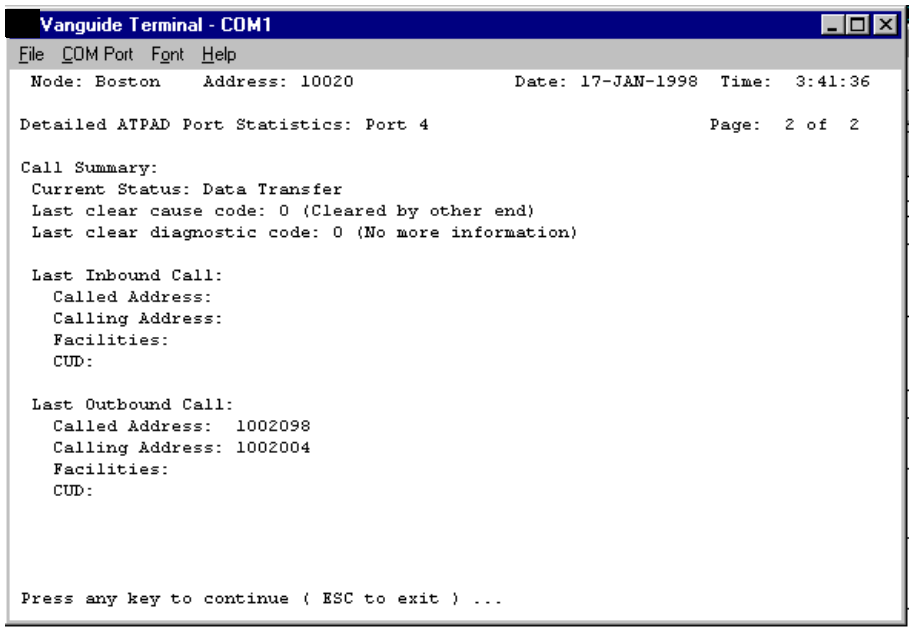


Figure 7-7. Example of Detailed Port Statistics - Page 2

Description of ATPAD Stats Page 2

The second Detailed X.25 Port Statistics screen contains the following information:

Screen Term	*Tells You*
Call Summary	Maximum/Current (SVC/PVC): Number of SVCs and PVCs currently using the port and the maximum number since the last reset
Last Inbound Call	Shows called address, calling address, facilities, and CUD for last inbound call.
Last Outbound Call	Shows called address, calling address, facilities, and CUD for last outbound call.

Detailed Link Statistics

Function

The Detailed Link Statistics option provides detailed information about a selected link's state and status. Detailed Link Statistics is one of the places you should look when you are troubleshooting your WAN connection. You can use these screens to determine if the link you configured is up or down.

Example

Figure 7-8 shows an example of the Detailed Link Statistics screen.

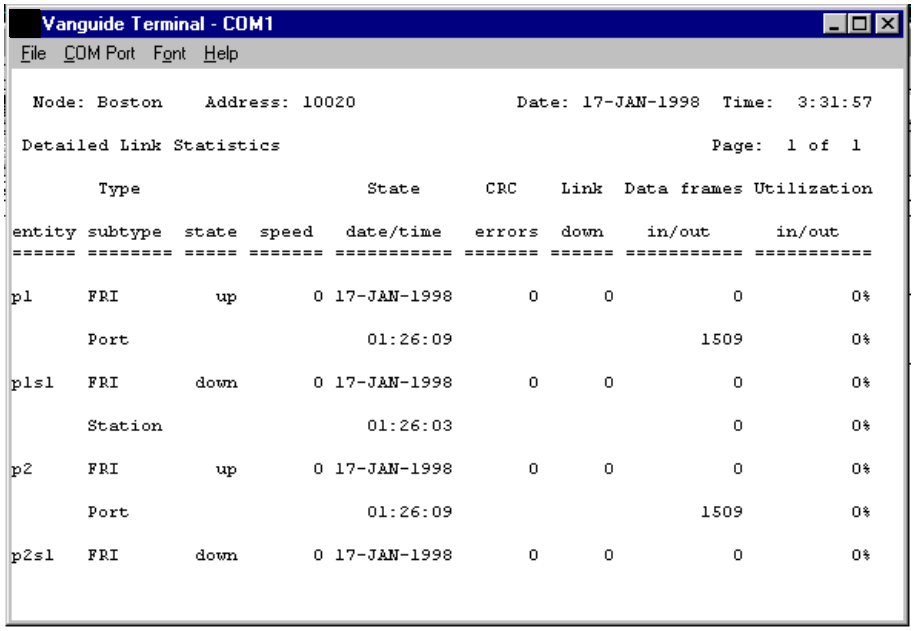


Figure 7-8. Example of Detailed Link Statistics Screen

Description

The Detailed Link Statistics screen contains the following information:

Screen Term	*Tells You*
Entity	Port or Station number (p1, p2, or s1, s2, and so on).
Type or Subtype	Type or subtype of the link: X.25, SDLC, and so on.
State	Link State: Up, Down, Disabled, Busy-Out.
Speed	Actual port speed.
State Date/Time	Time and date of the last state change.
CRC Errors	Number of CRC errors since the last reset.
Link Down	Number of times the link was down since the last reset.
Data: IN/OUT	Number of data frames sent and received over the link since the last node, boot, or statistics reset.
Utilization: IN/OUT	Percentage of bandwidth being used.

Software Options Statistics

Function

The Software Options Statistics option shows the software options purchased and enabled in your Vanguard node.

Note

If the software image installed in your Vanguard does not support an option, you may not be able to use the option even though you correctly installed it, and it appears enabled in software Options Statistics.

Examples

Figures 7-9, 7-10, and 7-11 show examples of the Software Options Statistics screen for a Vanguard 320. Your screen may look different depending on the options purchased and enabled for your system.

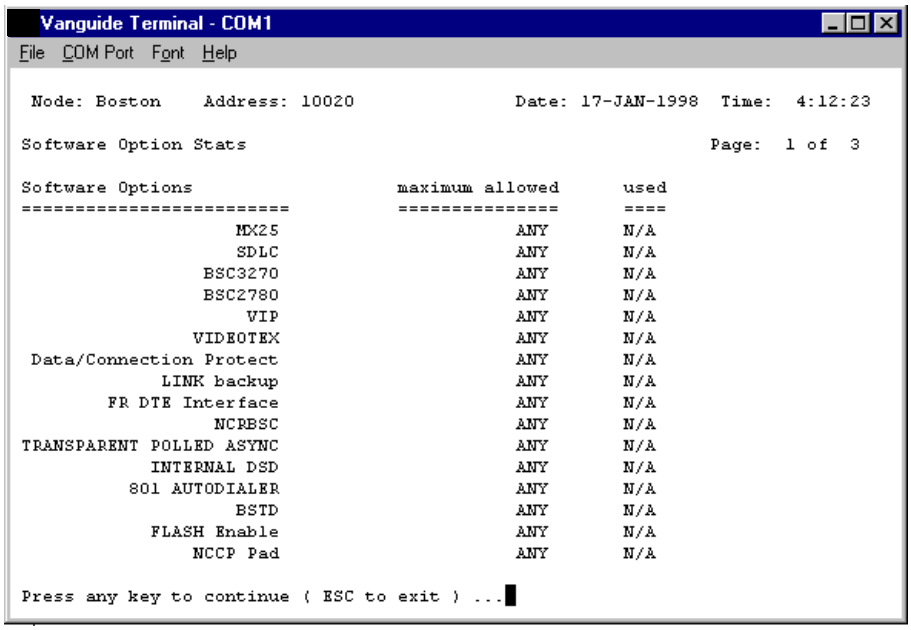


Figure 7-9. Software Options Statistics - Page 1

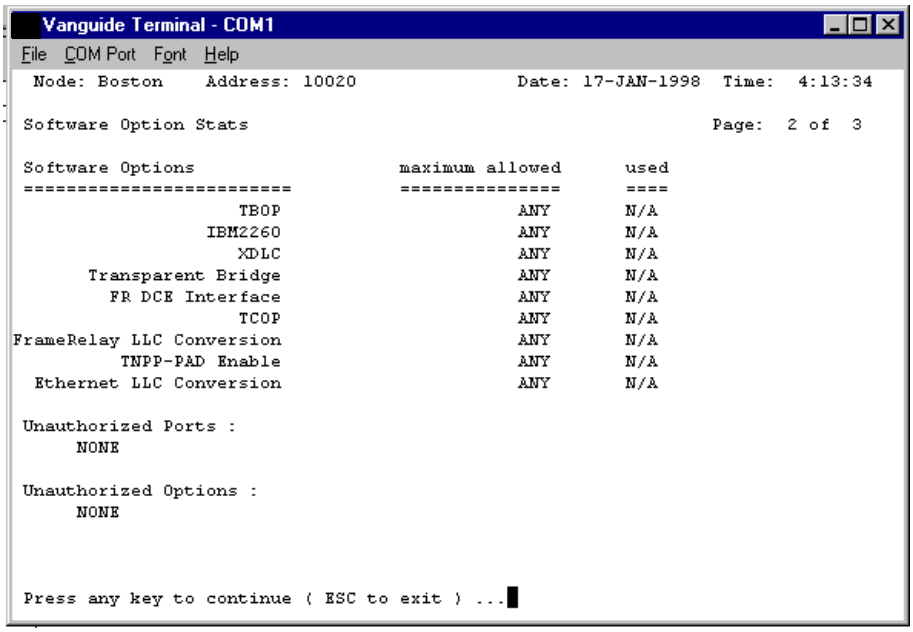


Figure 7-10. Software Options Statistics - Page 2

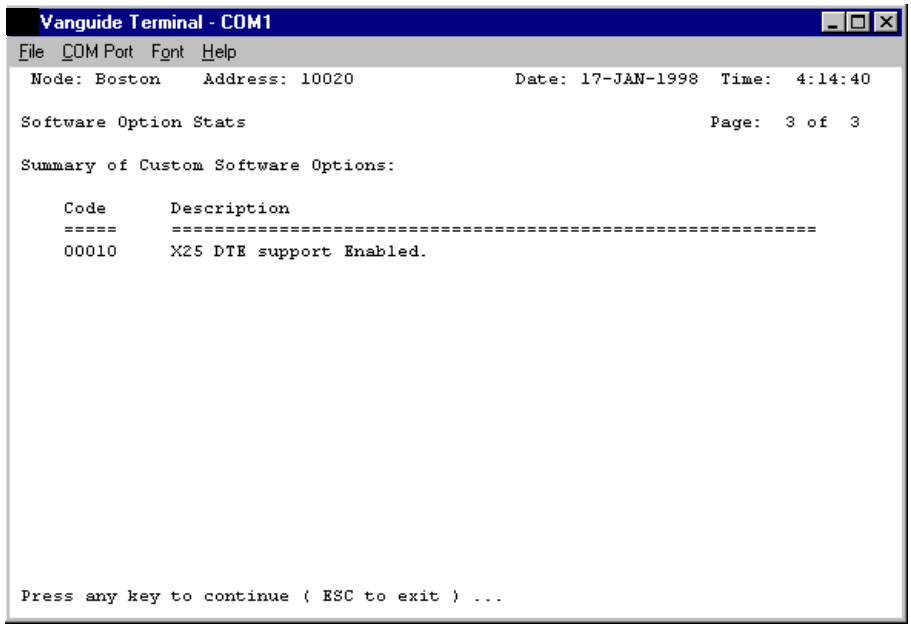


Figure 7-11. Software Options Statistics - Page 3

Description

The Software Options Statistics screen contains this information:

Screen Term	Tells You
Software Options	Type of software option.
Maximum Allowed	Number of ports that this option can support. Options can be purchased to support different numbers of ports.
Used	Number of ports actually being used with the option.
Unauthorized Ports	Indicates an attempt to use more ports than the option allows.
Unauthorized Options	Indicates an attempt to use an option that has not been purchased or enabled.

Resetting Statistics

Function

The Status/Statistics menu provides several options for resetting different statistics:

- Reset Port Statistics
- Reset All Statistics

Depending on the options you purchased and enabled, other reset statistics are available, such as Reset FRI Station Stats, Reset Internal DSD Stats, or Reset LAN Connection Stats. Refer to the appropriate feature protocols manual for more specific information.

Other Methods Of Resetting Statistics

You can also reset all the statistics by booting the node.

Guidelines for Use

You can reset only those statistics that have counters.

When you select Reset Port Statistics, the last call information from the Detailed Port Statistics screens is not cleared. Only a node boot clears this information.

Procedure

Follow these steps to reset statistics:

Step	*Action*		*Result/Description*
1	From the CTP Main menu, select **Status/Statistics**.		The Status/Statistics menu appears.
2	***If You Want To Reset...***	***Select***	***Result***
	Port statistics	**Reset Port Stats**.	A prompt appears to identify the correct port.
	All the statistics	**Reset All Stats**.	A prompt appears to proceed or not.
3	Enter **N** (no) to stop the reset process. Or: Enter **Y** (yes) to initiate the reset process.		

Chapter 8
What To Do If Something Goes Wrong

Display Alarms First

Introduction

When you are troubleshooting a problem with your Vanguard, the first thing you should do is look at the alarms generated by the node. This chapter shows how to set up an alarm/event log and how to view alarms and events.

How to Set Up Event Logging

Follow these steps to set up alarm/event logging in the unit .

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Configure -> Node**.	The Node record appears.
2	At the Alarm Selection: parameter, type **HIGH+MED+LOW+CONN** followed by a semicolon (**;**).	This sets the alarm selection to log all levels of alarms. The semicolon (**;**) saves your entry in the CMEM.
3	Press CTRL+T to return to the top menu.	The Main menu appears.
4	From the Main menu, select **Boot -> Table and Node Record**.	The **Proceed (Y/N):** prompt appears.
5	Type **Y** to boot the node.	The node resets and implements the changes you made to the node record.
6	Log back into the unit and select **Diagnostics** from the CTP Main Menu and follow the steps in the section, How to Display Event Log.	

Note

Use the CTRL+N and CTRL+O keyboard commands to control the Alarms displayed on the CTP.

How to Display Event Log

If alarm/event logging is already set up in the unit, follow these steps:

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Diagnostics -> Logged Alarms -> Display**.	The most recent logged alarms appears.

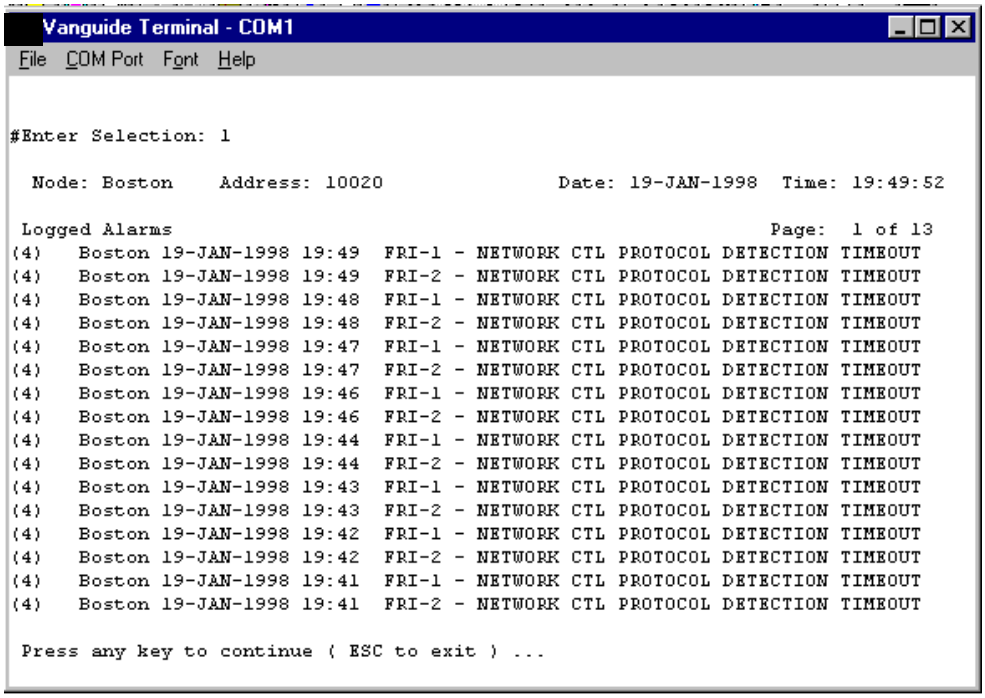


Figure 8-1. Sample Event Log

Figure 8-1 illustrates multiple alarms being generated for the same event. You can prevent this from happening by using the Trap Throttling feature. Refer to the *Vanguard Applications Ware Alarms and Reports Manual* (Part Number T0005) for details on throttling unwanted alarms and complete descriptions of all Alarms and Reports found in your release of Applications Ware. The *Vanguard Applications Ware Alarms and Reports Manual* is available on the Vanguide CD-ROM that shipped with your Vanguard product.

Check for Fatal Errors

Introduction

When there is a major problem within the Vanguard, the unit logs fatal errors. This error report needs to be interpreted by the VanguardMS Engineering Staff. Save this report as a flat ASCII text file and send it to Vanguard Managed Solutions.

With Release 6.1 or greater, the fatal error report (FER) holds up to 20 of the latest alarms. Prior to Release 6.1, five alarms were included.

Note

The Vanguard 7300 Series holds up to 100 alarms in the fatal error report.

Display Fatal Error Reports

Follow these steps.

Step	*Action*	*Result/Description*
1	From the CTP Main menu, select **Diagnostics -> Fatal Error Reports -> Display**.	If your Vanguard has experienced no fatal errors, the terminal appears as shown in Figure 8-2. Otherwise, the most recent fatal errors appear.
2	If fatal errors appear, save the report as an ASCII text file.	
3	Call VanguardMS Technical Support to inform them of the problem and where to send this gathered information.	

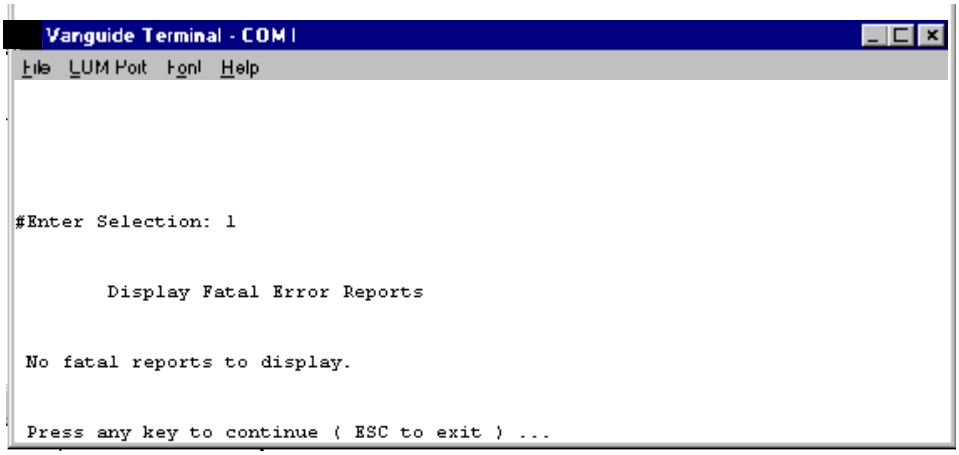


Figure 8-2. Fatal Error Report

Note

Besides the Fatal Error Report, Vanguard Managed Solutions Engineering also requires the Logged Alarms Report, Node Statistics, and the CMEM file for the node that crashed.

Fatal Error Report Node Statistics

Release 6.1 and greater now includes the node statistics in the Fatal Error Report. The major sections of the Fatal Error Report are as follows:

- Crash Information
- DES File
- Alarms
- Node Statistics at the time of the crash
- The CMEM file at the moment of printing the FER

Problem with a Frame Relay Port

Introduction

Follow these steps to troubleshoot a problem with a frame relay port.

Step	Action
1	Determine if there are any alarms associated with this Frame Relay port by displaying the Logged Alarms.
2	Display the Detailed Link Statistics, shown in Figure 8-3.

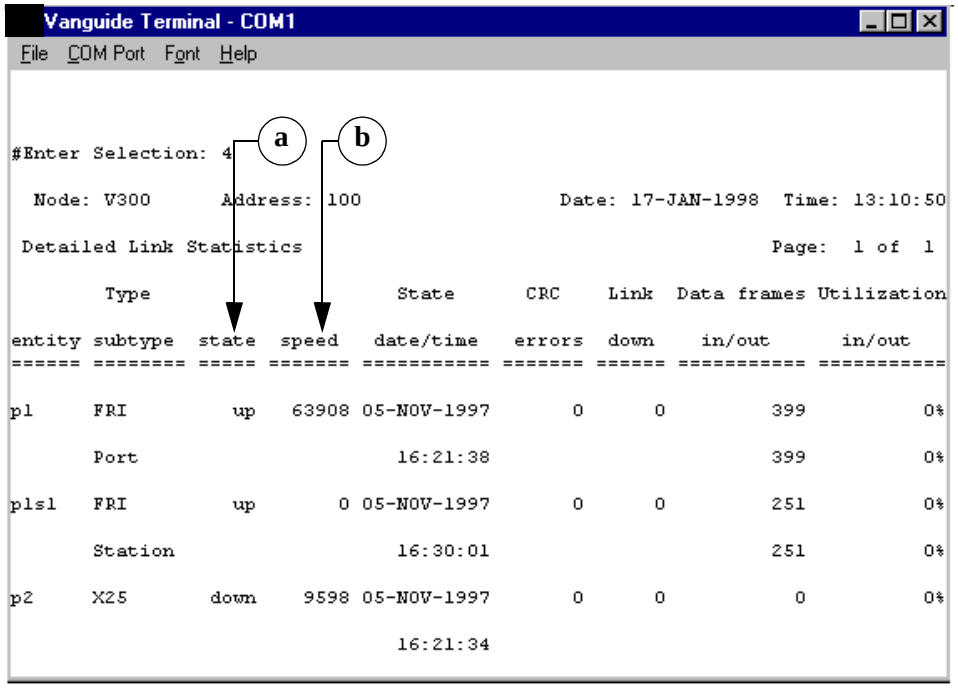


Figure 8-3. Detailed Link Statistics Screen

ⓐ A state of “up” for the Port state indicates the port hardware is operational and the port has not been disabled. A state of “up” for station means the Annex G station has established the X.25 link to the Annex G station at the other end of the link. This means that WAN connectivity is correct for this FRI port and the DLCI associated with the “up” station. This should read “up” at both ends of the circuit.

ⓑ The Speed column does not have significance for a FRI Station. If the port is set to external clocking and there is a speed value listed for the FRI Port, then the port, cable, and transmission device are probably functioning properly.

Step	Action *(continued)*
3	Display the Detailed Frame Relay Port Statistics, shown in Figure 8-4.

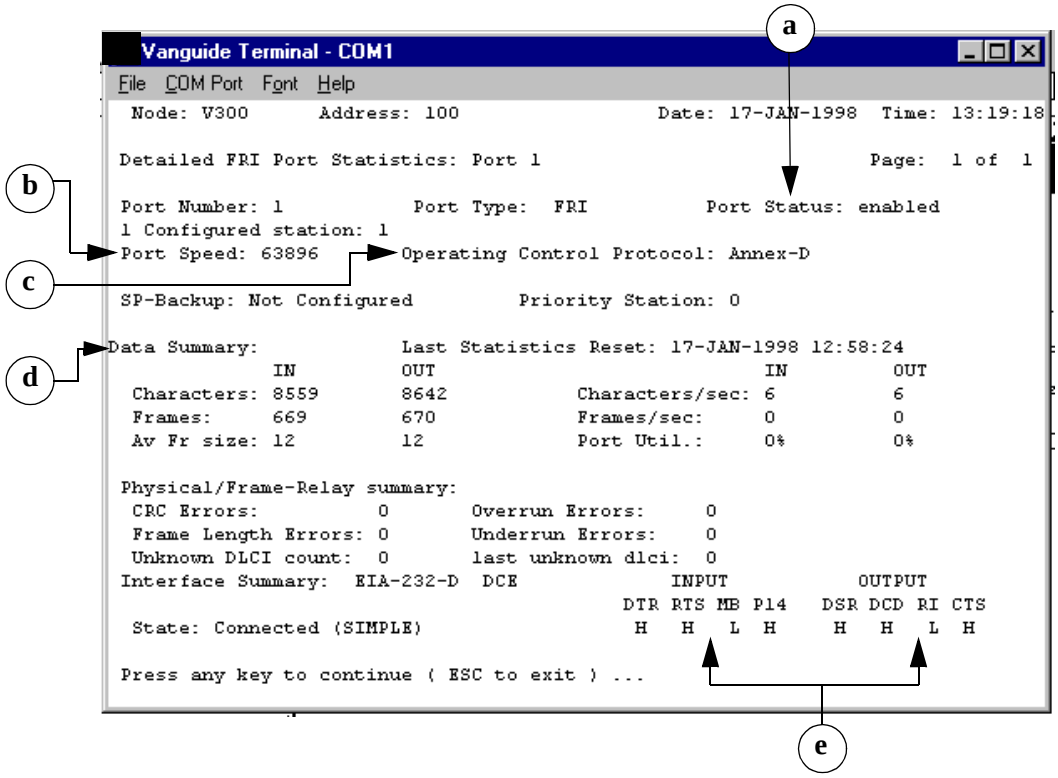


Figure 8-4. Detailed FRI Port Statistics Screen

ⓐ Port Status -

- Enabled: This is the normal state for the port.
- Disabled: The port has been disabled. Enable the port through the Port/ Station/Channel Control Menu.

ⓑ Port Speed - A port speed of 0 indicates that there is no clock/timing source. The port is misconfigured or inoperative (if the port was supposed to provide link clocking) or the attached device/cable is inoperative.

ⓒ Operating Control Protocol - indicates the control protocol being used if the link is up. If the link is not up, then this lists the configured control protocol. Auto indicates that the port is trying to learn the type of control protocol being used on the link. If it stays in the Auto condition, this value indicates a bad cable or a transmission device to the link has not been set up for a control protocol.

ⓓ Data Summary - Proper operation indicates that the In and Out counters are incrementing. Type CTRL+R to refresh the screen. If there is a count in the Out column but not in the In column, then this is often an indication that the Control Protocol is configured incorrectly. (The network is expecting Annex D and this unit is sending LMI.) If the Control Protocol is incorrectly configured, then there should be Alarms indicating that the Control Protocol Error Threshold has been reached.

ⓔ Control Signals - If the INPUT signals (DTR, RTS, MB, P14) are “L”, then this indicates that the attached device/cable are inoperative, the port on this unit is inoperative, or (if this is a DIM port) that the DIM is in the wrong position and/or the DIM is the incorrect interface type.

Step	***Action*** *(continued)*
4	Display the FRI Station Statistics, shown in Figures 8-5 and 8-6.

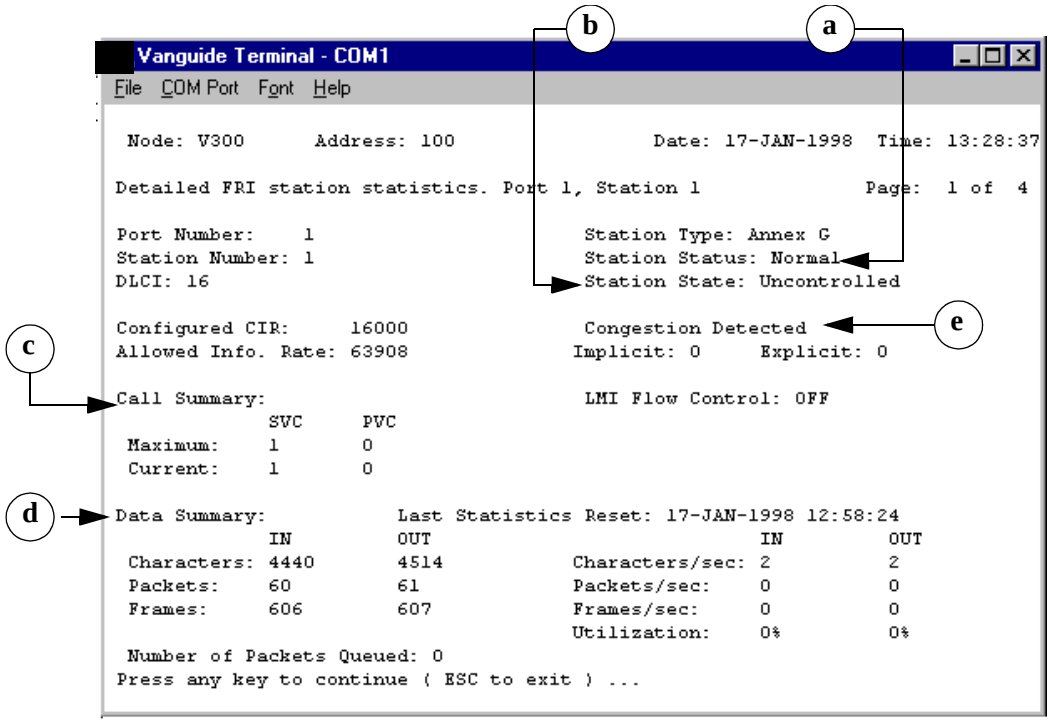


Figure 8-5. Detailed FRI Station Statistics - Page 1

ⓐ Station Status - Indicates the status of this FRI Station.

- Active: The normal state of the FRI Station.
- Link Setup: The (Annex G) X.25 link between this station and the FRI Annex G station on the other end of the link has not been established. In new installs or additions this is often caused by the FRI Station parameter Link Address being set to the same value in both directions. This may also indicate a problem with the frame relay link. Often this is a problem with the configuration of the FRI port Control Protocol parameter. In established networks, this is an indication that the frame relay network or the distant end node is having problems.

ⓑ Station State - Indicates if the station has experienced the receipt of any BECNs or has lost a transmitted frame.

- Uncontrolled: This is the normal state: no BECNs or lost frames.
- Unused: The station is disabled. Go to the Port/Station/Channel Control menu and enable the station.

ⓒ Call Summary - Any number other than 0 indicates that the port and station are configured correctly and that the frame relay link was or is operational.

ⓓ Data Summary - Values being incremented in the In and Out fields indicates that there is traffic in both direction and that the logical frame relay link and control protocol are operational. If data is going out but is not being received, then this often indicates a control protocol mismatch.

ⓔ Congestion Detected - Explicit indicates congestion due to BECN. Implicit indicates Lost Frames.

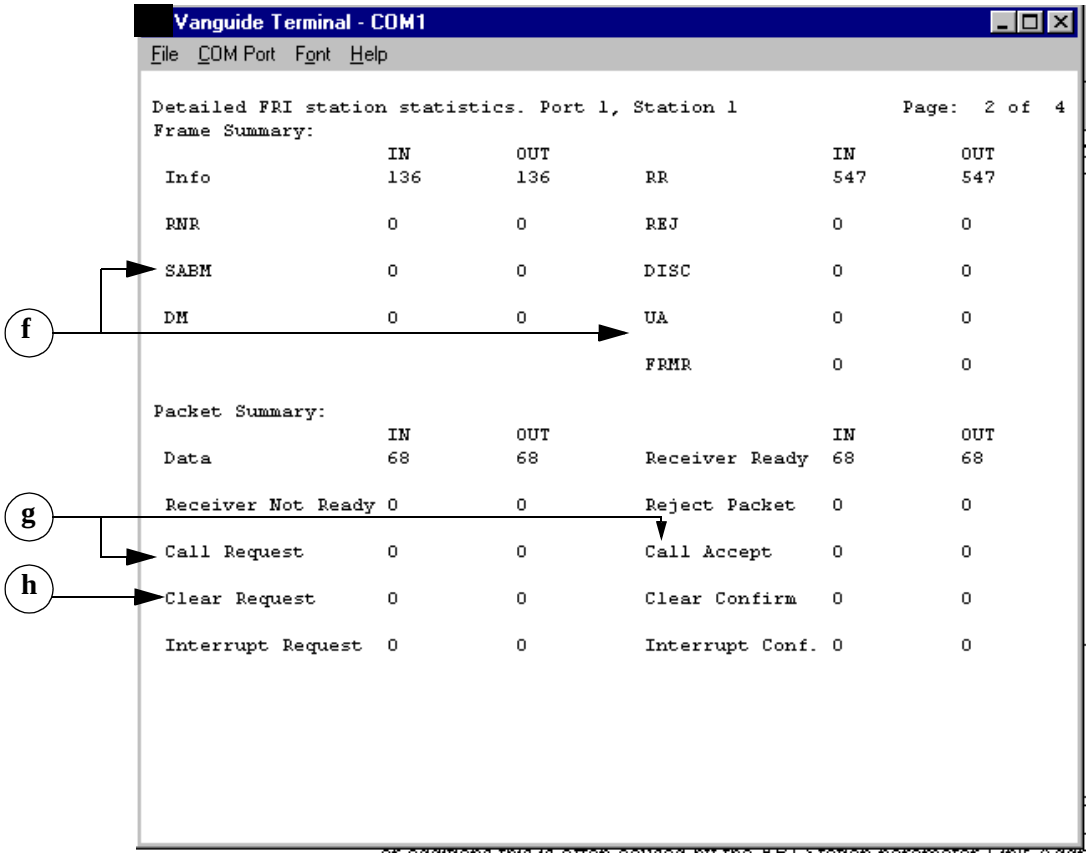


Figure 8-6. Detailed FRI Station Statistics - Page 2

ⓕ SABM/UA - In normal operation there should be one or more SABMs sent out and at least one UA received (there may also be SABMs and UAs in the opposite directions).

If there are only SABMs going out, but no UA responses, this indicates that the Annex G station on the other end of the WAN is not responding. Often this is a Link Address configuration error in the FRI station configurations or a Frame Relay Network problem.

ⓖ Call Request/ Call Accept - In normal operation there should be one or more Call Request/ Call Accept exchanges. If the call to establish the connection is supposed to be generated from this node, and there is a count in the Call Requests Out column, but not in the Call Accept In column, then a portion of the configuration to generate the call request is correct, but there still may be other configuration errors in the originating node that may be unrelated to routing the call.

ⓗ Clear Request - This indicates rejections by this unit (Out column) or other units (In column) of Call Requests. If the In column has a count, this indicates that calls are getting to another node. It also indicates that the node at the other end of the link is rejecting the received Call Request because of insufficient resources in the receiving node. The insufficient resources may simply be that the call destination is busy. The busy condition may be normal based on network design criteria and how the application is specified to function. The rejected received Call Request may indicate a configuration error in either node.

If there are no counts in the In column and the link is not functioning, then this indicates that the Call Requests are getting lost in the network.

Step	***Action*** *(continued)*
5	If you determine that the Frame Relay port is defective, then before replacing the node, save the configuration onto your PC and be sure to restore this saved configuration back on to the new node.

Problem with an X.25 Port

Introduction

Follow these steps to troubleshoot an X.25 port problem.

Step	Action
1	Determine if there are any alarms associated with this X.25 port by displaying the Logged Alarms.
2	Display the X.25 Port Statistics, shown in Figures 8-7 and 8-8.

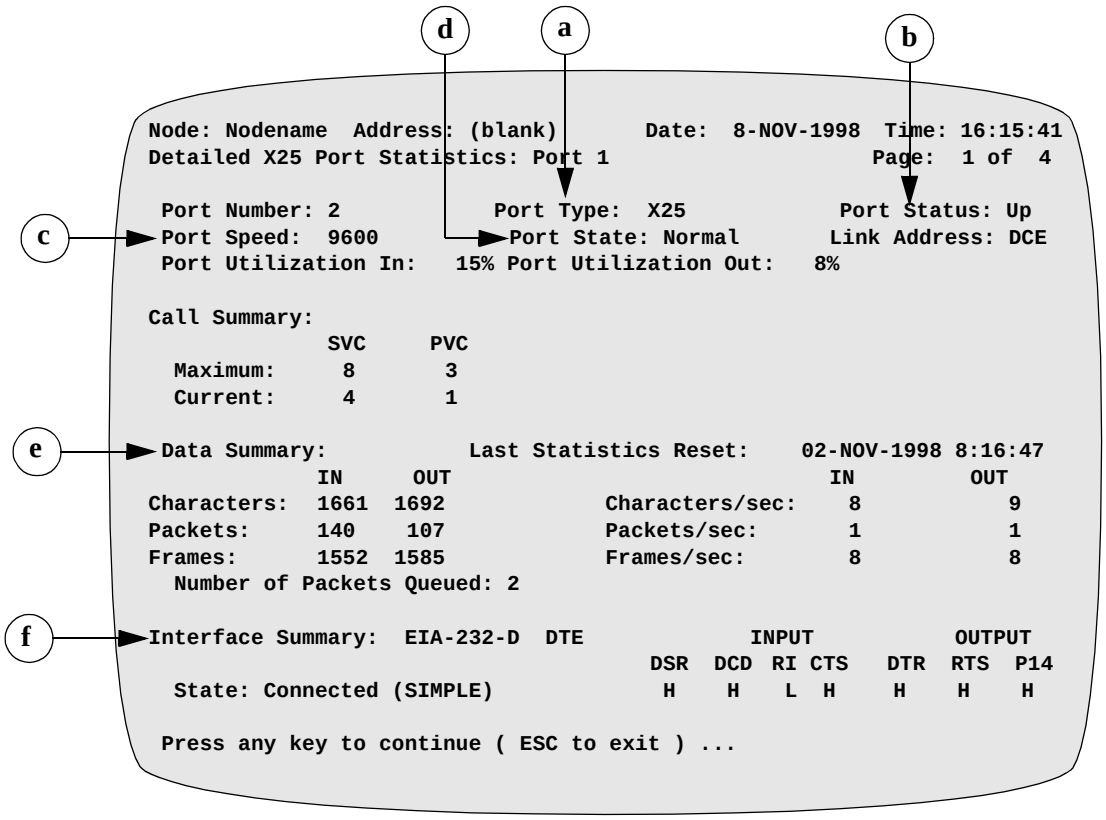


Figure 8-7. X.25 Port Statistics Screen - Page 1

ⓐ Port Type - identifies the type of port.

ⓑ Port Status -

- Up: identifies the port as active.
- Down: indicates that the port does not see inbound EIA signals. Check the cable and attached equipment for proper operation. This could also signify a carrier service problem or a problem with the equipment at the remote end of the circuit.

ⓒ Port Speed - identifies the speed of the link. Most X.25 ports use an external clock. If this is the case, then the speed of the clock that is being supplied is displayed in this field. If this value is 0, then no clock is being supplied on the link.

ⓓ Port State -

- Disabled: The port has been disabled. Enable the port through the Port/Station/Channel Control Menu.
- Busy Out: The port has been busied out. Enable the port through the Port/Station/Channel Control Menu.
- Remote Busy: The port is receiving RNR frames from the remote unit. This is a flow control mechanism indicating that the remote node cannot accept data.
- Send_rej: This port is sending REJ frames for bad frames. Check the line for problems such as CRC or Non-Octet Aligned Errors.
- Normal: The link is able to pass data. This is the normal state of the port.
- Link Setup: The port is sending SABM frames and is waiting for a UA response frame in order to establish the link connection. If a port stays in this state, then check the modems to see if the modems have carrier and that the lines are clean and connected end-to-end. Also, check the DCE-DTE link address to make sure it is set properly.

ⓔ Data Summary - Identifies that data is passing through the port. If these parameters are not incrementing (using the Control R keyboard command), then verify the Port Status and Port State.

ⓕ Interface Summary - Identifies the status of the identified control signals.

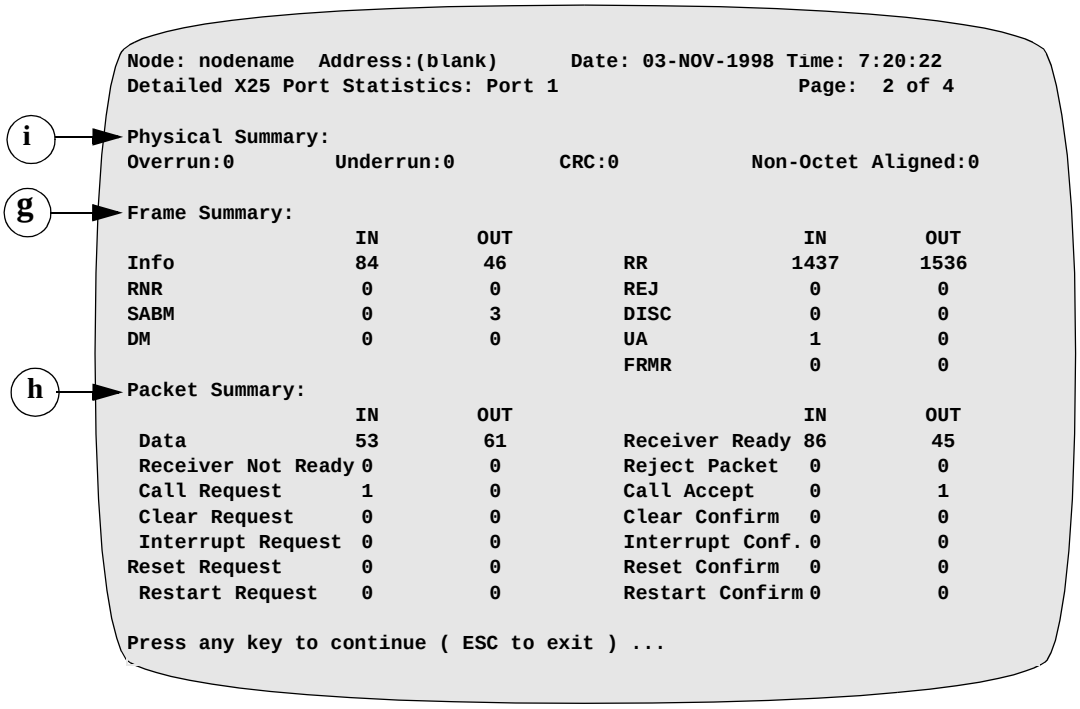


Figure 8-8. X.25 Port Statistics Screen - Page 2

ⓖ Frame Summary - Identifies the type of frames that have been transmitted and received by this port. IN refers to frames received by the port. OUT refers to frames being transmitted out of this port. In order to establish an X.25 link, there must be an exchange of SABM and UA between the devices. Without establishing the Frame Layer, the Packet Layer cannot be established.

ⓗ Packet Summary - Identifies the type of packets that have been transmitted and received by this port.

ⓘ Physical Summary - Identifies any framing problems associated with the physical connection. Overrun identifies number of lost frames. Underrun means number of transmission frames lost. Not all frames were sent to the network port. CRC and Non-Octet Aligned probably identify problems caused by the transmission line.

Step	Action *(continued)*
3	Display the Detailed Link Statistics, shown in Figure 8-9.

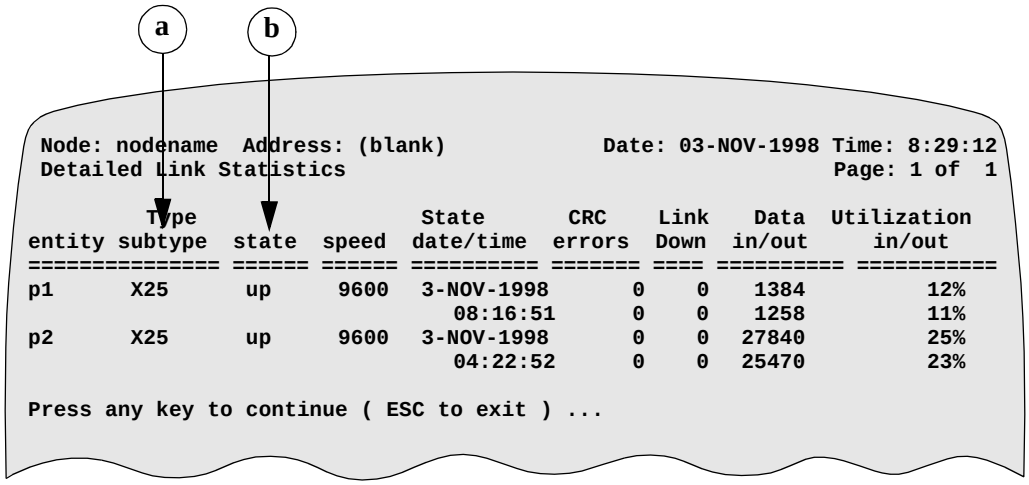


Figure 8-9. Link Statistics Screen

ⓐ Type/Subtype - Defines the type of link.

ⓑ State -

- Up: The normal state of the link.
- Down: The port is not operational.
- Disabled: The port has been disabled, go to the Port/Station/Channel Control Menu and enable the port.
- Busy-Out: The port has been busied out. Go to the Port/Station/Channel Control Menu and enable the port.

Step	Action *(continued)*
4	If you determine that the X.25 port is defective, then before replacing the node, save the unit's configuration to your PC disk and restore this saved configuration back on to the new node.

Problem with an Ethernet Port

Introduction

Follow these steps to troubleshoot problems with an Ethernet port.

Step	Action
1	Determine if there are any alarms associated with this Ethernet port by displaying the Logged Alarms.
2	Display Port Stats for the Ethernet Port, shown in Figure 8-10.

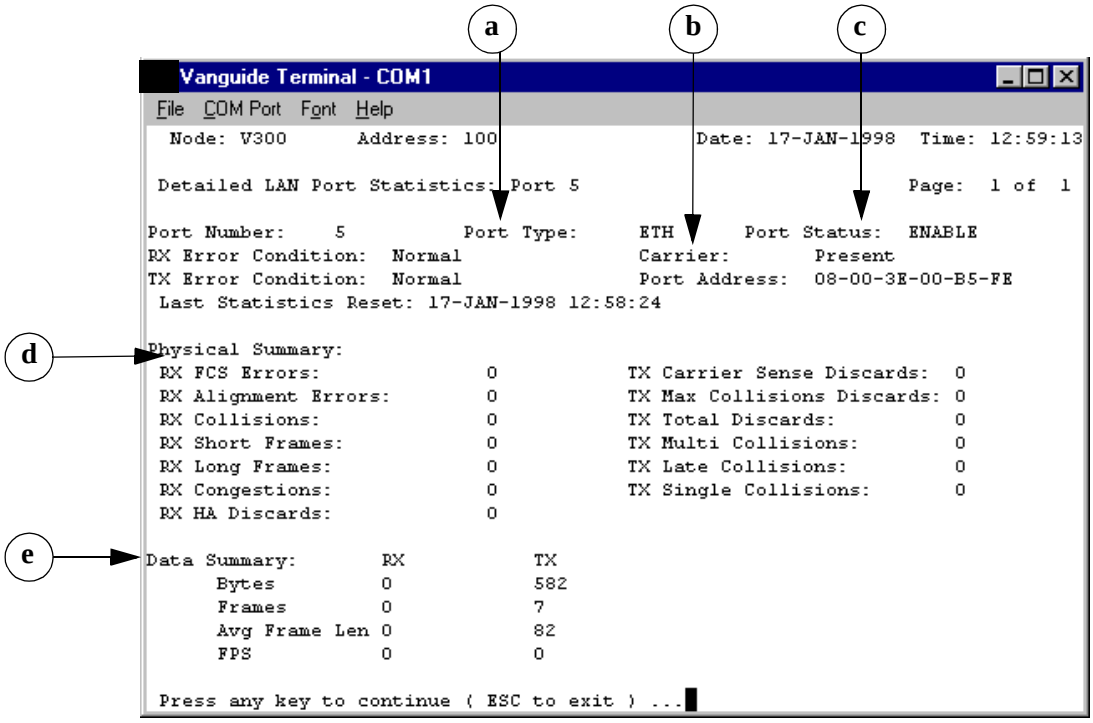


Figure 8-10. Detailed LAN Port Statistics Screen

ⓐ Port Type - The normal setting is ETH for an ethernet port.

ⓑ Carrier -

- Present: The normal state of the carrier.
- Anything else: Check the physical connection between the ethernet port of this device and the LAN connection.

ⓒ Port Status -

- Enable: The normal state of the port.
- Disable: The port is disabled. Go to the Port/Station/Channel Control Menu

and enable the port.

ⓓ Physical Summary - Reset the port statistics through the Reset Port Stats selection in the Statistics menu. Check the physical summary for rapid increments of any particular parameter by using the CTRL+R keyboard command.

Note

RX HA Discards are identified as local frames which did not require any processing by the unit. These are used to communicate between devices which are on the same Ethernet segment as this Ethernet port. This does not imply that there is a problem.

ⓔ Data Summary - The normal state is for the values to be incrementing. Monitor this by using the CTRL+R keyboard command. If these values do not increment and everything else on this screen appears to be in proper operation, then contact Vanguard Managed Solutions Technical Support for further assistance.

Step	***Action*** *(continued)*
3	If it is determined that the Ethernet Port is defective, then before replacing the node, save the configuration to your PC diskette and restore this saved configuration back on to the new node.

Appendix A
Configuring a Node

Overview

Introduction

This appendix describes the Node record:

- A general description of the Node record and its parameters
- Features that are implemented by configuring certain parameters in the Node record including:
  - Table size
  - Billing
  - Data Connection Protection
  - Traffic Priority
  - Broadcast
  - Addressing and Address Blanking
  - Memory Management
- Descriptions of the thresholds that monitor overload situations

Node Record

What You See in This Record

The Node Record contains parameter values that define the node characteristics. It specifies many key node values, including node name, address, alarm thresholds, and timers.

Figure A-1 shows the parameters available from a default Node record.

Note

An asterisk (*)denotes that you must perform a node boot for changes to the parameter to take effect.

Figure A-1. Example of Node Record

CTP Banner Message

You can specify a banner message to be displayed when users log on to your system. The message is displayed after the user enters their user name and before they are prompted for their password. The banner message can be up to 320 alpha/numeric characters long.

To create a banner, follow the steps below.

Step	Process
1	Select Configure from the main window.
2	Select Node.
3	Enter the Node name, in this case E1_7_1_S.
4	Press RETURN until you see the Login Banner field as in Figure A-2.

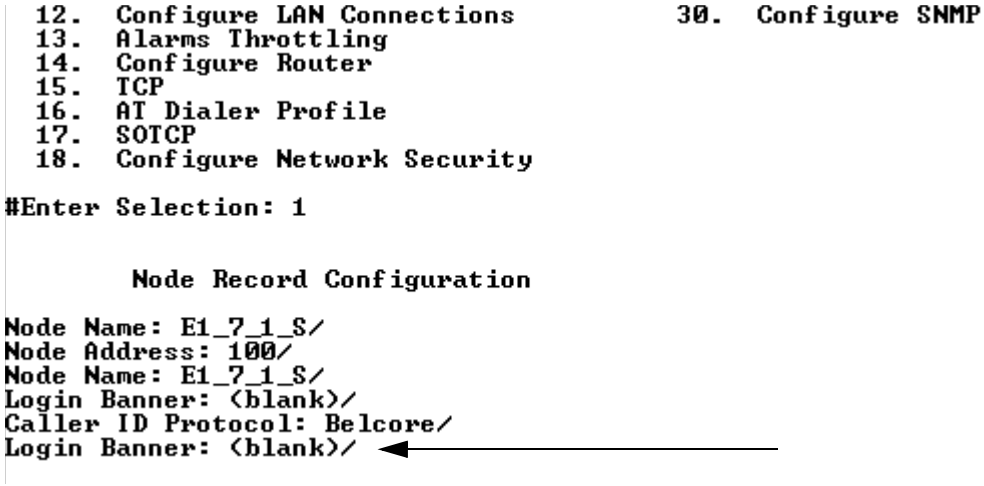


Figure A-2. PAD Bulletin Message Field

Step	Process
5	Enter the message, up to 320 alpha/numeric characters long, and press RETURN. **Note** If there is a message present you can delete it by pressing the SPACE bar. **Note** You can save a record or records by pressing the semi-colon and RETURN keys.
6	Continue to press RETURN to view other fields or press the Esc key to exit Node Configuration.
7	If you have not saved a record or records by pressing the semi-colon and RETURN keys, when you press the Esc key the system prompts Save changes to table entry? <y/n>.
8	Type y to save changes or n not to save changes.

Configuring the Node Record

Before You Begin

Before you can configure parameters, you must log on to the node's Control Terminal Port.

Steps to Configure the Node Record

Follow these steps to access the Node Record:

Step	*Action*	*Result*
1	From the CTP Main menu, select **Configure**.	The Configure menu appears.
2	Select **Node** from the Configure menu.	The first parameter appears: Node Name, as shown in Figure A-1.
3	Enter parameter value, then press semicolon (;) when you finish.	This saves your changes to the Node record.
4	Press ESC.	The Configure menu appears.

Implementing Changes to Record Parameters

Follow these steps to implement changes to a record after entering parameter values:

Step	*Action*
1	Select **Boot** from the CTP Main menu.
2	Select **Table and Node Record** from the Boot menu.

Node Record Parameters

Introduction

This section describes the Node Record parameters. Any parameter preceded by an asterisk (*) requires a Node Boot to implement changes.

Note

If you have enabled Ease of Configuration, you need to boot only the port to make changes to the parameters marked with an asterisk. For more information on Ease of Configuration refer to the introductory section of the *Basic Protocols Manual*, Part Number T0106.

Parameters

These are the Node Record parameters:

Node Name

Range:	0 to 8 alphanumeric characters
Default:	Nodename
Description:	Unique name that identifies the node and tops control terminal port menus; the name appears on alarms and billing records. **Note** Use the space bar to blank the parameter.

Node Address

Range:	0 to 13 decimal digits
Default:	(blank);
Description:	Specifies the main part of the network address for calls destined within the node: PAD port or node resource calls. The individual subaddresses specify the exact destination. You must enter a *unique* value for Node Address and Node Number for each node in a network. This parameter indicates the main part of the network address for this node: • Incoming calls with this Node Address as the first part of the network address are routed to this node. • The network-address subaddress (Control Port Subaddress) routes the incoming call to a specific node destination. **Note** If you enter a (blank) value, the node accepts all incoming calls and attempt to route the call to one of its resources according to the call's subaddress.

Node Number

Range:	0 to 65535
Default:	0
Description:	Specifies a unique number identifying the node for network routing. Every node in your network must have a unique node number.

Chassis Type

Range:	Standalone, Modulus 8, Modulus 18, Modulus 9, Modulus 21, 6520, 6560
Default:	6520
Description:	Specifies the node chassis. This is necessary to interpret the fan and power supply signals correctly. ■ **Note** Appears only for Vanguard 6520/6560.

Maximum Routing Hops

Range:	2 to 15
Default:	15
Description:	Specifies the maximum number of nodes (Internodal Links) through which a call may pass enroute to its destination. ■ **Note** The value entered for this parameter should be no greater than the number of nodes in the longest path across the network.

Maximum Routing Hops For Voice

Range:	1 to 10
Default:	2
Description:	Specifies the maximum number of hops that a voice call can pass through before it reaches its destination.

Hop Count Facility Code

Range:	200 to 254
Default:	200

Hop Count Facility Code *(continued)*

Description:	Specifies the facility used in call packets on X.25 links with the INL option set for network routing. **Note** Change this parameter value only when it interferes with another private network facility.

Control Port Subaddress

Range:	0 to 3 decimal digits
Default:	98
Description:	Specifies the control terminal port subaddress for this node. Incoming calls with a network address (consisting of the Node Address and this Control Port Subaddress) arrive at this node's control terminal port. A Routing Table entry is not needed. **Note** Changing this parameter is not recommended.

Control Port Idle Disconnect Time (minutes)

Range:	1 to 255
Default:	10
Description:	Specifies how many minutes of inactivity can occur before the control terminal port disconnects the connection.

Alarm Distribution

Range:	NONE, CTP, PRIN, LOG
Default:	CTP
Description:	Specifies where alarm and event reports are sent: • NONE: Sends no alarm. • CTP: Sends alarms to Control Terminal Port. • PRIN: Sends alarms to a printer, terminal, or personal computer as specified by the parameter Alarm Printer Mnemonic. **Note** Use summing to combine several parameter values, for example, CTP+PRIN.

Alarm Printer Mnemonic

Range:	0 to 8 alphanumeric characters
Default:	(blank)
Description:	Specifies the mnemonic name for the destination of alarms sent by the node (if Alarm Distribution = PRIN). If you specify an Alarm Printer Mnemonic, you must have a corresponding entry in the Mnemonic Table record. **Note** Use the space bar to blank the parameter value and prevent any alarms from being sent.

Alarm Selection

Range:	NONE, HIGH, MED, LOW, CONN, CODE
Default:	HIGH
Description:	Specifies alarm and event types the node reports: • NONE: No alarms reported • HIGH: High-severity alarms reported • MED: Medium-severity alarms reported • LOW: Low-severity alarms reported • CONN: Connection events reported • CODE: Alarms from Codex 6000 communications processors reported • DEBUG: Alarms generated for debugging purposes **Note** Use summing to combine several parameter values, for example HIGH+MED.

Threshold Alarm Timer (minutes)

Range:	15 to 255
Default:	15
Description:	Specifies the time the node waits before sending the same threshold alarm report again. **Note** Set this parameter to a high number to prevent an alarm from generating an excessive number of reports.

Broadcast Port Subaddress

Range:	0 to 3 decimal digits
Default:	95
Description:	Specifies the broadcast port subaddress for this node. Incoming broadcast messages with a network address (consisting of the Node Address and this Broadcast Port Subaddress) arrive at this port in this node. Use the mnemonic BCST as the source or destination connection in the PVC Setup Table for routing to the Broadcast Module; no Routing Table entry is needed. **Note** Use the space bar to blank the parameter.

***Number of Broadcast Nets**

Range:	0 to 100
Default:	0
Description:	Specifies the number of Broadcast Networks to which this node can send broadcast messages. **Note** Set to zero (0) to disable the Broadcast function. **Note** You must perform a Node boot for changes to this parameter to take effect.

***Number of Broadcast Input Channels**

Range:	0 to 10
Default:	1
Description:	Specifies the number of simultaneous call connections permitted to the broadcast port at one time. **Note** You must perform a Node boot for changes to this parameter to take effect.

***Billing Printer Mnemonic**

Range:	0 to 8 alphanumeric characters
Default:	(blank)
Description:	Specifies the mnemonic of the printer or personal computer port to which the node sends billing records. If you specify a Billing Printer Mnemonic, you must have a corresponding entry in the Mnemonic Table record. **Note** This parameter configures a mnemonic table entry for the printer or personal computer port. **Note** Use the space bar to blank the parameter.

***Billing Record Call Threshold**

Range:	1 to 99
Default:	10
Description:	Specifies the number of billing records that can be queued before they are sent to the logging device. When the number of billing records equals the threshold, a call is placed to the logging device to dump the billing records.

Maximum Billing Records

Range:	0 to 512
Default:	100
Description:	Specifies the maximum number of billing records the node stores if the logging device cannot receive the records for printing. **Note** After the number of records exceeds this value, new records are deleted from the buffer.

***Billing Record Timer (minutes)**

Range:	0 to 65535
Default:	0
Description:	Specifies how long billing records are stored before they are automatically sent to a logging device for printing. Setting this parameter value to 1440 (24 hours), for example, causes internally stored records whose number has not reached the Billing Record Call Threshold to be printed every 24 hours.

PVC Billing Record Timer (minutes)

Range:	0 to 65535
Default:	0
Description:	Specifies how long billing records for PVCs (with billing activated) are stored before they are sent to a logging device for printing. Setting this parameter value to 1440 (24 hours), for example, generates billing records every 24 hours.

SVC Billing Record Timer (minutes)

Range:	0 to 65535
Default:	0
Description:	Specifies how long billing records for all SVCs (with billing activated) are stored before they are sent to a logging device for printing. When this parameter is set to a value other than zero, the collect parameter is printed as part of the billing record. This indicates that the billing record being printed is the first, last, or intermediate record during the time set by SVC Billing Timer parameter. It prints as a hexadecimal value, for example: • If bit 4 is set, this is the first record during this time interval (example: 18H). • If bit 5 is set, this is the last record during the time interval (example: 28H). • If bits 4 and 5 are set, this is the only record during this time interval (example: 38H). • If bits 4 and 5 are not set, this is an intermediate record during this time interval (example: 08H). **Note** Setting this parameter value to 0 disables Periodic Billing.

***Maximum Simultaneous Calls**

Range:	0, 1 to 2000
Default:	100
Description:	Specifies the maximum number of simultaneous calls in the node. Set this parameter to zero (0) for unlimited simultaneous calls. Limiting the number of simultaneous calls eliminates data loss in extreme traffic conditions. **Note** If you configured the maximum number (4096) of Switched Virtual Circuit (SVC) channels on the Port record for the corresponding X.25 port, set the Maximum Simultaneous Calls parameter to zero (0) to support an unlimited number of calls.

Port Utilization Threshold (%)

Range:	10 to 99
Default:	75
Description:	A percentage of the port's capacity specifying how much data traffic can be handled relative to port speed before triggering a medium-severity alarm. **Note** Refer to the *SNMP/MIB Management Manual* (Part Number T0106-04), and the *Alarms and Reports Manual* (Part Number T0005) for information on customizing the severity levels of alarms.

Buffer Utilization Threshold (%)

Range:	10 to 99
Default:	75
Description:	Specifies the percentage of the buffer that can be used before triggering a medium-severity alarm. **Note** Refer to the *SNMP/MIB Management Manual* (Part Number T0106-04), and the *Alarms and Reports Manual* (Part Number T0005) for information on customizing the severity levels of alarms.

CPU Utilization Threshold (%)

Range:	10 to 99
Default:	75
Description:	Specifies the percentage of the CPU that can be used before triggering a medium-severity alarm. **Note** Refer to the *SNMP/MIB Management Manual* (Part Number T0106-04), and the *Alarms and Reports Manual* (Part Number T0005) for information on customizing the severity levels of alarms.

Port Error Threshold

Range:	1 to 255
Default:	10
Description:	Specifies number of port errors (such as parity or framing) that can be detected before triggering a medium-severity alarm. **Example:** If set to 10, an alarm is sent when 10 errors are detected; another alarm is sent when the 20th error is detected, and so on. **Note** Refer to the *SNMP/MIB Management Manual* (Part Number T0106-04), and the *Alarms and Reports Manual* (Part Number T0005) for information on customizing the severity levels of alarms.

PAD Bulletin Message

Range:	0 to 255 alphanumeric characters
Default:	(blank)
Description:	Specifies the message that appears when a terminal connects to a PAD port and enters Command Mode. This is only effective on PAD ports configured with: • PAD Profile parameter #6 • Service Signals Control set to 9 (extended service signals) or 13 (all service signals) Use these special characters to display the PAD Bulletin Message. If the character following the % symbol is not a special character, both the % and the next character are discarded. • A: Node address • C: Channel number • G: Group subaddress • N: Node name • P: Port number • S: Subaddress • T: Time • V: Software revision Enter the caret (^^) twice (it is discarded otherwise) as an escape character to tell the PAD to send control characters. The character following the caret is converted to a control character and is sent to the PAD port for output. **Note** Use the default when you do not want a message to appear.

PAD Banner Message

Range:	0 to 63 alphanumeric characters
Default:	^M^JMotorola VANGUARD (node %N) port %P(%C)^M^J
Description:	Specifies the message PAD ports send to attached terminals that enter the Command Mode. Use these special characters to display information about the PAD Banner Message. If the character following the % symbol is not a special character, both the % and the next character are discarded. • A: Node address • C: Channel number • G: Group subaddress • N: Node name • P: Port number • S: Subaddress • T: Time • V: Software revision Enter the caret (^^) twice (it is discarded otherwise) as an escape character to tell the PAD to send control characters. The character following the caret is converted to a control character and is sent to the PAD port for output.

DCP Facility

Range:	201 to 254
Default:	201
Description:	Specifies the facility code used in call request and call accept packets on X.25 links to carry DCP information at call setup and reconnection time. • Set all network nodes to the same value. • Change the default value only when it interferes with another facility. • The value must not be the same as the parameter Hop Count Facility. • Valid only if you have Data Connection Protection enabled on the node.

***Codex Proprietary Protocol ID**

Range:	192 to 255
Default:	192
Description:	Provides the Codex Proprietary Protocol ID whose value is placed in the first byte of the Protocol Identifier field of the CUD in Call Request packets for protocols assigned a standardized value by the CCITT. **Note** You must perform a Node boot for changes to this parameter to take effect.

***LAN Connection Subaddress**

Range:	0 to 3 decimal digits
Default:	94 (usually used unless it conflicts with an address already in use).
Description:	Routes calls, with a network address composed of the node address and this subaddress, to a LAN Connection in this node. **Note** You must perform a Node boot for changes to this parameter to take effect.

Contact

Range:	0 to 255 alphanumeric characters
Default:	(blank)
Description:	Identifies who is responsible for this managed node and how to contact that person. This is part of the MIB-II System group. **Note** You must perform a Node boot for changes to this parameter to take effect. **Note** Use the space bar to blank the field.

Domain Name

Range:	0 to 255 alphanumeric characters
Default:	(blank)
Description:	Specifies an administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name. This is part of the MIB-II System group. **Note** You must perform a Node boot for changes to this parameter to take effect. **Note** Use the space bar to blank the field.

Node Location

Range:	0 to 255 alphanumeric characters
Default:	(blank)
Description:	Identifies the physical node location. This is part of the MIB-II System group. **Note** Use the space bar to blank the field.

***Traffic Priority**

Range:	LOW, MED, HIGH, EXP
Default:	MED
Description:	Specifies the default traffic priority used on this node: • LOW: One Low Priority packet is sent for every Traffic Priority Step number of Medium priority packets. • MED: One Medium priority packet is sent for every Traffic Priority Step number of High priority packets. • HIGH: High is the first level of priority packets sent, if no expedite priority packets are sent. • EXP: Expedite priority packets have the highest priority and use all of the link bandwidth that they need. Any remaining bandwidth is shared by the high, medium, and low priority packets. **Note** You must perform a Node boot for changes to this parameter to take effect.

*Traffic Priority Step

Range:	1 to 65000
Default:	8
Description:	Specifies the number of packets that a higher priority queue sends (as long as it has packets queued) before one packet in the next- lower priority queue is sent. **Note** This global parameter applies to all networking links in the node. **Note** You must perform a Node boot for changes to this parameter to take effect.

*Maximum Frame Size

Range:	1620, 2200, 4096, 4590
Default:	1620
Description:	Specifies the largest datalink level frame, excluding trailers, that can be received on any LAN/WAN link on the node. An extra 70 bytes is added to this frame for header manipulations. If Ethernet frames are received which are larger than this setting then the Ethernet Port statistic RX Long Frame should be incrementing. The Maximum Frame Size parameter can be used to filter out unwanted and unexpected ethernet frames that are larger than what the network was designed. **Note** You must perform a Node boot for changes to this parameter to take effect.

VanguardMS Facility

Range:	202 to 254
Default:	202
Description:	Specifies the facility used in call packets on 6500 links for passing VANGUARD PRIVATE facilities, other than Hop Count and DCP Facilities, between 4.xx nodes. **Note** This parameter value should be the same on all network nodes. **Note** Change this parameter only if it interferes with another private network facility.

***Route Selection Table Size**

Range:	1 to 2000
Default:	16
Description:	Specifies the maximum allowable number of Route Selection Table entries. The CMEM value of this parameter determines the maximum entry number for new CMEM table entries. It may be necessary to increase this size parameter value before adding new table entries. **Note** You must perform a Node boot for changes to this parameter to take effect.

***Mnemonic Table Size**

Range: Range - 7300:	1 to 2000 Vanguard 7300 Series maximum Mnemonic Table Size has been increased from 2,000 to 8,000 with release 6.0.P02B and greater.
Default:	16
Description:	Specifies the maximum allowable number of Mnemonic Table entries. The CMEM value of this parameter determines the maximum entry number for new CMEM table entries. It may be necessary to increase this size parameter value before adding new table entries. **Note** You must perform a Node boot for changes to this parameter to take effect.

***PVC Setup Table Size**

Range:	1 to 2000
Default:	16
Description:	Specifies the maximum allowable number of PVC Setup Table entries. The CMEM value of this parameter determines the maximum entry number for new CMEM table entries. It may be necessary to increase this size parameter value before adding new table entries. **Note** You must perform a Node boot for changes to this parameter to take effect.

Inbound Call Translation Table Size

Range:	1 to 1000
Default:	64
Description:	Specifies the maximum allowable number of Inbound Translation Table entries. The CMEM value of this parameter determines the maximum entry number for new CMEM table entries. It may be necessary to increase this size parameter value before adding new table entries. **Note** You must perform a Node boot for changes to this parameter to take effect.

***Number of Network Services Channels**

Range:	0 to 10,000
Default:	256
Description:	Specifies the number of available Network Services Channels. **Note** You must perform a Node boot for changes to this parameter to take effect.

Node Switched Services Security Password

Range:	0 to 9 alphanumeric characters
Default:	(blank)
Description:	Specifies the security password used by switched services security for verification when determining if a call should be allowed to come up. **Note** You must perform a Node boot for changes to this parameter to take effect. **Note** Use the space bar to blank the field.

Maximum Calling Identifier Table Size

Range:	1 to 512
Default:	255
Description:	Specifies the maximum number of entries in the Calling Party ID Table Record. **Note** You can find the Calling Party ID Table Record under Configure Network Services Record.

***Quantity of DSP Devices**

Range:	1 to 1024
Default:	32
Description:	Specifies the maximum configured number of DSP type devices on this node. **Note** BSC3270, BSTD, IBM2260 all use DSP devices. **Note** You must perform a Node boot for changes to this parameter to take effect.

Quantity of SES Devices

Range:	1 to 1024
Default:	256
Description:	Specifies maximum configured number of SES type devices on this node. **Note** BSC3270, BSTD, IBM2260 all use SES devices. **Note** You must perform a Node boot for changes to this parameter to take effect.

Primary NUIC Data Network Address

Range:	0 to 15 decimal digits
Default:	(blank)
Description:	Specifies the Data Network Address of the primary NUIC. All NUI requests are first submitted to the primary NUIC. **Note** Use the space bar to blank field.

Secondary NUIC Data Network Address

Range:	0 to 15 decimal digits
Default:	(blank)
Description:	Specifies the Data Network Address of the secondary NUIC. All NUI requests are submitted to the Secondary NUIC in the event of the Primary NUIC being unreachable. **Note** Use the space bar to blank field.

Billing Printer2 Mnemonic

Range:	0 to 8 alphanumeric characters
Default:	(blank)
Description:	Specifies an alternate mnemonic to call and send the records to when billing records need to be printed. This location is a PC used to process billing records. **Note** Use the space bar to blank field.

E.164 format identifier

Range:	0 to 5 decimal digits
Default:	(blank)
Description:	Specifies an E.164 address. Addresses beginning with these digits are identified as E.164 format addresses. **Note** Use the space bar to blank field.

DORM Subaddress

Range:	0 to 3 decimal digits
Default:	91
Description:	Specifies the DORM Subaddress. Calls with network address composed of the node address and this subaddress are routed to the DORM in this node. **Note** No Routing Table entry is needed. **Note** Use the space bar to blank field.

Other DORM Address

Range:	0 to 15 decimal digits
Default:	(blank)
Description:	Specifies the DNA of the other DORM in this network. This parameter does not have to be configures if there is only one DORM. **Note** Use the space bar to blank field.

Number of X32 Ports

Range:	1 to 1024
Default:	50
Description:	Specifies the total number of X32 Dial-Out Ports in this network. **Note** You must perform a Node boot for changes to this parameter to take effect.

***Ring Frequency**

Range:	25Hz, 50Hz
Default:	25Hz
Description:	Specifies the ringer frequency in Hz. This is used by an FXO port to verify incoming ringer frequency. The FXO ports recognize only incoming ringer voltages that match this frequency. **Note** On the Vanguard, this also programs the frequency of the ringing signal generated by the FXS port. **Note** You must perform a Node boot for changes to this parameter to take effect.

***Voice Switching Table Size**

Range:	See Description below
Default:	16
Description:	1 to 1024 (Vanguard 320, Vanguard 305) 1 to 3000 (Vanguard 6400 Series, 6560, Vanguard 340) - Rel. 6.0 and greater 1 to 3000 (Vanguard 340 Enhanced) - Rel. 6.4 and greater 1 to 3000 (Vanguard 342) - Rel. 6.2 and greater 1 to 10,000 (Vanguard 7300 Series) - Rel. 6.0 and greater 1 to 6,000 (Vanguard 6435/6455) - Release 6.1.S100 and greater (Save your CMEM before configuring a large number of entries.) Specifies maximum permitted number of Voice Switching Table entries. The CMEM value of this parameter determines the maximum entry number for new CMEM table entries. It may be necessary to increase this size parameter value before adding new table entries. **Note** You must perform a Node boot for changes to this parameter to take effect.

***Max Switch Service Entries**

Range:	1 to 1024
Default:	200
Description:	Specifies the maximum allowable number of Switch Service entries. The CMEM value of this parameter determines the maximum entry number for new CMEM table entries. It may be necessary to increase this size parameter value before adding new table entries. **Note** You must perform a Node boot for changes to this parameter to take effect.

***LOCAL Dynamic Port Creation Heap Size**

Range:	0 to 16000000
Default:	0
Description:	This specifies the size of the special shared memory pool dedicated for Ease of Configuration. • To disable this parameter set to zero (0). • To enable Ease of Configuration, set this parameter to the maximum value. **Note** You must perform a Node boot for changes to this parameter to take effect.

***SHARED Dynamic Port Creation Heap Size**

Range:	0 to 16000000
Default:	0
Description:	This specifies the size of the special local memory pool dedicated for Ease of Configuration. • To disable this parameter set to zero (0). • To enable Ease of Configuration, set this parameter to the maximum value. **Note** You must perform a Node boot for changes to this parameter to take effect.

Number of Digits to be Omitted from CAEF

Range:	0 to 15
Default:	0
Description:	Specifies the number of digits to be omitted from the ISDN number received in a Call Address Extension Facility (CAEF) of a call request. Digits are omitted from the most significant digits of the ISDN number.

Digits to prefix in CAEF

Range:	0 to 15 decimal digits; use the space bar to blank the field.
Default:	blank
Description:	Specifies the digits to be prefixed to the ISDN number received in the CAEF of a call request. The prefix of digits takes place after omitting the specified digits from the ISDN number.

***Outbound Call Translation Table Size**

Range: Range - 7300:	1 to 1600 Vanguard 7300 Series maximum Outbound Call Translation Table Size has been increased from 1,600 to 16,000 with release 6.0.P02B and greater.
Default:	64
Description:	Specifies the maximum number of Outbound Translation Table entries. The CMEM value of this parameter determines the maximum entry number for new CMEM table entries. It may be necessary to increase this size parameter value before adding new table entries. **Note** You must perform a Node boot for changes to this parameter to take effect.

GSC Call Rate (Number of Calls per Second)

Range:	0 to 100
Default:	0
Description:	Specifies the number of calls that can be made by GSC HPAD ports for the node within a second.

Table Size

Introduction

The table size parameter in the Node Record lets you configure the size for these tables:

- Route Selection Table
- Mnemonic Table
- PVC Setup Table

Active Table Size & Configured Table Size

There is an important distinction between the configured table size and the active table size. Each table that you configure is allocated space in local memory at node boot time. This is the active table size and remains in effect until the next Node boot.

The configured table size sets the size of the active table at node boot. It also restricts the maximum entry number that you can enter when adding new CMEM table entries. It is important to configure the table size parameter slightly larger than the size required for your network.

Once the system is running, a Table and Node Record boot or the Table boot, reloads the active table with the CMEM table contents.

Boot Types

Figure A-3 shows that if you change the number of entries, you need to perform a Table boot. If, however, you change the active table size, you need to perform a full Node boot.

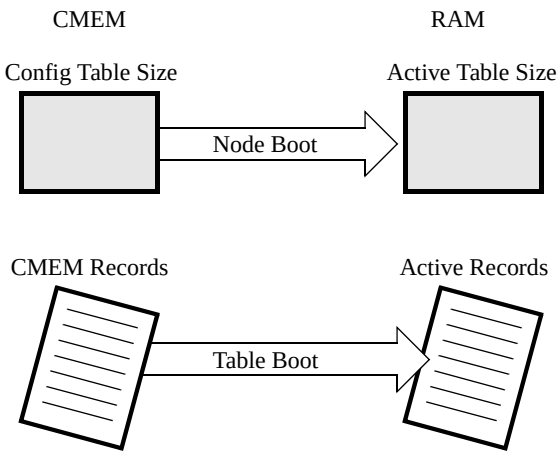


Figure A-3. Boot Types

Adding Entries

This table shows how to add table entries up to, but not to exceed, the active table size.

Step	Action	
1	Add a number of new table entries up, to the configured parameter size, in the Table record.	
	If you make a table entry	***Then***
	That exceeds the active table size	You get this warning: **Warning: Maximum number of ROUT table entries in CMEM is different than the active number of ROUT table entries. A node boot is required to activate the number of entries in CMEM.**
2	Perform a Table boot, which does not disturb connections in progress.	
	If you make a table entry	***Then***
	That exceeds the active size and you do not perform a node boot	You get this report: **Node boot required. The number of MNEM table entries in CMEM does not match the active number.**

Adding Entries that Exceed the Active Table Size

This table shows how to add table entries when you exceed the active table size.

Step	Action
1	Reconfigure the configurable table size parameter, in the Node Record, to the appropriate value and save it using the semicolon (;) key.
2	Perform a Table boot.
3	Add a number of new table entries up, to the configured table size, in the Table record.
4	Perform a Node boot; all connections are terminated and restarted.

Moving, Copying, and Inserting Table Entries

If you perform any other functions such as moving, copying, and inserting table entries, the maximum entry number permitted is the CMEM value of the configured table size parameter. If you make entries that exceed the active table size, you must perform a Node boot in order to change the active table size.

Billing

Introduction

This section explains how to configure the Billing function:

Node Record Parameters

Configure these entries in the Node record:

Parameter Name	Enter
Billing Printer Mnemonic	The mnemonic name where the billing records are sent.
Billing Record Call Threshold	The number of records to be stored before being sent to a logging device
Maximum Billing Records	The maximum number of records that you want to store. The Maximum Billing Records value must be greater than Billing Record Call Threshold.
Billing Record Timer (minutes)	The maximum length of time that a record can be stored before it must be sent to a logging device.
PVC Billing Record Timer (minutes)	The maximum length of time that a PVC record can be stored before being it must be sent to a logging device.

Mnemonic Table Entries

You must enter the mnemonic name and the address where the billing records are to be sent must be entered into the table.

Port Record Entries

Configure these entries in each Port Record:

Parameter Name	Enter
Billing Records	Set this parameter to: • On: This instructs the node to generate billing records for the port. • Off: To disable billing records for the port.

PAD Port Parameter

You also need to turn on the parameter Billing Records, which is located in the PAD Port Parameters.

When Logging Devices Are Unavailable

If the logging device port is an active connection type and the logging device is unavailable, the Vanguard products device continues to initiate a call every 10 seconds. If the call is not established within three minutes, the device waits for 30 minutes and tries again. This process repeats indefinitely.

To Disable Double Billing

Under normal circumstances, Billing Records are generated at both the Called and Calling ends of the network. This table identifies the steps to follows to disable the generation of Billing Records on PAD and X.25 ports:

Step	Action
1	Select **Configure** from the CTP Main menu.
2	Select **Software Key Table** from the Configure menu.
3	Press ENTER to access the Key Value field and enter this CSK: **SUVZ9R43F8F76A4CUU9U**
4	Boot the node.

Format of a Billing Record

The format of a typical billing record as transmitted to the output device is:

BOSTON,1234,(NONE),31-JAN-1991,10:43:29,13-0CT-1990,11:52:30, X25-1(16),X25-4 (15),123004,123004,2000006,1250,6 280,1250,6280, 160000,803840,63,00,00,04,14

The billing record consists of fields separated by commas. The fields are described in sequence in this table. The entire record is terminated by a **<CR>/Line Feed.**
This format lets you use the data in a database program.

Billing Record Parameters

This table describes the parameters available from the billing record:

Parameter	Character Length	Description
Node Name	8 ASCII	Name of Node from which the record was sent
Sequence	5 ASCII	Sequence number of the record for the originating node
Account Name	8 ASCII	Password or NUI, if used. Default is “NONE.”
Connect Date	11 ASCII	Connect date (dd-mmm-yyyy)
Connect Time	8 ASCII	Connect time (hh:mm:ss)
Disconnect Date	11 ASCII	Disconnect date (dd-mmm-yyyy)
Disconnect Time	8 ASCII	Disconnect time (hh:mm:ss)
Source	16 ASCII	Variable length string
Destination	16 ASCII	Variable length string
Called Address (before)	15 ASCII	Called address before address translation was performed
Called Address (after)	15 ASCII	Called address after address translation was performed
Calling Address	15 ASCII	Address from which call originated

Parameter *(continued)*	***Character Length***	***Description***
Packets Received	10 ASCII	Number of packets received on originating channel
Packets Transmitted	10 ASCII	Number of packets sent on originating channel
Segments Received	10 ASCII	Number of segments received on originating channel (the number of characters received divided by configured segment size)
Segments Transmitted	10 ASCII	Number of segments sent on originating channel (the number of characters received divided by configured segment size)
Characters Received	10 ASCII	Number of characters received on originating channel
Characters Transmitted	10 ASCII	Number of characters transmitted on originating channel
Clear Cause Code	2 Hex	Cause Code from the Call Clear Packet
Clear Diagnostic Code	2 Hex	Diagnostic Code from the Call Clear Packet
Facilities Used	2 Hex	Facilities used from the Call Request Packet: **BitFunction** 0Reverse Charging 1Fast Select 2Closed User Group| 3Packet Negotiation 4Window Negotiation 5NUI
General Information	2 Hex	General call information: BitFunction 0Call cleared before acceptance 1Not used 2Caller initiated disconnect 3Network initiated disconnect
Speed Indication	2 ASCII	Data rate of the source PAD port in X.3 code format. This is set to 97 if you are using a PVC and if an X.3 speed code cannot be generated because the PAD port's call cannot be completed or because the port that initiates the call is not a PAD port.

Data Connection Protection

Introduction

Data Connection Protection (DCP) lets you recover lost data packets and reroute calls around failed network links. All PAD and X.25 ports can use DCP when it is enabled.

Note

You must enable DCP on the port that originates the call and the port that receives it. Do not use the control terminal to disconnect a call that is protected by DCP. Instead, disable the port.

SAK Required for Releases prior to 5.2

Although you see the DCP parameters as part of the record, they are active only after you have purchased DCP and enabled the SAK if you are using Vanguard Applications Ware release 5.1M and earlier. Because DCP in these releases is a option, you must purchase it from yourVanguardMS representative and enable it with the SAK. If you are using Vanguard Applications Ware 5.2 and later, DCP is part of the software.

If you configured the port for DCP and enabled the SAK, the Call Summary Statistics Screen shows that the port is protected with an asterisk (*) next to the port number.

Data Protection

Data protection ensures data delivery during link outages and rerouting. Though this function can be enabled only in conjunction with connection protection, it can save data that has been lost for any number of causes. These include degraded lines where frames are lost because a link or intermediate node has gone down.

Note

DCP does not support calls to the Broadcast module.

Connection Protection

The connection protection portion of DCP acts to reestablish a call when a network link or an intermediate node fails.

Connection protection is transparent so that you do not know that the link went down. However, if only connection protection is enabled (without data protection), some data may be lost.

For rerouting to occur, be sure that the Route Selection Tables in each node in the network contain enough information so that incoming calls can be properly routed to their final destinations.

Data Connection Example

Figure A-4 shows a data connection example. Nodes B and C have DCP configured for the ports attached to the terminal and mainframe.

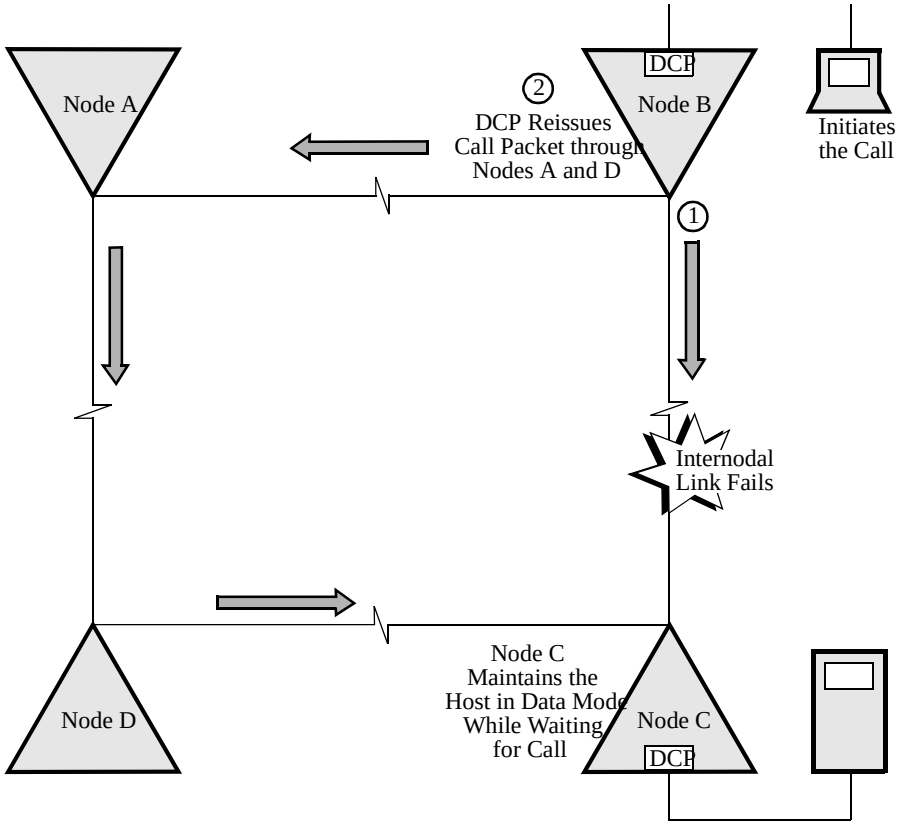


Figure A-4. Data Connection Example

Data Protection Process

This table describes how data protection works, as shown in Figure A-4.

Step	Action	Result
1	The terminal attached to Node B made an X.25 call to the mainframe connected to Node C.	• The link between Nodes B and C fails and data is lost. • X.25 sent a Clear Request to both ends of the call.
2	Once the new call was established, DCP at both nodes cooperatively entered retransmission mode. DCP reissues a call packet which Node B reroutes to Node A, through Node D, and finally to Node C, where it is sent to the port connected to the mainframe.	
	If	***Then***
	The link between Nodes B and C remained up but a data packet was lost	A Reset Request is sent to both ends.DCP at both nodes cooperatively enter retransmission mode and retransmit the missing packet.

DCP Parameters

Configure these parameters to enable DCP on your network:

Parameter	Record	Description
DCP Facility	Node Record	Indicates the module that is used to carry DCP information in Call Request and Call Accept packets at call setup and reconnection time. Leave this parameter at the default value (201) unless it interferes with another module. The DCP Facility value must not equal Hop Count Facility value.
Protection Level	In the PAD Port or X.25 Port Records	Lets you set protection for connection only, set protection for data and connection, or turn off the feature entirely.
Reconnection Timeout	PAD Port or X.25 Port Records	Specifies how long the originating node waits between reconnection attempts.
X.25 Option	X.25 Port Record	INL must be selected for X.25 networking links passing DCP data.
Reconnection Tries Limit	PAD Port or X.25 Port Records	Specifies the number of times that DCP attempts to reconnect a call before the call is cleared.

Traffic Priority

Priority Assignments By Port Type

The type of data passing on your node determines the record where you configure the priority. This table shows how priorities are assigned for all serial data protocols.

If the Port Type Is	*Assign Priority in this Record*
Async PAD	Node
Transparent Async	Node
NCR 270	Node
SDLC	Station
Transparent Bit Oriented Protocol	Node
Frame Relay (user access, FRI-DCE)	Station
X.25 (user access)	Node
3270 BSC	Station
2780/3780 BSC	Port
NRC POS (BSC)	Node
Burroughs Poll Select Sync	Node
NCR DLC	Node
LAN	LAN Connection Record

How Traffic Priority Functions

Configure these parameters before you can use the Traffic Priority feature:

- Traffic Priority
- Traffic Priority Step

The X.25, FRI-DTE, MX25, and XDLC ports use the Traffic Priority Step parameter in the Node record to specify the number of high and medium priority packets sent before transmission of any lower priority packets.

For example, if you configure the traffic priority step parameter as 3, then three high priority packets are sent before one medium priority packet. Three more high priority packets are sent and one medium priority packet. Finally, three more high priority packets are sent followed by one medium priority packet and then by one low priority packet. The process continues in this fashion.

Broadcasting

Broadcast Example

Broadcasting lets you send a message to multiple nodes simultaneously. Figure A-5 shows a simple PVC Broadcast application where the DTE connected to Port 5 sends Broadcast messages to the devices connected to Ports 6 and 7.

Note

Before a port can receive a PVC Broadcast message, that port must have already established a PVC connection to another port.

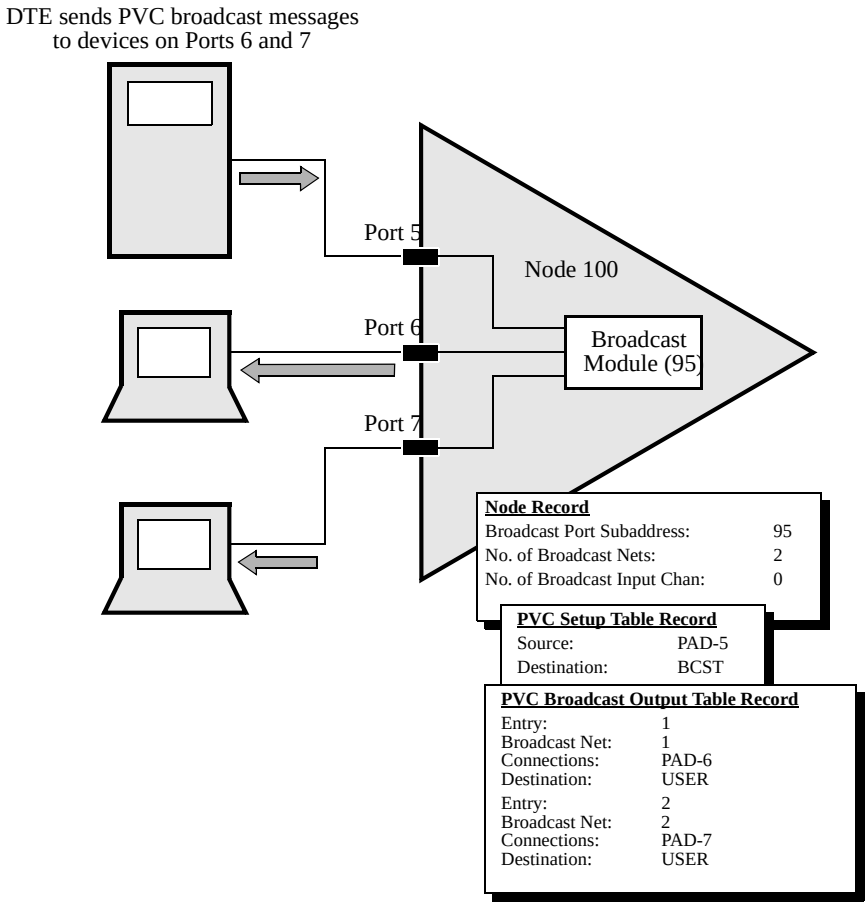


Figure A-5. Simple PVC Broadcast Example

Guideline

When only one broadcast network is configured in the Node record (parameter Number of Broadcast Nets = 1), broadcast data does not have to be preceded by a hexadecimal network ID. If more than one broadcast network is configured, broadcast data must be preceded by a two-digit hexadecimal ID which is the same as the network number.

Note

Broadcast does not support calls for a port configured for Data Connection Protection.

Addressing and Address Blanking

Basic Addressing

To establish calls between two points in your network, include two types of addresses in the Call command:

- The network address of the node that is attached to the terminal being called.
- The subaddress, which identifies the port to which the called terminal is attached.

Required Parameters

This table lists the parameters required for a port to receive a call and for a port to send a call.

If a Port	*Configure*
Receives a call	These parameters in the receiving node: • Node Address: This parameter in the Node Record specifies the node's network address. • Subaddress: This parameter in the Port Record provides the subaddress for the particular port that is to receive the call.
Sends a call	These parameters in the Route Selection Table Record of the sending node: • Entry Number: This identifies the specific Route Selection Table entry being configured. • Address: This is the Network Address of the node that receives the call. It should be represented in the receiving node's Node Address parameter in its Node Record. • Destination: This is the local port that the call is sent to. You can configure up to eight destination ports for each entry. • Priority: This is a priority of the destination port and is used for load sharing and alternate routing.

Address Blanking

You can blank an address, that is, enter no address value with the Node Address parameter = (blank).

Blanking has two uses:

- Blank a node’s address so calls go to one of its ports.
- Disable a function.

Disabling a Function

If you set the parameter Alarm Printer Mnemonic (in the Node Record) to blank, no alarms are sent. If you set the parameter Group Subaddress (in the PAD Port Record) to blank, the parameter is disabled.

Setting Thresholds

Introduction

The Node Record contains these threshold parameters that monitor specific overload situations:

- Port utilization threshold
- Buffer utilization threshold
- CPU utilization threshold
- Port error threshold
- Threshold alarm time

How the Port Utilization Threshold Sets the Alarm Level

This table describes the steps followed by the Port Utilization Threshold to set the alarm level for traffic on every port in a node.

Step	*Action*	*Description/Result*
1	Traffic is checked over a 64-second interval to give an average (in characters per second).	
2	The average is compared to the port's clock rate.	A utilization factor is produced.
	If	***Then***
	The utilization percentage exceeds the setting	This alarm is generated: **Port Utilization > Threshold** Port utilization records are kept for each port and the port in question is noted in the report.

Buffer Utilization Threshold

The buffer utilization threshold sets the alarm level for data buffers. When data passes through a node, buffers provide temporary storage. If the number of buffers used exceeds the specified percentage of available storage, this alarm is generated:

Buffer Pool Utilization > Threshold

CPU Utilization Threshold

The CPU has two functions:

- To run background diagnostic tests to ensure that the hardware is not faulty
- To process data communications traffic

If the CPU is not processing data, it is running diagnostic checks. It is never idle. The CPU utilization threshold parameter specifies the amount of time spent performing nondiagnostic functions as a percentage of the total time. If this percentage exceeds the threshold, This alarm is generated:

CPU Utilization > Threshold

How Ports Detect Errors

This table describes how Vanguard ports detect errors.

Step	Action	
1	Error detection schemes protect data transferred between a port and an attached device.	
	If	*Then*
	Synchronous protocols (X.25 port)	Data is transferred in frames, along with a cyclic redundancy check (CRC) field as part of the frame.
	Asynchronous data	A parity bit is attached to each character.
2	Each port detects errors by examining these bits.	
3	When an error is detected, a counter increments, The counter is also incremented for framing, overrun, and underrun errors.	
	If	*Then*
	The count exceeds the threshold	An alarm is generated.
4	The count continually increments. You can reset the count from the Status/Statistics menu.	

Threshold Alarm Timer

The threshold alarm timer parameter prevents a node from sending threshold alarms too frequently. If a node generates an alarm, the threshold alarm timer is started and the node is not allowed to generate the same alarm until the timer has expired.

Appendix B
Implementing SNTP

Overview

Introduction

Simple Network Time Protocol (SNTP), defined by RFC 2030, is a small client/server application that synchronizes time between points on a network. It allows the node to communicate with any other SNTP server on any other platform in order to synchronize time with it.

SNTP is best suited to provide synchronization on the network for accurate billing, packet stamping, and alarm information.

Note

You do not have to boot the node to activate SNTP.

Server

When a node acts as an SNTP server, it must be synchronized with its primary source before responding to a client's request for synchronization. A server synchronizes after each node boot or reset. It also synchronizes after each SNTP record change. The server stops functioning when the configuration record is disabled.

Client

When a node acts as a client, it is silent on the SNTP network. It does not respond to synchronization requests from another client. Because an SNTP client is silent, you cannot determine which time server is providing its synchronization by passing a synchronization request to it. A client synchronizes to within 50 milliseconds of its reference server. It also synchronizes after each node boot or reset and after each SNTP record change.

Limitations

SNTP has these limitations:

- The largest offset used for Daylight Saving Time (DST) is one hour.
- It cannot provide accuracy beyond one second.
- It can provide synchronization with the network but not real-time synchronization.
- The node can synchronize only with clients and servers that can receive UDP packets on port 123.

SNTP Record

Introduction

The SNTP Record is in the Update System Parameters menu. The parameters for SNTP reside in the Network Time Synchronization menu.

Procedure

To implement SNTP:

Step	*Action*	*Result/Description*
1	Select **Update System Parameters** from the CTP Main menu.	The Update System Parameters menu appears as shown in Figure B-1.
2	Select **Network Time Synchronization** from the Update System Parameters menu.	The Network Time Synchronization menu appears.
3	Select **Configuration**.	The SNTP parameters begin to appear.
4	Configure the SNTP parameters.	The node begins to synchronize with the other SNTP nodes on the network.
5	When done, press semi-colon (**;**), then press ENTER.	The node synchronizes with the other SNTP nodes on the network.

Accessing the SNTP Record

Figure B-1 shows you how to navigate the CTP menu to the SNTP Record:

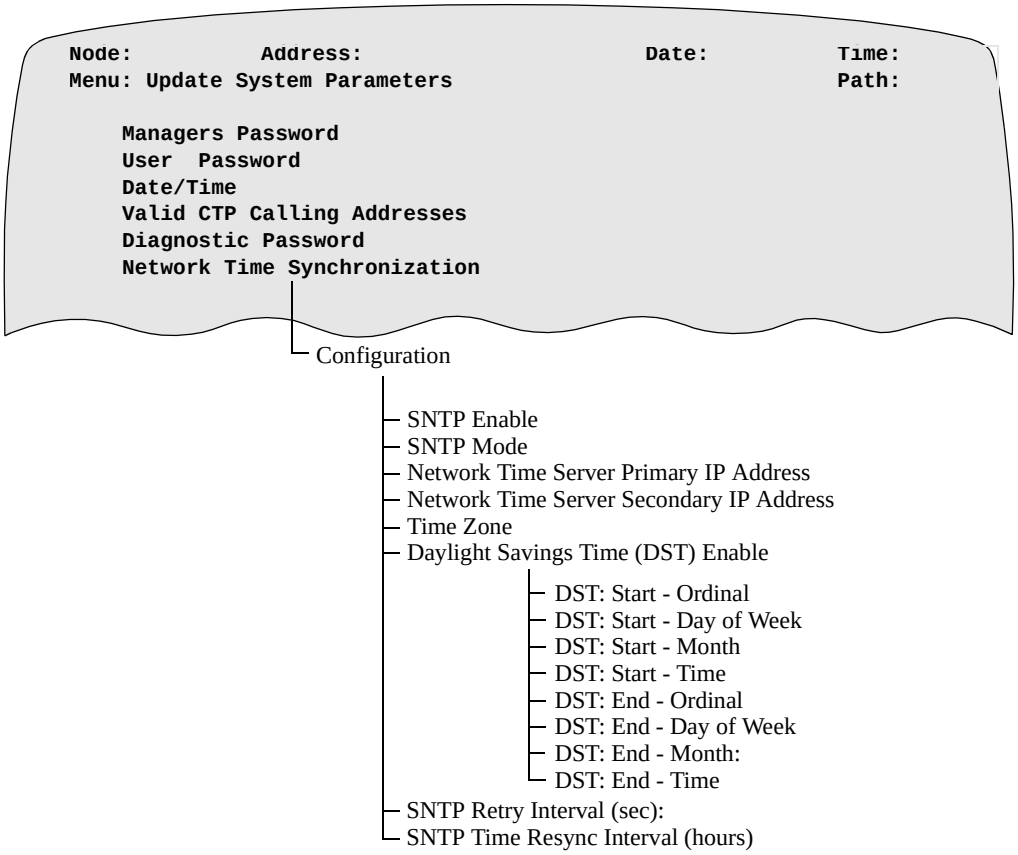


Figure B-1. How to Get to the SNTP Record

SNTP Record Parameters

Configuring SNTP

These are the SNTP record parameters you must configure:

SNTP Enable

Range:	Disable, Enable
Default:	Disable
Description:	Enables SNTP functions on the node.

SNTP Mode

Range:	Both, Client, Server
Default:	Both
Description:	Specifies whether this node is to operate as a client, a server, or as both a client and a server in the time synchronization process. • Both - Node acts as a client to another time server, and a time server to other nodes. The client must be synchronized before the server functions properly. • Client - Node acts as client to a time server. This node does not respond to requests for time synchronization from other nodes. • Server - Node acts as a time server to other nodes.

Network Time Server Primary IP Address

Range:	A valid IP address in dotted notation.
Default:	(blank)
Description:	Specifies the IP Address of the SNTP server. **Note** Use the space bar to blank this field.

Network Time Server Secondary IP Address

Range:	A valid IP address in dotted notation.
Default:	(blank)
Description:	Specifies the IP Address of the secondary SNTP server. **Note** Use the space bar to blank this field.

Time Zone

Range:	-12:00, -11:00, -10:00, -9:30, -9:00, -8:30, -8:00, -7:00, -6:00, -5:00, -4:00, -3:00, -3:30, -2:00, -1:00, 00:00, 1:00, 2:00, 3:00, 3:30, 4:00, 4:30, 5:00, 5:30, 6:00, 6:30, 7:00, 8:00, 9:00, 9:30, 10:00, 10:30, 11:00, 11:30, 12:00, 13:00
Default:	-5:00
Description:	Specifies the time offset between your time and Greenwich time: • WEST of Greenwich your time offset is negative. • EAST of Greenwich your time offset is positive. Offset is based on the Greenwich Mean Time (GMT), the international from standard which times are calculated. **Note** The standard times used in countries around the world are tabulated from Nautical and Air Almanacs relevant to each region.

Daylight Savings Time (DST) Enable

Range:	Disable, Enable
Default:	Enable
Description:	Enables Daylight Savings Time support. When you enable this parameter, the eight Daylight Savings Time parameters that control Daylight Savings Time settings appear below. When you disable it, they disappear. **Note** Daylight Savings Time is a period (that varies from country to country) during which clocks are set ahead one hour or more to provide more light at the end of the day during spring, summer and early fall. The Daylight Savings Time settings compensate for this time shift.

DST: Start - Ordinal First

Range:	First, Second, Third, Fourth, Last
Default:	First
Description:	Specifies the set of calendars (ordinal) in which Daylight Savings Time begins. The ordinal begins with a designated day of week. For example: If that day is Wednesday, and Daylight Savings Time starts on or after the first Wednesday of the month, the ordinal is First.

DST: Start - Day of Week

Range:	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
Default:	Sunday
Description:	Specifies the day of the week when Daylight Savings Time begins. **Note** You can find the beginning and end of Daylight Saving Time for your country, time zone, and current year in Nautical and Air Almanacs relevant to your region.

DST: Start - Month

Range:	January, February, March, April, May, June, July, August, September, October, November, December
Default:	April
Description:	Specifies month of the year when Daylight Savings Time begins. **Note** You can find the beginning and end of Daylight Saving Time for your country, time zone, and current year in Nautical and Air Almanacs relevant to your region.

DST: Start - Time

Range:	0:00, 1:00, 2:00, 3:00, 4:00, 5:00, 6:00, 7:00, 8:00, 9:00, 10:00, 11:00, 12:00, 13:00, 14:00, 15:00, 16:00, 17:00, 18:00, 19:00, 20:00, 21:00, 22:00, 23:00
Default:	2:00
Description:	Specifies the time when Daylight Savings Time begins. **Note** This parameter specifies when the clock transitions from standard time to DST.

DST: End - Ordinal Last

Range:	First, Second, Third, Fourth, Last
Default:	Last
Description:	Specifies the set of calendars (ordinal) in which Day Savings Time ends. The ordinal begins with a designated day of week. For example: If that day is Sunday, and Daylight Savings Time ends on or after the last Sunday of the month, the ordinal is Last.

DST: End - Day of Week

Range:	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
Default:	Sunday
Description:	Specifies the day of the week when Daylight Savings Time ends. **Note** You can find the beginning and end of Daylight Saving Time for your country, time zone, and current year in Nautical and Air Almanacs relevant to your region.

DST: End - Month

Range:	January, February, March, April, May, June, July, August, September, October, November, December
Default:	April
Description:	Specifies the month in which Daylight Savings Time ends. **Note** You can find the beginning and end of Daylight Saving Time for your country, time zone, and current year in Nautical and Air Almanacs relevant to your region.

DST: End - Time

Range:	0:00, 1:00, 2:00, 3:00, 4:00, 5:00, 6:00, 7:00, 8:00, 9:00, 10:00, 11:00, 12:00, 13:00, 14:00, 15:00, 16:00, 17:00, 18:00, 19:00, 20:00, 21:00, 22:00, 23:00
Default:	2:00
Description:	Specifies the time when Daylight Savings Time ends. **Note** This parameter specifies when the clock transitions from standard time to DST.

SNTP Retry Interval

Range:	5 to 255
Default:	15
Description:	Enter the time interval in seconds that the SNTP client should wait between SNTP synchronization requests. **Note** The client sends out synchronization requests when SNTP Time Resync Interval expires.

SNTP Time Resync Interval

Range:	1 to 240
Default:	24
Description:	Enter the time interval in hours that the SNTP client should wait before attempting to resynchronize with the server. When the Resync Interval expires, the client sends out synchronization requests. **Note** The time between these synchronization requests is specified in SNTP Retry Interval.

Index

Symbols

A

B

C

D

E

F

H

I

L

M

N

P

R

S

T

U

W

X