Vanguard Managed Solutions

Vanguard Applications Ware
Basic Protocols

X.25 Configuration Basics Manual

Notice

Restricted Rights Notification for U.S. Government Users

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

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

Restricted Rights Legend

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

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

Notice

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

Unpublished - rights reserved under the copyright laws of the United States.

Proprietary Material

Part No. T0107, Rev J

Publication Code DS

Printing August 1998

Manual is current for Release 6.2 of Vanguard Applications Ware.

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

Contents

Chapter 1. X.25 Protocol Theory Of Operation

OSI Layers and X.25 Functionality 1-2
Theory of Operation 1-5
Communications Ports 1-6
  Vanguard DTE and DCE Ports 1-7
EIA Connection Types 1-8
  SIMP (Simple) Connections 1-9
  DTR Connections 1-10
  DTRD Connections 1-11
  DTRP Connections 1-13
  DIMO Connections 1-15
  EMRI/EMDC Connections 1-23

Chapter 2. Configuring the X.25 Protocol

Configuring the Example X.25 Application 2-3
  Configuring the Node Record 2-4
  Configuring the Port Record 2-5
  Configuring the LAN Connections 2-9
  Configuring the Mnemonic Table 2-14
Configuring the T1/E1 Interface 2-15
  Booting the Node or Port 2-28
X.25 Configuration Parameters 2-29
  Port Record Configuration Parameters 2-30
  Best Path Routing 2-57
  Periodic SVC Billing 2-58
  Configuring X.25 Options to Prevent Routing Loops 2-60
  Configuring an X.25 Port for Suppression of Call Rerouting 2-61
  Limiting Calls Between Ports 2-62
  D-bit Modification 2-63
  Call Redirection 2-65
  Call Facility Manipulation for Inbound Calls 2-66
  Call Facility Manipulation for Outbound Calls 2-69
  Link Address Negotiation for Dial On Demand 2-71

Contents (continued)

Chapter 3. Configuring Call Translation Functions

Inbound Call Translation Table Record 3-2
  Inbound Call Translation Table Record Parameters 3-4
Outbound Call Translation Table Record 3-5
  Outbound Call Translation Table Record Parameters 3-7
Configuring the REGSO Option 3-9
  Configuring Mnemonic Calls 3-12
  Searching for and Deleting an Address 3-13
Calling Address Translation Table Record 3-16
  Calling Address Translation Table Record Parameters 3-18
CUD Based Address Translation Table 3-19
Call Redirection Table 3-21
  Call Redirection Table Parameters 3-23

Chapter 4. Statistics

Accessing the Detailed Port Statistics 4-2
  Port Statistics Screen 4-3
T1/E1 Interface Statistics 4-10

Chapter 5. Troubleshooting with Delay Path Tracing

How Delay Path Tracing Works 5-4
Delay Measurement Test 5-11
  Accessing Delay Path Tracing 5-12
  Running A Delay Measurement Test 5-16
  Terminating Delay Path Tracing Measurement 5-17
  Delay Path Tracing Measurement Reporting 5-19

Chapter 6. Logical Channel Number Maps

Chapter 7. X.25 Facility Codes

Index

Chapter 1
X.25 Protocol Theory Of Operation

Overview

This chapter provides a brief explanation of the OSI model, as it applies to X.25 and the basic theory of operation for the X.25 protocol. It explains what the protocol is, how it works, and defines the port types available when using X.25.

What Is X.25

X.25 is the protocol used to connect devices with DTE and DCE interfaces, such as the Vanguard family of products, to Packet Switched Data Networks (PSDN). In X.25, a data stream is segmented (packetized) into small packets, and transmitted over a physical connection.

X.25 uses a virtual call service which establishes an end-to-end path through the packet network and permits virtual circuit service to simulate dialed circuit switch connections. X.25 is capable of multiplexing up to 4096 logical channels (virtual circuits) on a single access link.

Packet Structure

Each packet contains a header and the data segment, as shown in Figure 1-1.

Header	Data	Trailer

Figure 1-1. The X.25 Packet Structure

OSI Layers and X.25 Functionality

Introduction

The structure of X.25 follows the seven layer OSI model shown in Figure 1-2, and roughly corresponds to the lower three layers: Physical, Link, and Network.

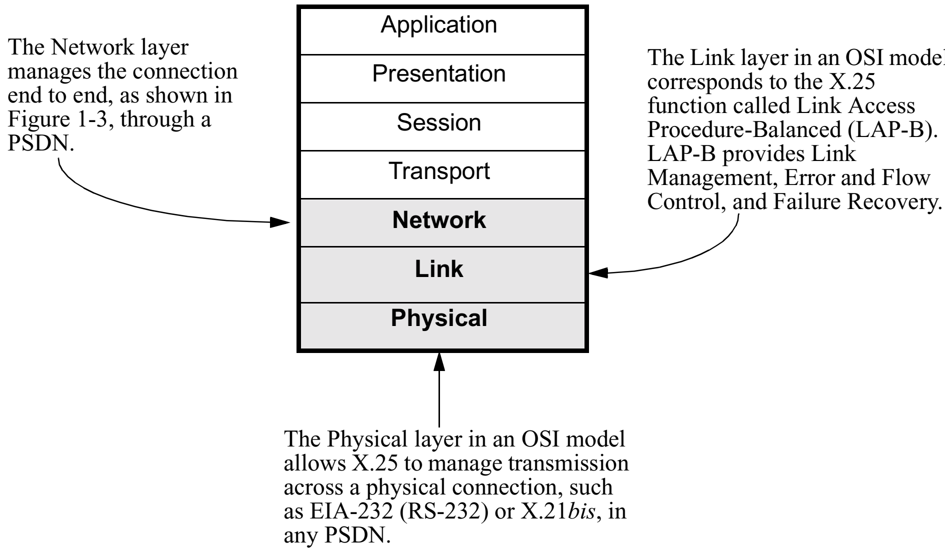

Figure 1-2. OSI Model

OSI/X.25 Example

Figure 1-3 illustrates and example network in which the OSI/X.25 Model is identified. The Physical layer applies to the connection from one device to a PSDN. The Link layer (LAP-B) applies to the connections from one device to a second device such as a DTE port to a DCE port. The Network layer is represented by the between ports on Vanguard devices.

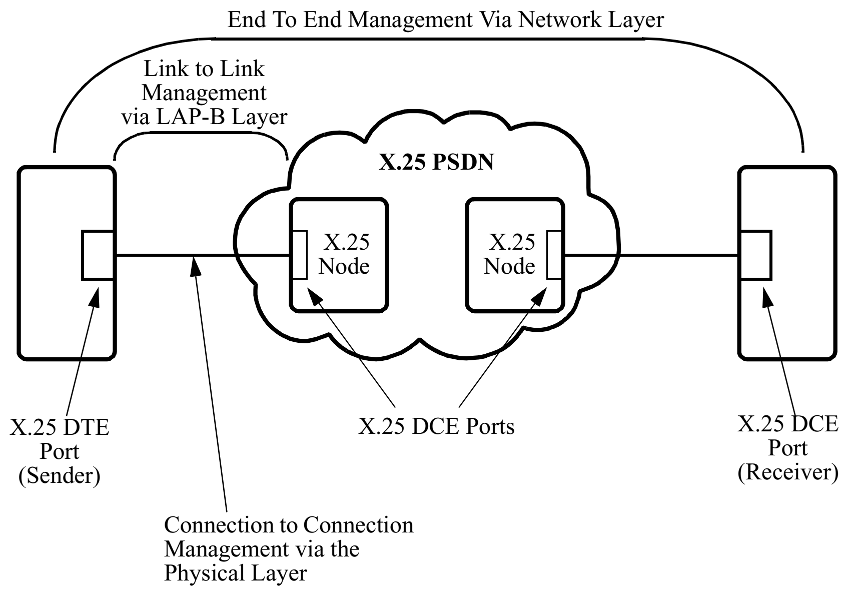

Figure 1-3. Network Example of OSI/X.25 Connections

Link Access Procedure - Balanced (LAPD

LAP-B is used to manage the transfer of data using frames. Each frame is divided into three specific segments: the header, data, and the trailer. Each segment is further divided into fields as shown in Figure 1-4.

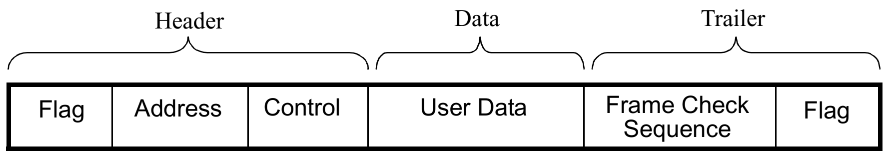

Figure 1-4. X.25 Segment and Field Structure

Each field contains information generated by the frames sending device. This information is read by the receiving device to perform the link functions required. These functions are:

- Link Management. This includes management functions such as accepting or rejecting data frames, disconnecting the link, and setting link response modes. These frames contain commands and responses to coordinate and maintain the link.
- Error Control. LAP-B provides error detection and correction by ensuring that data is transferred across the link accurately. The sending device sequentially numbers each frame it sends and fills in the Frame Check Sequence field with a number it calculates from information derived from the frame contents. The receiving device performs the same calculation and compares it to the frame contents. If the frame data is corrupted, the receiver uses the Link Management frame to tell the sender to resend the corrupted frame. Of course, the corrupted frame is identified by its sequence number. An acknowledgment is sent back to the sending device when a correct frame is received.
- Flow Control. This refers to a process in which the receiving device tells the sender to stop transmitting data when memory (storage or display) limitations are reached. If the receiving device senses that it is nearing its memory limitation, it does not send out the acknowledgment signal to the sender. Once sufficient memory is available, the acknowledgment is send and the sending device continues to send its data.
- Failure Recovery. LAP-B provides failure recovery through the frame sequencing and acknowledgment schema. This allows LAP-B to remember the status of any failed link. Once the failure is corrected, the link will resume sending and receiving data.

  One interesting consideration to take note of is that many private PSDNs provide multiple paths for data to follow. In these cases, an alternate path is always available should a link fail. The benefit of these multiple links is that when a call is in progress and the link fails, the call is not disconnected. The alternate route is automatically used and the call continues.

Theory of Operation

Introduction

This section describes what occurs when you:

- Connect to a Vanguard device
- Enter the Command mode
- Communicate in Data mode

Connecting to A Vanguard Device

Before you can send commands to a Vanguard Device or pass data, your terminal must communicate with an APAD or ATPAD port. Refer to the Vanguard Basics Manual for complete instructions on Accessing the Node, and the APAD/ATPAD Configuration Manual for further explanation of APAD and ATPAD ports.

Command and Data Modes

When accessing a node's CTP, i.e., making a call to the CTP, you see either an asterisk (if connecting to an APAD port) or an OK prompt (if connecting to an ATPAD port) your terminal is in what is referred to as the Command Mode. When your call is accepted, i.e., the CTP Main Menu is displayed, your terminal enters the Data Mode.

When your terminal is in the Command mode you can send X.28 commands to the X.28 handler.

One of the commands that can be entered is the Call command. When a call is established, your terminal is in Data mode. When the call is terminated, your terminal returns to the Command mode.

Communications Ports

Introduction

This section describes

- Vanguard DTE and DCE Ports
- EIA Connection Types

Ports

Vanguard products can be fitted with an internal DIM or a DIM Site Daughtercard to offer multiple port configurations. Vanguard physical ports can be configured as either Data Communication Equipment (DCE) or Data Terminal Equipment (DTE). When a DTE terminal is attached to a port, a straight-through cable should be used. When a DCE port connects to a modem or other DCE device, a crossover cable is required.

Vanguard DTE and DCE Ports

Introduction

Control signals are used to establish and maintain an electrical connection between network devices, such as Data Communications Equipment (DCE) or Data Terminal Equipment (DTE).

How Vanguard Products Handle Control Signals

Vanguard products generate these control signals from DCE and DTE ports:

Signals Generated by DCE Port	*Signals Generated by DTE Port*
Data Carrier Detect (DCD) Pin 8	Request to Send (RTS) Pin 4
Data Set Ready (DSR) Pin 6	Data Terminal Ready (DTR) Pin 20
Clear To Send (CTS) Pin 5	Data Restraint Out (DRO) Pin 14
Ring Indicator (RI) Test Mode Pin 22	N/A

Monitoring Control Signals

Vanguard products monitor these control signals from DCE and DTE ports:

Signals Monitored by DCE Port	*Signals Monitored by DTE Port*
Data Terminal Ready (DTR) Pin 20	Data Set Ready (DSR) Pin 6
Request To Send (RTS) Pin 4	Data Carrier Detect (DCD) Pin 8
Ring Indicator (RI) Test Mode Pin 22	Ring Indicator (RI) Pin 25
Make Busy (MB) Pin 25	Make Busy (MB) Pin 22

Ring Indicator and Test Mode

Vanguard products assign dual functions (Ring Indicator and Test Mode) to pin 22 at the EIA-232 interface. When port 1 or 2 is set as a DCE port, the RI/TM DIP switch in the front panel (refer to your Installation Manual for the exact location of this DIP switch) connects an EIA-232 driver to pin 22 so the DCE port can emulate a modem.

When connecting to a DCE device, use a crossover cable with pin 25 from the modem connecting to pin 22 of the connector. Pin 22 receives the Test Mode signal from the modem used when running V.54 loopback tests. In this case, the DIP switch must be set to the TM (Test Mode) to disconnect the EIA-232 output and avoid contention.

When connecting to a DTE device using a straight-through cable and when the port connection type is configured as EMRI (Emulate Modem using Ring Indicator), the front panel DIP switch must be set to the Ring Indicator (RI) position. This connects the extra EIA-232 output to pin 22 to act as the Ring Indicator.

EIA Connection Types

Introduction

A device connected to a port can establish and maintain a connection only after a proper handshake using control signals has occurred. This is called the EIA connection establishment and should not be confused with the physical connection to the port. A port's physical level is in an idle state when there is no EIA connection and when it is disconnected.

Connection Types

Different types of EIA connections can be used depending on the setting of the Connection Type parameter (in the Port Record):

- SIMP: Simple connection with no control signal handshake. See “SIMP (Simple) Connections” on page 9 for additional information.
- SIMPv: The modem switches from leased to dial-only mode when leased line goes down. See “SIMPv” on page 9 for additional information.
- DTR: Connection with DTR control signal handshake. See “DTR Connections” on page 10 for additional information.
- DTRD: Same as DTR but control signals drop. See “DTRD Connections” on page 11 for additional information.
- DTRP: When DTR needs to be passed end-to-end. See “DTRP Connections” on page 13 for additional information.
- DIMO: Dial modem attached to the port and does dial-in/out handshake. See “DIMO Connections” on page 15 for additional information.
- DIMOa: Same as DIMO except DSR not raised.
- DIMOb: Same as DIMO except DSR follows DTR.
- DIMOv: The port handshakes with attached V.25 *bis* dial modem.
- EMRI: Port emulates a modem and does dial-in/out handshake with RI. See “EMRI/EMDC Connections” on page 23 for additional information.
- EMDC: Port emulates a modem and does dial-in/out handshake with DCD. See “EMDC” on page 23 for additional information.

Disable/Enable Ports

When a port is disabled, its EIA connection type is changed to NULL and all input control signals are ignored. All output control signals are dropped. If the parameter Port Control is set to MB (Make Busy), RI (pin 22) is raised.

When a disabled port is enabled, its EIA connection type changes back to the configured EIA connection type. If the parameter Port Control is set to MB (Make Busy), RI (pin 22) is lowered.

■ **Note**

Make Busy (MB) is not supported for any port type if the DIM is installed in the DTE position.

DIMs

When using V.21, V.35, or V.36 DIMs in either the DTE or the DCE position, use the Connection Type SIMP. When using EIA-232-D DIMs in the DTE position, do not select Connection Type EMRI.

SIMP (Simple) Connections

Introduction

This connection type is used when terminals are connected to a port with a cable that has minimal conductors. Most control signals are absent because of the lack of conductors. This kind of cabling provides only ground, transmit and receive data, transmit and receive clock.

■ **Note**

For DCE ports, DCD, DSR, and CTS control signals remain high. For DTE ports, RTS, DTR, and DRO control signals remain high.

DCE EIA Status for SIMP

Connection - Outbound control signals DCD, DSR, and CTS (pins 8, 6, and 5) are held high at all times. On asynchronous PAD ports, if EIA data restraint is enabled, CTS and RTS (pins 5 and 4) may change according to the requirements of data restraint. Inbound control signals DTR and MB (pins 20 and 25) are ignored.

DTE EIA Status for SIMP

Connection - Outbound control signals RTS, DTR, and DRO (pins 4, 20, and 14) are held high at all times. On asynchronous PAD ports, if EIA data restraint is enabled, DCD and DRO (pins 8 and 14) may change according to the requirements of data restraint. Inbound control signals are ignored: DCD, DSR, and CTS (pins 8, 6, and 5).

SIMPv

This is a combination of SIMP and DIMOv Connection Types. It starts as SIMP and after the SIMP connection goes down (leased line), the Connection Type switches to DIMOv (dial line). This is used with dial restoral modems.

DTR Connections

Introduction

Use this connection type when the device connected to the port provides basic control signals to maintain the EIA connection. The remote user calling the device through a PAD port will know if the device is disconnected or powered down because the call will not be completed. Users connecting to a PAD port will access the terminal handler. They can manually call or be automatically connected if the port is configured for autocalling.

DCE Port States

This table describes the conditions during various states for DTR connections on DCE ports.

State	***DCE Ports***
Idle	DCD, DSR, and CTS (pins 8, 6, and 5) are held high at all times.
Connection	The port monitors DTR (pin 20). If it is detected high, the EIA connection is established. RTS is ignored. A device on the asynchronous PAD port connects to the terminal handler. A call from the network is accepted if DTR is active. On asynchronous PAD ports, if EIA data restraint is enabled, CTS (pin 5) may go low during the connection.
Disconnection	The port monitors DTR (pin 20). If it goes low for more than 1.5 seconds, disconnection occurs. A call clear is sent to the network if disconnection occurs.

DTRD Connections

Introduction

Use this connection type only on asynchronous PAD ports. Some devices require APAD ports to lower the control signals for a short period after the call is terminated.

DCE Port States

This table describes the conditions during various states for DTR connections on DCE ports.

State	DCE Ports
Idle	DCD, DSR, and CTS (pins 8, 6, and 5) are held high at all times.
Connection	The port monitors DTR (pin 20). If it is detected high, the EIA connection is established. RTS is ignored. A device on the asynchronous PAD port connects to the terminal handler. A call from the network is accepted if DTR is active. On asynchronous PAD ports, if EIA data restraint is enabled, CTS (pin 5) may go low during the connection.
Disconnection	The port monitors DTR (pin 20). If it goes low for more than 1.5 seconds, the port drops DCD, DSR, and CTS (pins 8, 6, and 5) for one second. A call clear is sent to the network, and the port returns to the idle state. During the control signal drop, the port cannot receive calls from the network. If the user clears the call by entering [CLR] the signals do not drop. If the call is cleared by an X.29 invitation to clear, the signals remain high when the parameter Invitation to clear = CLRWO: the signals are dropped when the parameter Invitation to clear = CLRWD.

DTE Port States

This table describes the conditions during various states for DTR connections on DTE ports.

State	***DTE Ports***
Idle	RTS, DTR, and DRO (pins 4, 20, and 14) are held high at all times.
Connection	The port monitors DSR (pin 6). If it is detected high, the EIA connection is established. DCD is ignored. A device on the asynchronous PAD port connects to the terminal handler. A call from the network is accepted if DSR is active. On asynchronous PAD ports, if EIA data restraint is enabled, DRO (pin 14) may go low during the connection.
Disconnection	The port monitors DSR (pin 6). If it goes low for more than 1.5 seconds, the port drops RTS, DTR, and DRO (pins 4, 20, and 14) for one second. A call clear is sent to the network, and the port returns to the idle state. During the control signal drop, the port cannot receive calls from the network. If the user clears the call by entering [CLR], the signals do not drop. If the call is cleared by an X.29 invitation to clear, the signals remain high when the parameter Invitation to clear = CLRWO: the signals are dropped when the parameter Invitation to clear = CLRWD.

DTRP Connections

Port States for DTRP (Originate End: Autocall Configured

These tables describe the conditions during various states for DTRP (Originate End: Auto Calling Configured) connections on DCE and DTE ports.

State	DCE Ports
Idle	DCD, DSR, and CTS (pins 8, 6, and 5) are maintained low.
Connection	The port monitors DTR (pin 20). If it is high or goes high, the port makes a network call according to the autocall mnemonic and waits for the call to be accepted by the remote PAD. If the call is accepted, the port raises DCD, DSR, and CTS (pins 8, 6, and 5) and the connection is established. If the call is not accepted, the port continues to autocall until it reaches the autocall limit. DCD, DSR, and CTS (pins 8, 6,and 5) will remain low.
Disconnection	The port monitors DTR (pin 20). If it goes low for at least 50 milliseconds, the port drops control signals DCD, DSR, and CTS (pins 8, 6, and 5), clears the call, and returns to the idle state. If the call is cleared from the network or by the user entering [CLR] at the port, the port, immediately drops the controls signals

This table describes the conditions during various states for DTRP connections on DTE ports.

State	DTE Ports
Idle	RTS, DTR, and DRO (pins 4, 20, and 14) are maintained low.
Connection	The port monitors DSR (pin 6). If it is high or goes high, the port makes a network call according to the autocall mnemonic and waits for the call to be accepted by the remote PAD. If the call is accepted, the port raises RTS and DTR (pins 4 and 20) and the connection is established. If the call is not accepted, the port continues to autocall until it reaches the autocall limit. RTS, DTR and DRO (pins 4, 20, and 14) remain low.
Disconnection	The port monitors DSR (pin 6). If it goes low for at least 50 milliseconds, the port drops RTS, DTR, and DRO (pins 4, 20, and 14), clears the call, and returns to the idle state. If the call is cleared from the network or by the user entering [CLR] at the port, the port immediately drops the controls signals.

Port States for DTRP (Answer End: No Auto Calling)

These tables describe the conditions during various states for DTRP (For the Answer End: No Auto Calling) connections on DCE and DTE ports.

State	***DTE Ports***
Idle	DCD, DSR, and CTS (pins 8, 6, and 5) are maintained low.
Connection	When a call arrives from the network, the port raises DCD, DSR, and CTS (pins 8, 6,and 5) and monitors DTR (pin 20). If DTR is high or goes high, the PAD accepts the call.
Disconnection	The port continues to monitor DTR (pin 20). If it goes low for at least 50 milliseconds, the port drops DCD, DSR, and CTS (pins 8, 6,and 5), clears the calls and returns to the idle state. If the call is cleared from the network or by the user entering [CLR] at the port, the port immediately drops the controls signals. If DTR is not raised within three seconds after the call arrives from the network, the port drops the control signals and clears the call.

This table describes the conditions during various states for DTRP connections on DTE ports.

State	***DTE Ports***
Idle	RTS, DTR, and DRO (pins 4, 20, and 14) are maintained low.
Connection	When a call arrives from the network, the port raises RTS, DTR, and DRO (pins 4, 20, and 14) and then monitors DSR (pin 6). If DSR is high or goes high, the PAD accepts the call.
Disconnection	The port continues to monitor DSR (pin 6). If it goes low for at least 50 milliseconds, the port drops RTS, DTR, and DRO (pins 4, 20, and 14), clears the call, and returns to the idle state. If the call is cleared from the network or by the user entering [CLR] at the port, the port immediately drops the controls signals. If DSR is not raised within three seconds after the call arrives from the network, the port drops the control signals and clears the call.

DIMO Connections

Introduction

Use this connection type with a crossover cable to connect a dial modem to the DCE port. When calls are made, the port handshake uses the modem control signals.

There are several types of operation that can occur with this connection type including:

- Dial In
- Dial Out
- Dial In/Dial Out Collision

Dial In

When a user dials into a PAD port through a telephone network, the connection depends on whether the port is configured for manual calling or autocalling. When the port is configured for manual calling, the user is connected to the terminal handler when the EIA connection is completed. When the port is configured for autocalling, the call request must be accepted before the EIA connection is completed. This prevents users from being charged for the telephone call if the call cannot be completed.

These tables describe the conditions during various states for DIMO (Dial In, No Autoconnect).

State	*DCE Ports*
Idle	DCD, DSR, and CTS (pins 8, 6, and 5) are maintained low.
Connection	The port monitors MB (pin 25) [modem RI]. If it goes high, the port raises DSR, DCD, and CTS (pins 6, 8, and 5) [modem DTR, RTS, and DRO (pins 20, 4, and 14)], then waits up to 240 seconds for DTR and RTS (pins 4 and 20) [modem DSR and DCD] to go high. If the timer expires, DCD, DSR, and CTS (pins 8, 6, and 5) are dropped, the network call is cleared, and the port returns to the idle state. The connection is established when DTR and RTS go high. After the port receives the MB signal, it cannot receive calls from the network, so the dial procedure can be completed.

State	DCE Ports (continued)
Disconnection	The port monitors DTR and RTS (pins 20 and 4) [modem DSR, DCD]. If either goes low for at least 50 milliseconds, the port immediately drops DCD, DSR, and CTS (pins 8, 6 and, 5) [modem RTS and DTR] and a call clear is sent to network. A PAD port also drops the control signals and returns to the idle state if the user fails to establish a call within the time configured by the Port Record parameter Call Accept Timeout or makes three unsuccessful call attempts. If the call is cleared by an X.25 clear from the network, the port immediately drops DCD, DSR, and CTS [modem RTS, DTR, and DRO]. The port waits for DTR and RTS [modem DSR, DCD] to go low, at which time the port returns to idle state, ready for another dial-in sequence. If the call is cleared from the port by the user entering [CR] at the port, control signals are not dropped until Call Accept Timeout expires. The port is unavailable to take network calls while waiting for the control signals from the modem to drop. If a call is cleared by an X.29 invitation to clear, the signals remain high when the parameter Invitation to clear = CLRWO: the signals are dropped when the parameter Invitation to clear = CLRWD.

State	DTE Ports
Idle	RTS and DTR (pins 4 and 20) are maintained low.
Connection	The port monitors RI (pin 22). If it goes high, the port raises RTS, DTR, and DRO (pins 4, 20, and 14) then waits up to 240 seconds for DSR and DCD (pins 6 and 8) to go high. If the timer expires, RTS, DTR, and DRO (pins 4, 20, and 14) are dropped, the network call is cleared, and the port returns to the idle state. The connection is established when DSR and DCD go high. After the port receives the RI signal, it cannot receive calls from the network so the dial procedure can be completed.

State	DTE Ports (continued)
Disconnection	The port monitors DSR and DCD (pins 6 and 8). If either goes low for at least 50 milliseconds, the port immediately drops RTS, DTR, and DRO (pins 4, 20, and 14) and a call clear is sent to network. A PAD port also drops the control signals and returns to the idle state if the user fails to establish a call within the time configured by the Port Record parameter Call Accept Timeout or makes three unsuccessful call attempts. If the call is cleared by an X.25 clear from the network, the port immediately drops DTR and RTS. The port waits for DSR and DCD to go low, at which time the port returns to idle state, ready for another dial-in sequence. If the call is cleared from the user entering [CLR] at the port, control signals are not dropped until the Call Accept Timeout expires. The port is unavailable to take network calls while waiting for the control signals from the modem to drop. If a call is cleared by an X.29 invitation to clear, the signals remain high when the parameter Invitation to clear = CLRWO: the signals are dropped when the parameter Invitation to clear = CLRWD.

These tables describe the conditions during various states for DIMO (Dial In, With Autoconnect).

State	DCE Ports
Idle	DCD, DSR, and CTS (pins 8, 6, and 5) are maintained low.
Connection	The port monitors MB (pin 25) [modem RI]. If it goes high, the port makes a network call according to the autocall mnemonic. When the call is accepted, the port raises DCD, DSR, and CTS (pins 8, 6, and 5) [modem RTS, DTR, and DRO (pins 4, 20, and 14)], then waits up to 240 seconds for DTR and RTS (pins 4 and 20) [modem DSR and DCD] to go high. If the timer expires, the DCD, DSR, and CTS (pins 8, 6, and 5) are dropped, the network call is cleared, and the port returns to the idle state. If DTR and RTS go high before the timer expires, the connection is established.

State	DCE Ports (continued)
Disconnection	The port monitors DTR, and RTS (pins 20 and 4) [modem DSR and DCD]. If either goes low for at least 50 milliseconds, the port immediately drops DCD, DSR, and CTS (pins 8, 6, and 5) [modem RTS, DTR and DRO] and a call clear is sent to network. A PAD port also drops the control signals and return to the idle state if the user fails to establish a call within the time configured by the Port Record parameter Call Accept Timeout or makes three unsuccessful call attempts. If the call is cleared by an X.25 clear from the network, the port immediately drops DCD, DSR, and CTS [modem RTS, DTR, and DRO]. The port waits for DTR and RTS [modem DSR and DCD] to go low, at which time the port returns to idle state, ready for another dial-in sequence. If the call is cleared from the port, control signals are not dropped until the Call Accept Timeout expires. The port is unavailable to take network calls while waiting for the control signals from the modem to drop. If the call is cleared by an X.29 invitation to clear, the signals remain high when the parameter Invitation to clear = CLRWO: the signals are dropped when the parameter Invitation to clear = CLRWD.

State	DTE Ports
Idle	RTS and DTR (pins 4 and 20) are maintained low.
Connection	The port monitors RI (pin 25). If it goes high, the port makes a network call according to the autocall mnemonic. When the call is accepted, the port raises RTS, DTR, and DRO (pins 4, 20, and 14) then waits up to 240 seconds for DSR and DCD (pins 6 and 8) to go high. If the timer expires, the RTS, DTR and DRO (pins 4, 20, and 14) are dropped, the network call is cleared, and the port returns to the idle state. If the DSR and DCD go high before the timer expires, the connection is established.

State	DTE Ports (continued)
Disconnection	The port monitors DSR and DCD (pins 6 and 8). If either goes low for at least 50 milliseconds, the port immediately drops RTS, DTR, and DRO (pins 4, 20, and 14) [modem DCD, DSR and CTS] and a call clear is sent to network. A PAD port also drops the control signals and returns to the idle state if the user fails to establish a call within the time configured by the Port Record parameter Call Accept Timeout or makes three unsuccessful call attempts. If the call is cleared by an X.25 clear from the network, the port immediately drops RTS, DTR, and DRO. The port waits for DSR and DCD to go low, at which time the port returns to idle state, ready for another dial-in sequence. If the call is cleared from the port, control signals are not dropped until the Call Accept Timeout expires. The port is unavailable to take network calls while waiting for the control signals from the modem to drop. If the call is cleared by an X.29 invitation to clear, the signals remain high when the parameter Invitation to clear = CLRWO: the signals are dropped when the parameter Invitation to clear = CLRWD. If the call is cleared from the port, control signals are not dropped until Call Accept Timeout expires.

Dial Out

In this case a modem is connected to a PAD port. Calls from the network connect to the PAD port and use the modem to call through the telephone network.

These tables describe the conditions during various states for the connection type DIMO (Dial Out).

State	DCE Ports
Idle	DCD, DSR, and CTS (pins 8, 6, and 5) are maintained low.
Connection	This is for modems with the autodial feature (the modem can dial the number when the DTR input goes from inactive to active). When a call arrives at a port that is idle and available, the call is accepted. The port raises DSR, [modem DTR]. The modem autodials the destination and, when a connection is made, raises its DCD output. The port monitors RTS (pin 4). If it goes high and if DTR remains high, the port raises DCD, DSR, and CTS. If RTS and DTR are not raised within three minutes after the call is accepted (and DSR being raised), the call is cleared.

State	DCE Ports (continued)
Disconnection	The port monitors DTR and RTS (pins 20 and 4) [modem DSR, DCD]. If either goes low for at least 50 milliseconds, the port immediately drops DCD, DSR, and CTS (pins 8, 6, and 5) [modem RTS, DTR, and DRO] and a call clear is sent to network. A PAD port will also drop the control signals and return to the idle state if the user fails to establish a call within the time configured by the Port Record parameter Call Accept Timeout or makes three unsuccessful call attempts. If the call is cleared by an X.25 clear from the network, the port immediately drops DCD, DSR, and CTS [modem RTS, DTR, and DRO]. The port waits for DTR and RTS [modem DSR and DCD] to go low, at which time the port returns to idle state, ready for another dial-in sequence. If the call is cleared from the port, control signals are not dropped until the Call Accept Timeout expires. The port is unavailable to take network calls while waiting for the control signals from the modem to drop. If the call is cleared by an X.29 invitation to clear, the signals remain high when the parameter Invitation to clear = CLRWO: the signals are dropped when the parameter Invitation to clear = CLRWD.

State	DTE Ports
Idle	RTS, DTR, and DRO (pins 4, 20, and 14) are maintained low.
Connection	This is for modems with the autodial feature (the modem can dial the number when the DTR input goes from inactive to active). When a call arrives at a port that is idle and available, the call is accepted and the port raises DTR. The modem autodials the destination and, when a connection is made, raises its DCD output. The port monitors DCD (pin 8). If it goes high and if DSR remains high, the port raises RTS, DTR, and DRO (pins 4, 20, and 14). If DCD and DSR are not raised within three minutes after the call is accepted (and DTR being raised), the call is cleared.

State	DTE Ports *(continued)*
Disconnection	The port monitors DSR and DCD (pins 6 and 8). If either goes low for at least 50 milliseconds, the port immediately drops DCD, DSR, and CTS (pins 8, 6, and 5) [modem RTS, DTR, and DRO] and a call clear is sent to network. A PAD port will also drop the control signals and return to the idle state if the user fails to establish a call within the time configured by the Port Record parameter Call Accept Timeout or makes three unsuccessful call attempts. If the call is cleared by an X.25 clear from the network, the port immediately drops RTS, DTR, and DRO. The port waits for DSR and DCD to go low, at which time the port returns to idle state, ready for another dial-in sequence. If the call is cleared from the port, control signals are not dropped until the Call Accept Timeout expires. The port is unavailable to take network calls while waiting for the control signals from the modem to drop. If the call is cleared by an X.29 invitation to clear, the signals remain high when the parameter Invitation to clear = CLRWO: the signals are dropped when the parameter Invitation to clear = CLRWD.

If the attached modem does not store telephone numbers, or the caller uses standard AT commands, the modem must be configured so DCD output is always high so the port can send dial information to the modem. The modem's DSR must be strapped to follow DTR inputs so that when the network disconnects by dropping all EIA control signals, the modem will drop DSR to complete the disconnection. (DTR Control on the modem must be configured as 108.2. This drops the connection when DTR goes from on to off.)

Dial In/Dial Out Collision

This is the case of a telephone call causing the MB [modem RI] signal to arrive at the port at the same time a network call arrives at the port, thus causing the port to raise DCD, DSR, and CTS [modem RTS, DTR, and DRO]. The port can detect this circumstance because the MB signal is not the expected response. The port resolves the collision by clearing the call to the network while the DCD, DSR, and CTS stay raised at the modem. If DTR and RTS are not raised within one minute, the port drops DCD, DSR, and CTS [modem RTS, DTR, and DRO]. Call collision is resolved in favor of the telephone network caller, that is, the call is completed, not cleared. After the collision is resolved, the call is handled like any other incoming call from the telephone network.

Variations of DIMO Connections

This table identifies variations of DIMO connections that can be used.

Type	*Description*
DIMOa	This is the same as DIMO, except that the DSR signal is treated differently. Use DIMOa when modems do not have DSR raised on incoming calls.
DIMOb	This is the same as DIMO, except that the DSR signal is treated differently. Use DIMOb when modems have DSR following DTR on incoming calls.
DIMOv	This connection type provides the capability for interfacing to V.25 *bis* type modems and is the same as DIMO as far as EIA handshaking is concerned.

EMRI/EMDC Connections

Introduction

This case is for a situation where a PAD port connects to a host computer and replaces a modem.

■ **Note**

Do not use EMRI with hunt groups or autocalls or when using EIA-232-D DIMs in the DTE position.

DCE Port States for EMRI

This table describes the conditions during various states for EMRI connections on DCE ports.

State	*DCE Ports*
Idle	The front panel switch RI/TM is set to RI and DCD, DSR, and CTS (pins 8, 6, and 5) are maintained low.
Connection	When a call arrives from the network, the RI (pin 22) is pulsed (two seconds on, four seconds off) for up to five cycles (30 seconds). During the ringing, DTR (pin 20) is monitored. If it is high or goes high, the PAD clears RI (pin 22) and raises DSR and DCD (pins 6 and 8) and waits for RTS (pin 4) to go high. When RTS goes high, the PAD raises CTS (pin 5). The PAD accepts the incoming call from the network only after DTR and RTS are detected high.
Disconnection	After DTR is detected high, the PAD monitors DTR (pin 20) and if it is low for at least 50 milliseconds, the call is cleared. DSR and DCD (pins 6 and 8) are dropped and the PAD returns to the idle state. If the call is cleared by the network while waiting for RTS to be raised, DSR and DCD are dropped and the PAD waits for DTR to drop before completing the disconnect. The PAD will not accept another dial-out attempt until DTR is lowered. If RTS is not raised within 30 seconds of RI first being raised, then DCD and DSR (pins 8 and 6) are dropped and the call is cleared. If the call is cleared by the network while waiting for DSR to be raised, RI is immediately dropped. Once the call is connected, if the call is cleared from the network DCD, DSR, and CTS are dropped.

EMDC

This is similar to EMRI, but DCD is used to signal the host about arrival of the call.

■ **Note**

Do not use this setting with hunt groups or with autocalls.

■ **Note**

A change in a EIA control signal may not be detected for up to 50 milliseconds (average 25 ms). As a result, the Vanguard ignores data sent to port before the connection was recognized as valid. To prevent this, before passing data wait at least 50 milliseconds after the EIA handshake or until the Vanguard sends a connection prompt.

DCE Port States for EMDC

This table describes the conditions during various states for EMDC connections on DCE ports.

State	DCE Ports
Idle	The front panel switch RI/TM is set to TM and DCD, DSR, and CTS (pins 8, 6, and 5) are maintained low. DTR (pin 20) may be high.
Connection	When a call arrives from the network, the DCD (pin 8) is raised. DTR (pin 20) is monitored. If it is high or goes high, the PAD raises DSR (pin 6) and waits for RTS (pin 4) to go high. When RTS goes high, the PAD raises CTS (pin 5). The PAD accepts the call from the network only after DTR and RTS are detected high.
Disconnection	The PAD monitors DTR (pin 20) and if it is low for at least 50 milliseconds, the call is cleared. The control signals DSR and CTS (pins 6 and 8) are dropped, and the PAD returns to the idle state. If the call is cleared by the network, while waiting for RTS to be raised, and then DSR and DCD (pins 6 and 8) are dropped and the PAD returns to the idle state for the period after DTR is lowered. The PAD will not accept another dial-out attempt until DTR is lowered. If RTS is not raised within 30 seconds of RI being raised, DCD and DSR (pins 8 and 6) are dropped and the call is cleared. If the call is cleared by the network while waiting for DTR to be raised DCD is immediately dropped. Once the call is connected, if the call is cleared from the network DCD, DSR, and CTS are dropped.

DTE Port States for EMDC

This table describes the conditions during various states for EMDC connections on DTE ports.

State	DTE Ports
Idle	The front panel switch RI/TM is set to TM and RTS, DTR, and DRO (pins 4, 20, and 14) are maintained low. DSR (pin 6) may be high.
Connection	When a call arrives from the network, the RTS (pin 4) is raised. DSR (pin 6) is monitored. If it is high or goes high, the PAD raises DTR (pin 20) and waits for DCD (pin 8) to go high. The PAD accepts the call from the network after DSR and DCD are detected high.
Disconnection	The PAD monitors DSR (pin 6) and if it is low for at least 50 milliseconds, the call is cleared. The control signals RTS, DTR, and DRO (pins 4, 20, and 14) are dropped, and the PAD returns to the idle state. If the call is cleared by the network, while waiting for DCD to be raised. RTS and DTR (pins 4 and 20) are dropped and the PAD returns to the idle state after DSR is lowered. The PAD will not accept another dial-out attempt until DSR is lowered. If DCD is not raised within 30 seconds of MB being raised, RTS and DTR (pins 4 and 20) are dropped and the call is cleared. If the call is cleared by the network while waiting for DSR to be raised, MB is immediately dropped. Once the call is connected, if the call is cleared from the network RTS, DTR, and DRO are dropped.

Chapter 2
Configuring the X.25 Protocol

Overview

Introduction

This Chapter describes the configuration of two Vanguard products in a basic X.25 application, and describes all X.25 configuration parameters.

Example X.25 Application

Figure 2-1 illustrates a basic X.25 application.

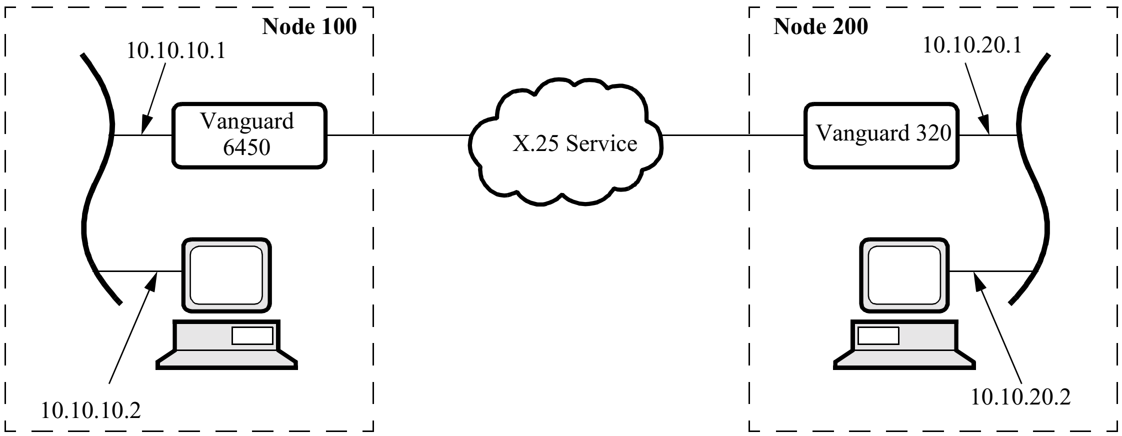

Figure 2-1. Basic X.25 Application

If You Want to Configure this Application

If you want configure the X.25 application in Figure 2-1, you will need this equipment:

- A Vanguard 320 and a Vanguard 6450, each loaded with Vanguard Applications Ware.
- 2 straight-thru cables.
- 1 DB-9 to DB-25 CTP cable.
- 2 personal computers.
- 1 Ethernet LAN hubs and cables.
- Access to X.25 service.

What About Loading Software?

Your Vanguard device should be loaded with Vanguard operating software and operational before you try to connect to the Control Terminal Port. If you require assistance in connecting to the CTP or accessing a node, refer to the *Vanguard Configuration Basics Guide* (Part Number T0113).

Use your Vanguide operator’s guide to set up your Vanguard hardware.

You should also make sure you have the correct software license installed. For the examples in this manual, the default image shipped with your Vanguard will work fine. If you need to load new operating software, refer to the *Vanguard 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 *Vanguard Software Builder Manual*, (Part Number T0030 found on the Vanguide CD-ROM) for more details.

Configuring the Example X.25 Application

What Do I have To Configure?

This table lists the records you need to configure for the application example shown in Figure 2-1.

Configure The...	*Result*
Node Record on the Vanguard devices.	This gives both nodes a name and address.
Port Record on the Vanguard 320 (Node 200) and Vanguard 6450 (Node 100).	This will tell the node that the X.25 protocol is used on the selected port. You are going to have to do this for both the Vanguard 320 and 6450.
LAN Connections on both devices.	This lets you set up the LAN connections you need and create the entries that setup communication between the LAN interfaces.
Mnemonic Table	This provides a short form name to call the other node. You only have to configure the Mnemonic Table in the node that is making the call. If you want to initiate a call from both nodes, then both must have the Mnemonic Table set up.
Boot the Nodes	Booting the node, after making changes, saves those changes into the devices Configuration Memory (CMEM). You need to do this for both of the nodes in this example.

Additional Information

This chapter describes how to configure the example application shown in Figure 2-1. As such, it focuses only on those parameters that must be changed from the default values in order to make the example work. it is important though, for you to understand exactly what all of the parameters mean and the implications of making modifications. Therefore, immediately following the configuration information for this example, all X.25 configuration parameters (even those that do not have to be addressed for this example) are identified and defined.

Configuring the Node Record

Introduction

The first thing you need to do is configure the Node record on your Vanguard. Use the CTP to display the Node record and fill out the required parameters.

Configuration

Complete these steps to configure the Node record:

Step	*Action*	*Result/Description*
1	Select **Configure** from the CTP Main menu.	The Configure menu will appear.
2	Select **Node** from the Configure menu.	The Node record will appear.
3	Fill out these parameters	
	• Node Name:	This can typically be any name that you want to assign to your node. In the case of this example, these node names are being used: • VG6450 for the Vanguard 6450 • VG320 for the Vanguard 320 ■ **Note** You should always try to follow the naming conventions used in your network. If one does not currently exist, you should create one.
	• Node Address:	This can be any number of digits (to a maximum of 13). In the case of this example, these node addresses are being used: • Vanguard 6450 device uses address 100 • VG320 for the Vanguard 320 uses address 200 ■ **Note** You should always try to follow the addressing conventions used in your network.
4	You can use the default values for the remaining parameters so type a semicolon (**;**) and press **Return**.	This saves the record.

Configuring the Port Record

Navigating the CTP

Figure 2-2 shows the X.25 port configuration parameters you will find once you access the CTP port.

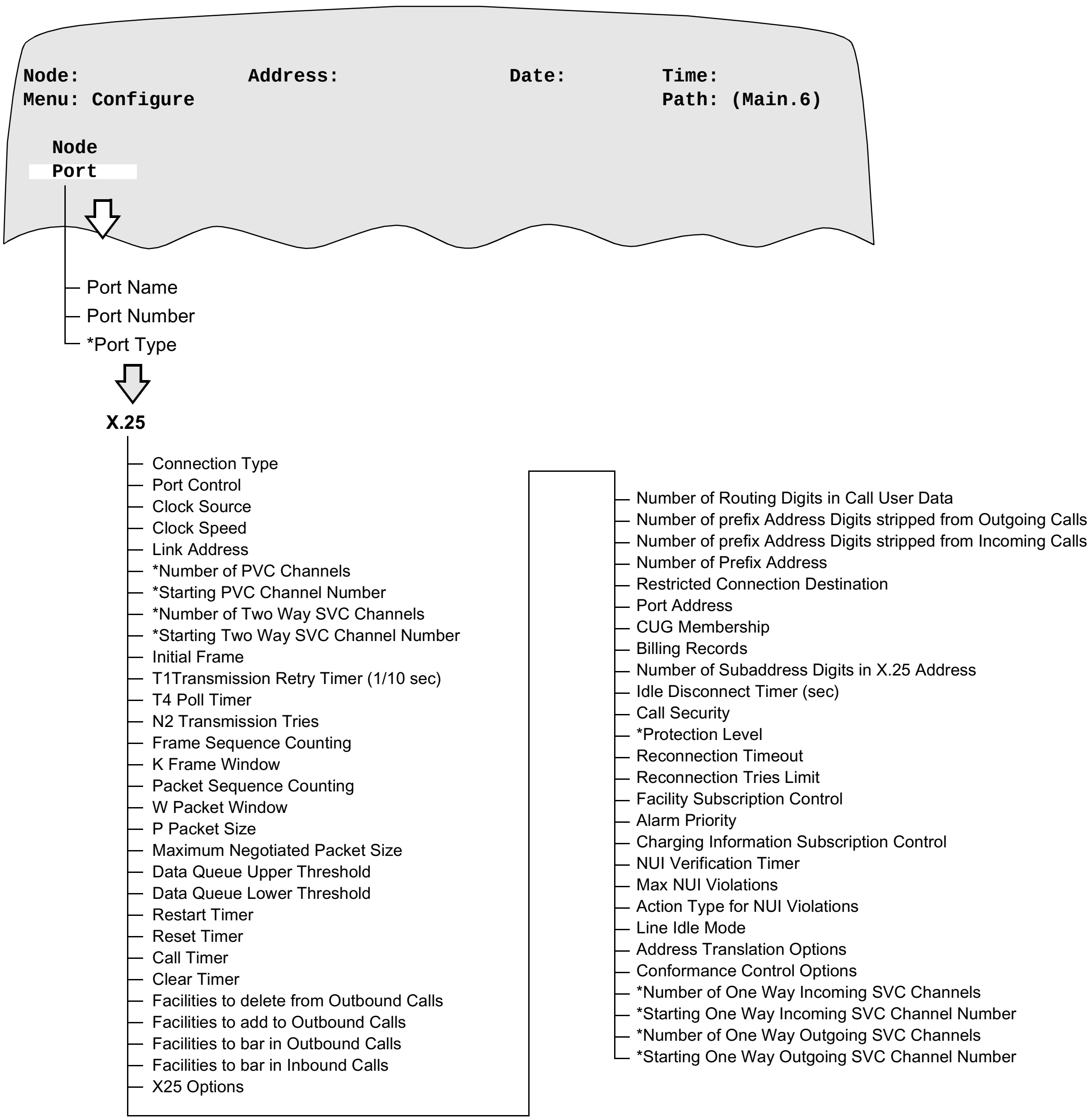

Figure 2-2. X.25 Port Record

Configuration Guidelines

Use these guidelines to configure X.25 parameters:

When You Configure...	*Then...*
SVC Channel range	The PVC Channel range should be below the SVC Channel range with no overlap. The total number of configured SVCs and PVCs combined must not exceed 4096.
T1 Transmission Retry Timer	T4 Poll Timer parameter value must be greater than T1 Transmission retry timer.
Window size with NORM (modulo 8) sequence counting	Window size cannot exceed 7.
Connection Type as SIMPv or DIMOv	Configure BKUP option.
X.25 Options as PDN+CUD	An Outbound Translation Table entry must exist.
X.25 Options as CUG	Enter a value for CUG Membership.
X.25 Options as CUD	Outbound Translation Table entries must use OLDA option.
X.25 Options as REGO or REGI	Port address must not be blank.
X.25 Options INL and PDN	They are mutually exclusive.
X.25 Options as BKUP	Connection Type must be DIMO/a/b, EMRI, or EMDC.
Idle Disconnect Timer	Connection must be DIMO/a/b with BKUP option set.
Billing Records as On	Specify Billing Printer Mnemonic in the Mnemonic Table.

Configure the Port Record on the Vanguard 320

Follow these steps to configure the Port Record for the Vanguard 320 (Node 200):

Step	*Action*	*Result/Description*
1	Select **Configure** from the CTP Main menu.	The Configure menu will appear.
2	Select **Port** from the Configure menu.	The port configuration parameters will start to appear on the screen. Press return to move through the list of parameters. Pressing the Backspace key will display the previous Port Record parameter.
3	Fill out these parameters	
	• Port Number:	The port number refers to the physical port on the back of the Vanguard 320. This is also the reference number of the port record. For this example, enter port number **3**.
	• Port Type:	This identifies the type of port you are configuring. Enter **X25** for the port type. If you are not sure what port types are available for the port number you have entered, type a question mark (**?**) at the Port Type prompt and press return. Allowable types will be displayed and, when necessary, an explanation given.
	• Clock Speed:	This is the speed at which the selected port will transmit/receive data. For this example, enter **64000**. ■ **Note** The highest speed depends on card type and the port interface. Refer to the Installation Guide for your platform.
4	You can use the default values for the remaining parameters so type a semicolon (**;**) after entering the Clock Speed and press **Return**.	This saves the record.

Configure the Port Record on the Vanguard 6450

To complete this configure the Port Record configuration for the Vanguard 6450 (Node 100), you must have the Configure Port menu displayed. Perform Steps 1 and 2 from the previous procedure, and fill out these parameters:

After entering the final parameter, you can use the default values for the remaining parameters by typing a semicolon (**;**) and pressing the Return key.

Parameter	***Configuration Description***
Port Number:	The port number refers to the physical port on the back of the Vanguard 320. This is also the reference number of the port record. For this example, enter port number **3**.
Port Type:	This identifies the type of port you are configuring. Enter **X25** for the port type. If you are not sure what port types are available for the port number you have entered, type a question mark (**?**) at the Port Type prompt and press return. Allowable types will be displayed and, when necessary, an explanation given.
Clock Source:	Set this parameter to **EXT**. This indicates that an external device (the PC) will be providing clocking for this node.
Clock Speed:	This is the speed at which the selected port will transmit/receive data. For this example, enter **9600**.
Link Address:	Set this parameter to **DTE**. Making this selection sets the port's logical address to operate with the X.25 protocol. This means that the port's logical address must complement the logical address of the X.25 port on Node 200. ■ **Note** If the X.25 port on Node 100 is DTE, the X.25 port on Node 200 must be DCE.
W Packet Window:	Set this parameter to **2** to specify the default packet level window size.
P Packet Size:	Set this parameter to **128**. This determines the maximum default packet size (in bytes) for inbound and outbound calls on the X.25 link.
Data Queue Upper Threshold:	Set this parameter to **63** since you may want to use large data packets. This parameter specifies the maximum number of data packets a channel on the X.25 port can queue for transmission before flow control is invoked.
Data Queue Lower Threshold:	Set this parameter to **15**.

Configuring the LAN Connections

Introduction

Making the LAN connections involves modifying parameters in the two records shown below and illustrated in Figure 2-3:

- LAN Connection Parameters
- LAN Connection Table

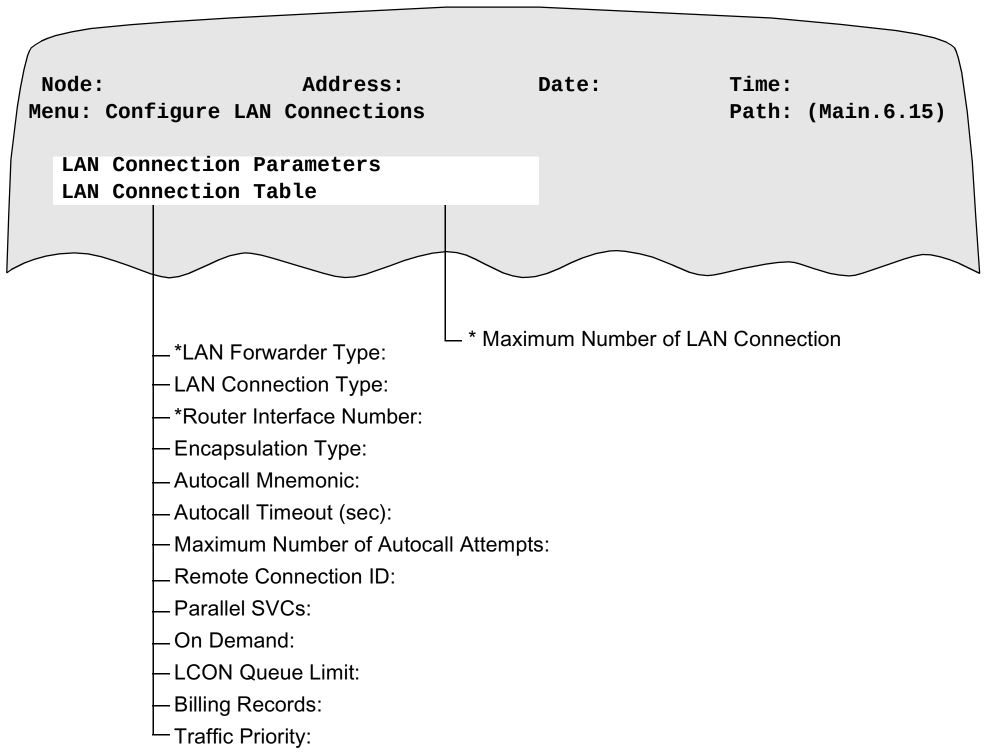

Figure 2-3. Configuring The LAN Connections

LAN Connection Parameters

The LAN Connection Parameters record lets you configure up to 250 LAN connections. The default is 32. In a real life application you may require additional LAN connections, however, for our purposes we only need to configure one LAN connection. Because the default values for the LAN Connection Table are sufficient for our example, you must access the table and save it. If you don't save it, the connections will not be made because you have not saved your changes to CMEM.

Step	*Follow These Steps*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears
2	Select **Configure LAN Connections** from the Configuration menu.	The Configure LAN Connection menu appears.
3	Select the **LAN Connection Parameters** from the Configure LAN Connection menu.	The LAN Connection Parameters record appears.
4	***Fill out these parameters***	***Description***
	Maximum Number of LAN Connections	This identifies the maximum number of LAN connections you want to configure for your node. For our purposes, we only need one LAN connection, so the default value of 32 is okay for now.
5	Type a semicolon (**;**) and press Return.	This saves the record.

Configuring the VG64500 LAN Connection Table Record

This is where configuring the Vanguard gets a little tricky. After you define the number of maximum LAN connections you want, you need to set up the actual LAN connections. This mean you need to connect LAN connection entries to actual interfaces inside the Vanguard so the node knows where to route traffic.

Step	*Follow These Steps*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears
2	Select **Configure LAN Connections** from the Configuration menu.	The Configure LAN Connection menu appears.
3	Select the **LAN Connection Table** from the Configure LAN Connection menu.	The LAN Connection Table appears.
4	***Fill out these parameters***	***Description***
	Entry Number	This is the entry number used to reference this record. This entry is mapped to a particular LAN interface. Type **1** (if it isn't already displayed) and press return.
	Interface #	Type **5** and press Return. This means the LAN Forwarder uses interface #5 to send LAN traffic to the WAN Adapter.

Step	***Follow These Steps***	***Result** (Continued)*
4 (Cont'd)	LAN Forwarder Type	This tells the LAN Forwarder how to pass traffic to the WAN Adapter. Since we're basically routing traffic, the default value ROUT is okay for our example.
	Autocall Mnemonic	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 our purposes, we'll set up the local node to do the calling. This means you need to configure an autocall name here. Type **320LAN** and press Return. Do not put any value in this parameter for the remote node.
	Maximum Number of Autocall Attempts	Set this parameter to zero (**0**) because we 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 a lesser value.
	Remote Connection ID	This specifies where the LAN Connection SVC call in the local node connects to the WAN Adapter in the remote node. This 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, this is where you connect your LCON entry in the local node to the WAN adapter interface in the remote node. Use the default value of **1** for the entry.
5	Everything else in the record can be set to the default values, so type a semicolon (;) after the last value and press Return.	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.

Configuring the Mnemonic Table

Introduction

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 used by the Vanguard to make calls to another node. You can configure up to 64 Mnemonic names if you need to, but for our purposes we only need one Mnemonic name.

Configuration

Follow these steps to fill out the Mnemonic Table.

Step	*Follow These Steps*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears
2	Select **Configure Network Services** from the Configuration menu.	The Configure Network Services menu appears.
3	Select the **Mnemonic Table** from the Configure Network Services menu.	The Mnemonic Table record appears.
4	***Fill out these parameters***	***Description***
	Entry Number	This identifies the Mnemonic Table entry. Use the default value **1**.
	Mnemonic Name	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, so type **320LAN** if you're following along with the example.
	Call Parameters	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. Basically, the LAN connection of one node connects to the WAN adapter of a remote node. That is what you are defining here. The default subaddress for a Vanguard LAN adapter is 94. So, type **20094** to call node 200 and connect to the LAN Adapter.
5	Everything else in the record can be set to the default values, so type a semicolon (**;**) after the last value and press Return.	This saves the record.

Configuring the T1/E1 Interface

Introduction

This section explains how to configure the parameters in the T1/E1 Interface.

Configuration Process

Here are the important steps in the configuration process:

- Use the configuration menus to configure the T1/E1 line according to the Service Provider's specification.
- Associate time slots to the application ports.
- If:
  - no CMEM record exists, a default CMEM record is generated when the node recognizes a T1./E1 Daughter Card.
  - a CMEM Record exists, but is incompatible with the Daughter Card type, the card is initialized with the appropriate default record.

Mapping Ports to Channels

When configuring a T1/E1 interface on a 6400 Series device, refer to this table to map ports to channels:

T1/E1 Interface	*Channel No.*	*Port No.*
1	1	7
1	2	8
1	3	9
2	1	10
2	2	11
2	3	12
3	1	13
3	2	14
3	3	15

Configure T1/E1 Interface

To configure the T1/E1 Interface perform these tasks:

Step	***Action***
1	From the configuration menu, select Configure T1/E1 Interfaces.
2	At the T1/E1 Interface prompt (See Figure 2-4), select the interface.
3	The first T1/E1 parameter appears (Entry Number). Configure the parameters. Figure 2-5 shows the T1 parameters and Figure 2-6 shows the E1 parameters. For detailed descriptions of the parameters go to the “Parameters” section on page 2-18.

T1/E1 Interface Menus

This section shows several T1/E1 configuration menus:

- Figure 2-4 shows the T1/E1 Interface selection menu.
- Figure 2-5 shows Configure T1/E1 Interface record and parameters when the Interface Type = T1.
- Figure 2-6 shows Configure T1/E1 Interface record and parameters when the Interface Type = E1.

```
Node:          Address:              Date:          Time:
Menu: Configure T1/E1 Interface          Path: (Main.6.19)
   1. T1/E1 Interfaces  <- 6450 1,2 or 3, v320 1 or 2


#Enter Selection:
```

Figure 2-4. T1/E1 Interface Selection Configuration Screen

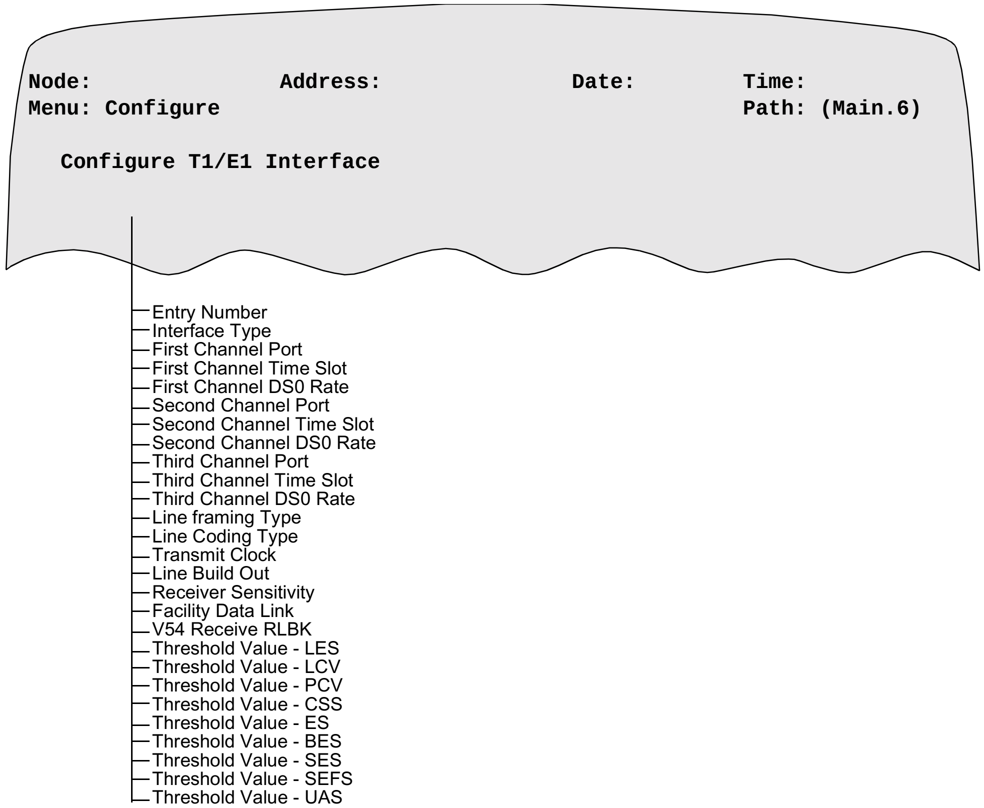

Figure 2-5. T1 Interface Configuration Screen

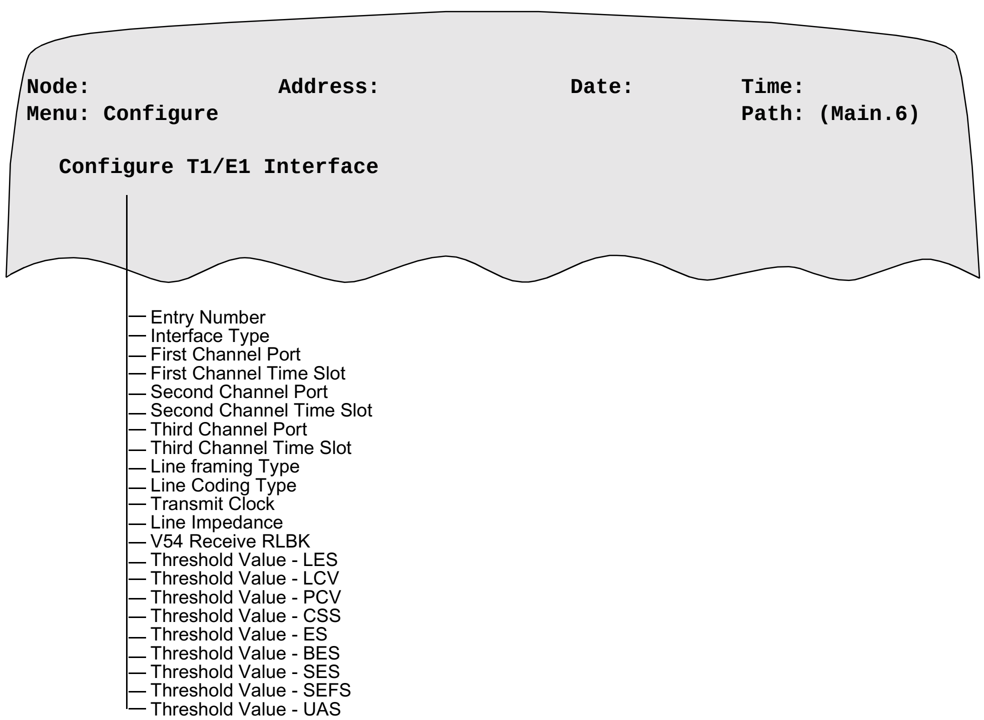

Figure 2-6. E1 Interface Configuration Screen

Parameters

Here are the parameters for configuring the T1/E1 Interface.

Interface Type

Range:	T1, E1
Default:	T1
Description:	Specifies the type of interface you are configuring.
Boot Type:	A change to this parameter requires a node boot to take effect.

First Channel Port

Range:	10, 0
Default:	10
Description:	Specifies the first of the Channel/Port associations. Refer to “Mapping Ports to Channels” section on page 2-15. Set to 0 (zero) when no data activity is specified on the First FT1/FE1 Channel The port must be configured to Bit Oriented Protocol, X25, or FRI.Also, the first port of each T1 or E1 Interface (ports 7, 10, and 13) must be used if the interface is installed. The other two ports are optional based on the application.

First Channel Timeslots

Range:	For T1: 0, 1 to 24 For E1: 0, 1 to 31
Default:	0
Description:	Specifies the time slot assignments for the first channel. For no channel, set to 0 (zero). You can select an individual time slot or time slot ranges (for example to select 2, 3, 4, 10, 12, 13, 14 enter 2-4, 10, 12-14.) ■ **Note** If a time slot is assigned to more than one channel, CMEM is not saved and an error message is generated. If you set this parameter to 0 (zero), the associated port does not receive the clock and is unusable.

First Channel DSO Rate

Range:	56, 64
Default:	56
Description:	Specifies the DS0 Rate for the first T1 Channel. Set this parameter as specified by service provider for each end of the circuit. If one end is set to 56, both ends must be set to 56. This parameter appears only when Interface Type = T1.

Second Channel Port

Range:	0, 11
Default:	11
Description:	Specifies the second of the Channel/Port associations. Refer to the “Mapping Ports to Channels” section on page 2-15 Set to 0 (zero) when no data activity is specified on the First FT1/FE1 Channel. **■Note** The port must be configured to Bit Oriented Protocol, X25, or FRI.Also, the first port of each T1 or E1 Interface (ports 7, 10, and 13) must be used if the interface is installed. The other two ports are optional based on the application.

Second Channel Timeslots

Range:	0, 1 to 24 for T1 0, 1 to 31 for E1
Default:	0
Description:	Specifies the time slot assignments for the second Channel. For no channel set to 0 (zero). You can select an individual time slot or time slot ranges (for example to select 2, 3, 4, 10, 12, 13, 14 enter 2-4, 10, 12-14.) **■Note** This parameter does not appear when configuring a Vanguard 320.

Second Channel DSO Rate

Range:	56, 64
Default:	56
Description:	Specifies the DS0 Rate for second T1 Channel. Set this parameter as specified by service provider for each end of the circuit. If one end is set to 56, both ends must be set to 56. This parameter appears only when Interface Type = T1.

Third Channel Port

Range:	0, 12
Default:	12
Description:	Specifies the third of the Channel/Port associations. Refer to the "Mapping Ports to Channels" section on page 2-15 Set to 0 (zero) when no data activity is specified on the First FT1/FE1 Channel. ■ **Note** The port must be configured to Bit Oriented Protocol, X25, or FRI.Also, the first port of each T1 or E1 Interface (ports 7, 10, and 13) must be used if the interface is installed. The other two ports are optional based on the application.

Third Channel Timeslots

Range:	0, 1 to 24 for T1 0, 1 to 31 for E1
Default:	0
Description:	Specifies the time slot assignments for the second Channel. For no channel set to 0 (zero). You can select an individual time slot or time slot ranges (for example to select 2, 3, 4, 10, 12, 13, 14 enter 2-4, 10, 12-14.) ■ **Note** This parameter does not appear when configuring a Vanguard 320.

Third Channel DSO Rate

Range:	56, 64
Default:	56
Description:	Specifies the DS0 Rate for the third T1 Channel. Set this parameter as specified by service provider for each end of the circuit. If one end is set to 56, both ends must be set to 56. This parameter appears only when Interface Type = T1.

Line Framing Type

Range:	For T1: ESF, SF For E1: E1, E1_CRC, E1_CRC_FEBE
Default:	For T1: SF For E1: E1
Description:	For T1: Specifies the type of framing used by the DS1 circuit. • ESF: Extended Super Frame • SF: Super Frame This parameter is specified by the service provider. SF is also called D4. For E1: Specifies the type of framing used by the DS1 circuit. • E1: D2048S or D2048U. • E1_CRC: D2048S with CRC. • E1_CRC_FEBE: D2048S with CRC and Si = FEBE. The maximum data rate is 1,984 kbps. Framing Type E1 meets the demands for the TBR13 Structured leased line D2048S, and TBR12 UnStructured D2048U parameters.

Line Coding Type

Range:	For T1: B8ZS, AMI For E1: HDB3, AMI
Default:	For T1: AMI For E1: HDB3
Description:	For T1: Specifies the type of line coding used for T1 applications. Selects variety of zero suppression used on the T1 link. • B8ZS: Bipolar 8 Zero Substitution. • AMI: Alternate Mark Inversion. This parameter is specified by the service provider. **■ Note** The FT1 card supports only the B8ZS and AMI line coding types. It dos not support the B7 line coding type as the Regional node T1/E1. For E1: Used to selects the variety of zero suppression used on the T1 link. • AMI: Alternate Mark Inversion. • HDB3: High Density Bipolar 3 This parameter is specified by the service provider.

Transmit Clock

Range:	INT, REC
Default:	REC
Description:	Selects the source of the transmit clock. • INT: Internal Timing, use when timing is not provided by the Network. • REC: Received Timing, use when connected to Public or Private Network. In most cases set this parameter to REC timing is used. Use INT in point to point applications, where one unit is set to INT and the other one to REC. When Loopback tests are run, set the unit automatically switches to INT.

Line Impedance

Range:	120, 75
Default:	120
Description:	Specifies the line impedance (in Ohms) as 75 or 120 The value is specified by the service provider. This parameter appears only when Interface Type = E1. **■ Note** When switching impedance, you must change the connectors to BNC/Modular 8 Pin Jack.

Line Build Out

Range:	0 to 7
Default:	0
Description:	Specifies the Line Build Out to match the physical interface. This parameter appears only when Interface Type = T1. For a DSX Interface, set the number based on the cable length. • 0: 0 ft. to 133 ft. • 1: 134 ft. to 266 ft. • 2: 267 ft. to 399 ft. • 3: 400 ft. to 533 ft. • 4: 534 ft. to 655 ft. For a DS1 Interface, set the number based on signal level. • 0: 0 dB • 5: 7.5 dB • 6: 15 dB • 7: 22.5 dB • 4: Not valid for DS1 interfaces DS1 and DSX interfaces are provided via the same 8 Pin Modular Jack. For DS1, the service provider specifies the setting. For DSX, the cable installer can provide the cable length.

Receiver Sensitivity

Range:	LOW, HIGH
Default:	LOW
Description:	Specifies the sensitivity of the receiver: • HIGH: -36 dB • LOW: -30 dB This parameter appears only when Interface Type = T1. Generally, use -30 dB when connected directly to the T1 line. This allows for nominal noise immunity. For some marginal cable lengths and line loss, use the -36 dB setting.

Facility Data Link

Range:	NONE, ANSI, ATT
Default:	NONE
Description:	Specifies the use of the facility data link channel. This parameter appears only when Interface Type = T1. Set this parameter according to carrier specifications.

V54 Receive RLBK

Range:	Disable, Enable
Default:	Disable
Description:	• Enable: Interface will respond to incoming V54 loopback Request. • Disable: Interface will not respond to incoming V54 Loopback Request.

Threshold Values - LES

Range:	1 to 255
Default:	10
Description:	Specifies the threshold value for the Line Errored Seconds (LES) report. When this value is exceeded within a 15 minute interval, a report is generated. There can be only one report per 15 minute interval. ■ **Note** A Line Errored Second is a second in which one or more Line Code Violation error events are detected.

Threshold Value - LCV

Range:	1 to 255
Default:	10
Description:	Specifies the threshold value for the Line Coding Violation (LCV) report. When this value is exceeded within one 15 minute interval, a report is generated. There is only one report per 15 minute interval. ■ **Note** Line Coding Violation is the occurrence of either a Bipolar Violation (BPV) or Excessive Zeroes (EXZ) Error Event.

Threshold Value - PCV

Range:	1 to 255
Default:	10
Description:	Specifies the threshold value for a Path Coding Violation (PCV) report. When this value is exceeded within a 15 minute interval a report is generated. There can be only one report per 15 minute interval. The Path Coding Violation error event is: • for D4 and E1 non-CRC formats: frame synchronization bit error • for ESF and E1-CRC formats: CRC error.

Threshold Value - CSS

Range:	1 to 255
Default:	10
Description:	Specifies the threshold value for Controlled Slip Seconds (CSS) report. When this value is exceeded within a 15 minute interval, a report is generated. There can be only one report per 15 minute interval. Controlled Slip Seconds is the replication or deletion of an E1/T1 frame. This parameter is applicable only when the Transmit Clock = INT.

Threshold Value - ES

Range:	1 to 255
Default:	10
Description:	Specifies the threshold value for the Errored Seconds (ES) report. When this value is exceeded within one 15 minute interval, a report is generated. There can be only one report per 15 minute interval. Errored Seconds for D4 and E1 non-CRC formats is a second with one or more Bipolar Violation. Errored Seconds for ESF and E1-CRC formats is a second with one or more Path Code Violation or one or more Out Of Frame or Controlled Slips.

Threshold Value - BES

Range:	1 to 255
Default:	10
Description:	Specifies the threshold value for the Bursty Errored Seconds (BES) report. When this value is exceeded within one 15 minute interval a report is generated. There can be only one report per 15 minute interval. Bursty Errored Seconds is a second with fewer than 320 and more than one Path Coding Violation error events, and no Severely Errored Frame defects. Controlled Slips are not included in this parameter. Bursty Errored Seconds is not incremented during an Unavailable Second.

Threshold Value - SES

Range:	1 to 255
Default:	10
Description:	Specifies the threshold value for Severely Errored Seconds (SES) report. When this value is exceeded within one 15 minute interval, a report is generated. There can be only one report per 15 minute interval. Severely Errored Seconds for D4 formats is a second with 1544 or more Line Coding Violations (LCV) or an OOF defect. Severely Errored Seconds for ESF formats is a second with 320 or more Path Code Violations or one or more Out of Frame defects or a detected AIS defect. Severely Errored Seconds for E1-CRC formats is a second with 832 or more Path Code Violations or one or more Out of Frame defects. Severely Errored Seconds for E1 non-CRC formats is a second with 2048 or more Line Coding Violations (LCV). Controlled Slips are not included in this parameter. Severely Errored Seconds is not incremented during an Unavailable Second.

Threshold Value - SEFS

Range:	1 to 255
Default:	10
Description:	Specifies the threshold value for Severely Errored Framing Seconds (SEFS) report. When this value is exceeded within one 15 minute interval, a report is generated. There can be only one report per 15 minute interval. Severely Errored Framing Seconds is a second with one or more Out of Frame defects or a detected AIS defect.

Threshold Value - UAS

Range:	1 to 255
Default:	10
Description:	Specifies the threshold value for the Unavailable Seconds (UAS) report. When this value is exceeded within one 15 minute interval, a report is generated. There can be only one report per 15 minute interval. Unavailable Seconds is the number of seconds that the interface is unavailable. The DS1 interface is said to be unavailable after 10 contiguous SESs.

Booting the Node or Port

Introduction

After configuring X.25 parameters, it may be necessary to boot either the port or node. Some Vanguard Applications Ware configuration parameters are displayed on your computer screen with an asterisk (*) in the parameter name. Whenever this occurs, it is an indication that you must perform a Node boot for any changes you make, to that parameter, to take effect.

This section explains how to perform a node or port boot.

Booting IPX Parameters

Follow these steps:

Step	Action	Result
1	Select **Boot** from the CTP Main menu.	The Boot menu will appear.
2	Select the type of boot operation you want to perform.	The Boot Router menu will appear.
3	Type Y at the prompt.	The node will reset itself and implement the changes you have made to the Vanguard CMEM.
	or...	
	Type N at the prompt	The Boot menu appears.

■ **Note**
Refer to the *Vanguard Configuration Basics Manual* for additional information on booting Vanguard products.

X.25 Configuration Parameters

Introduction

This section describes all X.25 configuration parameters and provides you with some detailed information describing Vanguard Managed Solutions's implementation of several X.25 features.

Port Record Configuration Parameters

Introduction

You can configure these parameters from the Configure -> Port menu.

Any parameter title containing an asterisk (*) indicates that a Node boot must be performed if any changes to that parameter are to take effect.

■ **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, refer to the Ease of Configuration section in the introductory portion of the *Basic Protocols Manual,* Part Number T0106.

Connection Type

Range:	SIMP, DTR, DTRD, DIMO, DIMOa, DIMOb, DIMOv, EMRI, EMDC, SIMPv
Default:	SIMP
Description:	Specifies the type of control signal handshaking that is required before logical connections can be made to this port. Refer to Appendix H for additional details on connection types. See "Connection Types" for more information about each connection type.

Port Control

Range:	MB, NONE
Default:	NONE (disables the Make Busy feature)
Description:	MB enables the make-busy feature for the specified port; disabling the port raises pin 22 only when Connection Type = DIMO, DIMOa, DIMOb, DTR, DTRD, or SIMP.

Clock Source

Range:	EXT, INT
Default:	EXT
Description:	• INT: Port provides clocking • EXT: External device provides clocking signals

Clock Speed

Range:	1200 to 2048000
Default:	9600
Description:	Port speed in bits per second (enabled only when Clock Source = INT). ■ **Note** The highest speed depends on card type and the port interface. Refer to the Installation Guide for your platform.

Invert TX Clock

Range:	NO, YES
Default:	NO
Description:	Specifies whether the phase of the transmit clock should be inverted. This parameter is primarily intended for X.21 electrical interfaces. • NO; Don't invert • YES; Invert

Link Address

Range:	DTE, DCE, Negotiate
Default:	DTE
Description:	Sets the port's logical address to operate with the X.25 protocol, which dictates that a port's logical address must complement the logical address of the port on the other end of the link. • If port A is logically defined as DTE, port B must be defined as DCE. • Set to DTE when it is connected to a PDN port (because all PDN ports are defined as DCE). • Define the port that is topologically closest to the network's central control site as DCE when configuring X.25 ports for remote 6500*PLUS* nodes. • Define ports facing the next intermediate, or endpoint of the network, as DTE to let nodes link with adjacent nodes and to gain control of the remote node should it operate with a default configuration. • Use Negotiate to enable the port to modify itself to complement the link address of the node at the other end of the link.

*Number of PVC Channels

Range:	0 to 128
Default:	0
Description:	Specifies the maximum number of logical channels used for Permanent Virtual Circuits. The total number of PVC and SVC channels on a link should be as small as possible. PVC connections must be configured in the PVC Table.

*Starting PVC Channel Number

Range:	1 to 4095
Default:	1
Description:	The starting logical channel number for the Permanent Virtual Circuits on this link. ■ **Note** If *Number of PVC Channels = 0, this parameter is ignored.

*Number of Two Way SVC Channels

Range:	0 to 4096
Default:	16
Description:	Specify the number of logical channels used in Two Way Switched Virtual Circuit (SVC) channels for this port. You can configure up to 4096 SVC channels per port. However, keep the number of configured PVC and SVC channels per port as small as possible. The total number of configured SVCs and PVCs combined can not exceed 4096. If you configure the maximum number of SVC channels on a port, set the Maximum Simultaneous Calls parameter on the corresponding Node record to zero (0) to support an unlimited number of calls, or enter the desired number of calls you expect pass. ■ **Note** The number of SVCs configured per port on a node is limited by the mount of available RAM. Eight megabytes (MB) of RAM is required to support the maximum number of 4096 SVC channels on one port per node (four MB on-board memory and four MB SIMM).

*Starting Two Way SVC Channel Number

Range:	0 to 4095
Default:	1
Description:	Specifies the starting logical channel number for the Two Way SVCs on this link. ■ **Note** If the parameter *Number of Two Way SVC Channels = 0, this parameter is ignored.

Initial Frame

Range:	NONE, SABM, DISC
Default:	SABM
Description:	Specifies the first frame the other end requires for link startup: • NONE: Do nothing (the other end starts) • SABM: Send SABM • DISC: Send DISC then SABM

T1 Transmission Retry Timer (1/10 sec)

Range:	1 to 254
Default:	30
Description:	Sets the T1 Retry Timer. • Set to a value less than the parameter T4 Poll Timer. • Avoid setting the value to less than 10. • If you use the DCP option, value on all INL or network links in the network should be the same. ■ **Note** Values are in tenths of a second: 30 = 3.0 seconds.

T4 Poll Timer

Range:	0, 10 to 255
Default:	40 (values are in tenths of a second: 40 = 4.0 seconds)
Description:	Sets the T4 Poll Timer. This parameter specifies how often an idle link is probed for assurance of a connection to the remote device. To disable this parameter, enter a value of 0. ■ **Note** Values are in tenths of a second: 30 = 3.0 seconds. ■ **Note** Set this parameter to a value greater than the parameter T1 Transmission Retry Timer.

N2 Transmission Tries

Range:	1 to 20
Default:	10
Description:	Specifies the maximum number of times a node attempts to complete a transmission.

Frame Sequence Counting

Range:	NORM, EXT
Default:	NORM
Description:	Specifies the type of frame-level sequence numbers the port uses: • NORM: Normal sequencing (Modulo 8) • EXT: Extended sequencing (Modulo 128) ■ **Note** Values must be the same for both ends of the link.

K Frame Window

Range:	1 to 63
Default:	7
Description:	Specifies the number of unacknowledged frames that can be outstanding at X.25 layer 2. • This parameter should be set relatively high when there is a high link delay to improve throughput. • Set this parameter to the same value for the devices on both ends of the link. • Set the parameter Frame Sequence Counting = EXT to select the values to 8 to 63. **■Note** To use the extended X.25 Window Size (modulo 128): • Set the INL option to Disabled. • Set the T1 Retry Timer to a value larger than your network's round trip delay time. Configure the adjacent port on the node to the X25/Annex G port as a X25/Annex G port. This is not mandatory, but it should improve performance with extended Window sizes.

Packet Sequence Counting

Range:	NORM, EXT
Default:	NORM
Description:	Specifies the type of packet level sequence numbers that the port uses: • NORM: Normal sequencing (Modulo 8) • EXT: Extended sequencing (Modulo 128) **■Note** Values must be the same for both ends of the link.

W Packet Window

Range:	1 to 63
Default:	2 7 for the Vanguard 7300 Series
Description:	Specifies the default packet level window size (X.25 layer 3) when it is not negotiated for the individual call. ■ **Note** Values must be the same for both ends of the link. ■ **Note** Set the parameter Packet Sequence Counting = EXT to select the values to 8 to 63. ■ **Note** To use the extended X.25 Window Size (modulo 128): • Set the INL option to Disabled. • Set the T1 Retry Timer to a value larger than your network's round trip delay time. ■ **Note** Configure the adjacent port on the node to the X25/Annex G port as a X25/Annex G port. This is not mandatory, but it should improve performance with extended Window sizes.

P Packet Size

Range:	128, 256, 512, 1024
Default:	128
Description:	Specifies the maximum default packet size (in bytes) for inbound and outbound calls on this X.25 link when packet size is not negotiated. ■ **Note** Values must be the same for both ends of the link.

Maximum Negotiated Packet Size

Range:	128, 256, 512, 1024
Default:	1024
Description:	Specifies the maximum negotiated packet size (in bytes) for inbound and outbound calls on this X.25 link.

Data Queue Upper Threshold

Range:	0 to 63
Default:	5
Description:	Specifies the maximum number of data packets a channel on this port queues for transmission before it invokes flow control to the attached channel. ■**Note** When applications that use large data packets are considered, set this value to **63**. ■**Note** To use the extended X.25 Window Size (modulo 128): • Set the INL option to Disabled. • Set the T1 Retry Timer to a value larger than your network's round trip delay time. ■**Note** Configure the adjacent port on the node to the X25/Annex G port as a X25/Annex G port. This is not mandatory, but it should improve performance with extended Window sizes.

Data Queue Lower Threshold

Range:	0 to 63
Default:	0
Description:	Specifies the minimum number of data packets a channel on this port queues for transmission when it releases flow control to the attached channel. ■**Note** When applications that use large data packets are considered, set this value to **63**. ■**Note** To use the extended X.25 Window Size (modulo 128): • Set the INL option to Disabled. • Set the T1 Retry Timer to a value larger than your network's round trip delay time. • Configure the adjacent port on the node to the X25/Annex G port as a X25/Annex G port. This is not mandatory, but it should improve performance with extended Window sizes.

Restart Timer

Range:	5 to 255 (seconds)
Default:	180
Description:	Specifies the length of time, in seconds, the node waits before an unacknowledged restart request is sent again.

Reset Timer

Range:	5 to 255 (seconds)
Default:	180
Description:	Specifies the length of time, in seconds, the node S waits before an unacknowledged reset request is sent again.

Call Timer

Range:	5 to 255 (seconds)
Default:	200
Description:	Specifies the length of time, in seconds, the node waits for the response to a call request. A call will clear whenever this timer expires. After two clear requests, the channel is marked as being idle.

Clear Timer

Range:	5 to 255 (seconds)
Default:	180
Description:	Specifies the length of time, in seconds, the node waits before an unacknowledged clear request is sent again. After two clear requests, the channel is marked as being idle.

Facilities to Delete from Outbound Calls

Range:	NONE, THRO, NUI, CUG, PROP
Default:	NONE
Description:	Specifies the facilities (which can be summed) that are deleted from outbound calls: • NONE: No facilities deleted • THRO: Delete throughput class negotiation • NUI: Delete NUI • CUG: Delete CUG • PROP: Delete all VanguardMS defined proprietary facilities. ■ **Note** The facility is negotiated to the configured value, not the maximum value. ■ **Note** Use summing to combine several parameter values. For example, THRO+NUI.

Facilities to Add to Outbound Calls

Range:	NONE, REV, PACK, WIND
Default:	NONE
Description:	Specifies the facilities (which can be summed) that are added to outbound calls: • NONE: No facilities added • REV: Reverse Charging added • PACK: Packet Size negotiation added • WIND: Window Size negotiation added ■ **Note** Use summing to combine several parameter values. For example, WIND+PACK.

Facilities to Bar in Outbound Calls

Range:	NONE, REV, FAST, BCUG, DGRAM
Default:	NONE
Description:	Specifies the facilities that, if present in an outbound call, will cause the call to be cleared: • NONE: No facility barred • REV: Reverse Charging barred • FAST: Fast select barred • BCUG: Bilateral Closed User Group barred • DGRAM: Datagram barred ■ **Note** Use summing to combine several parameter values.

Facilities to Bar in Inbound Calls

Range:	NONE, BCUG, DGRAM, REV
Default:	NONE
Description:	Specifies the facilities, if present in an inbound call, that clear the call: • NONE: No facility Blocked • BCUG: Bar Bilateral Closed User Group • DGRAM: Bar Datagram • REV: Bar Reverse Charging ■ **Note** Use summing to combine several parameter values.

X.25 Options

Range:	NONE, 1980, NUI, PDN, CUD, IBAR, OBAR, CBCK, CUG, CAUSE, HOLD, NRST, BKUP, INL, INLA, DELAY, AP, GP, CNUI, CNGL, CINFO
Default:	NONE
Description:	Defines the X.25 port operating characteristics. NONE: No options are specified 1980: The port is to operate with X.25/1980 implementation instead of 1984 or later versions. Post 1980 versions include changes that the 1980 version considers illegal or is incompatible with a particular implementation.

X.25 Options *(continued)*

Description: (Continued)	• NUI: An X.25 port validates an NUI facility for inbound calls. All inbound calls must have this facility present or the port clears them. If a call request successfully passes the NUI check, the NUI facility is stripped from the call request, which is then forwarded in the usual manner. If NUI is not selected, call requests with the NUI facility are forwarded with the facility intact. • Public Data Network (PDN): A port is connected to a PDN or non-VanguardMS router network using different addressing schemes. The port: • Selects PDN when these parameters are set to a value other than 0 (zero): – Number of Routing Digits in Call User Data. – Number of Prefix Address Digits Stripped from Outgoing Calls. – Number of Prefix Address Digits Stripped from incoming Calls. When PDN and CUD are selected, the network address and the Subaddress in the CUD: • For inbound calls: – Implement inbound called address translation using the Inbound Call Translation Table. • For outbound calls: – Implement outbound called address translation using the Outbound Call Translation Table. Or: – Strip the number of prefix digits specified in the port parameter Address Prefix Digits from the called address if no suitable entries exist in the Outbound Call Translation Table. PDN cannot be summed with INL. Call User Data (CUD): To specify that the subaddress for the call is carried in the call request's Call User Data (CUD) field. IBAR • Calls coming into the port are to be blocked. • Do not select IBAR and OBAR for a single port because they essentially disable the port; no status messages report this action. • Blocks calls leaving the port. • Do not select IBAR and OBAR for a single port because they essentially disable the port; no status messages report this action.

X.25 Options *(continued)*

Description: (Continued)	• CBCK Calls are to be routed back on the same link that received the call. The port number and address must be in the Routing Table. • CUG: Check CUG (Closed User Group) otherwise, call passes transparently. • CAUSE Passes cause codes in outbound packets. When not selected, cause codes are set to 00 in the Clear Request Packet. (Many X.25 implementations do not tolerate cause codes other than zeros in Clear Request Packets.) • HOLD: Calls are placed on hold when link level restarts occur. Individual logical channels can exchange resets, but the calls stay in place. Calls are lost, however, when the retransmission attempt expires, and the link is declared down. If data loss occurs, an indication is provided; a reset packet is not sent when the link comes up (after a short disruption); and the channel does not lock up. Both ends of the X.25 link must have X.25 Options = HOLD. • NRST: Suppresses the restart procedure at link-up time. Select when X.25 devices interpret the restart packet reception as a fault condition. • BKUP: Defines the port as a backup port that activates if other ports are down, enabling control signal operation when the link is idle. This value cannot be selected if Port Type is set to SIMP. • Internodal Link (INL): – Clears calls when call routing loops are detected because a link is down or an error exists in the route selection table. – Looks at clear calls and reroutes, improving unidirectional X.25 traffic. Window size is set to 7 or higher because internodal receiver readies (RRs) at levels 2 and 3 are reduced. – When selected, CAUSE is automatically selected. – If CAUSE is not selected, a warning message is printed. – INL cannot be summed with PDN. • INLA: When the link is connected to a node running revisions 2.10 and 2.12xx release (except revisions 2.12.05 and 2.13.34).

X.25 Options *(continued)*

	• Delay: Enable Delay and Path Trace on this link. Link must be connected to a Vanguard node.
	• AP: To recognize this port as an Access Protocol.
	• GP: To recognize this port as a Gateway Protocol.
	• CNUI: To select centralizd NUI verification.
	• CNGL: To reserve SVCs for NUIC operation.
	• CINFO: For charging Information.
■Note You can select several of these settings by summing the values. Example: CUG+HOLD.	

Conformance Control Options

Range:	None, CHKFAC
Default:	None
Description:	Specifies whether this X.25 will perform Facility Checking: • None: no Facility Checking is done. • CHKFAC: The port checks that: – the facility codes in the packet are valid. If not, the call is cleared with cause code 0, diagnostic code 65 (Facility/Registration code not allowed). – the facility code is allowed in this packet type. If not, with cause code 0, diagnostic code 65 (Facility/Registration code not allowed). The allowed facility codes are listed in this table. An X indicates that the Facility Code is allowed

Facility	***Facility Code Can Be Used in These Packet Types***							***Facility Code Bits***							
	Call Request	Incoming Call	Call Accepted	Call Connected	Clear Request	Clear Indication	DCE Clear Confer.	8	7	6	5	4	3	2	1
Flow Control parameter negotiation: - packet size - window size	X	X	X	X				0 0	1 1	0 0	0 0	0 0	0 0	1 1	0 1
Throughput class negotiation	X	X	X	X				0	0	0	0	0	0	1	0
Closed User group selection - basic format - extended format	X	X						0 0	0 1	0 0	0 0	0 0	0 1	1 1	1 1
Closed user group with outgoing access selection - basic format - extended format	X	X						0 0	0 1	0 0	0 0	1 1	0 0	0 0	1 0
Bilateral closed user group selection	X	X						0	1	0	0	0	0	0	1
Reverse charging	X	X						0	0	0	0	0	0	0	1
Fast Select	X	X													
NUI Selection	X		X					1	1	0	0	0	1	1	0

Facility *(continued)*	***Facility Code Can Be Used in These Packet Types***							***Facility Code Bits***							
	Call Request	Incoming Call	Call Accepted	Call Connected	Clear Request	Clear Indication	DCE Clear Confer.	8	7	6	5	4	3	2	1
Charging Information - requesting service - receiving information i) monitory unit ii) segment count iii) call duration	X		X			X	X	0 1 1 1	0 1 1 1	0 0 0 0	0 0 0 0	0 0 0 0	1 1 0 0	0 0 1 0	0 1 0 1
RPOA selection - basic format - extended format	X							0 1	1 1	0 0	0 0	0 0	1 1	0 0	0 0
Call deflection selection					X			1	1	0	1	0	0	0	1
Call redirection or deflection notification		X						1	1	0	0	0	0	1	1
Called line address modified notification			X	X	X	X		0	0	0	0	1	0	0	0
Transit delay selection and Indication	X	X		X				0	1	0	0	1	0	0	1
Marker	X	X	X	X	X	X		0	0	0	0	0	0	0	0
Reserved for extension								1	1	1	1	1	1	1	1

Number of Routing Digits in Call User Data

Range:	0 to 12
Default:	5
Description:	Specifies the number of routing digits in the Call User Data (CUD) field. This is used on X.25 links, attached to a PDN, where the private network address is carried in the CUD. ■ **Note** Set this parameter to 0 when the X.25 Options is *not* set to CUD. When the X.25 Options parameter is set to PDN, a non-zero value must be entered for this parameter.

Number of Prefix Address Digits Stripped from Outgoing Calls

Range:	0 to 14
Default:	0
Description:	Specifies the number of prefix digits that are removed from the called address when forwarding a call to a PDN. ■ **Note** When the X.25 Options parameter is set to PDN, a non-zero value must be entered for this parameter.

Number of Prefix Address Digits Stripped from Incoming Calls

Range:	0 to 15
Default:	0
Description:	Specifies the number of prefix digits that are removed from the called address when forwarding a call from a PDN. ■ **Note** When the X.25 Options parameter is set to PDN, a non-zero value must be entered for this parameter.

Restricted Connection Destination

Range:	0 to 32 alphanumeric characters
Default:	(blank);
Description:	Specifies the port destination of calls inbound from the port. This parameter overrides the Route Selection Table entries. For example, to route all calls to X.25 port 3, use X25-3. ■ **Note** Using the default disables this parameter.

Port Address

Range:	0 to 15 decimal digits
Default:	N/A
Description:	Specifies the address to be inserted into a call packet's calling address when the parameter X.25 Options = REGO or REGI.

CUG Membership

Range:	0 to 8 two-digit numbers
Default:	--,--,--,--,--,--,--,--
Description:	Specifies a port's membership in up to 8 Closed User Groups (CUGs). Each CUG membership must be a two-digit number (00 to 99), separated from other groups by a comma. ■ **Note** To delete a CUG, press the minus key twice for each group

Billing Records

Range:	OFF, ON
Default:	OFF
Description:	Billing Records summarize the data collected on calls to this port. • ON generates billing records for all calls to and from this port and for failed calls from this port. • OFF generates no billing records.

Number of Subaddress Digits in X.25 Address

Range:	0 to 3 digits
Default:	2
Description:	Specifies the number of digits in an X.25 address's subaddress for ports connected to a public data network.

Idle Disconnect Timer (sec)

Range:	0 to 3200
Default:	0 (set to 0 to disable)
Description:	Specifies how many seconds the X.25 port must be idle before it is automatically disconnected. Setting this parameter to 0 will disable the feature. Use this parameter only when: • The parameter Connection Type is set to DIMO, DIMOa, or DIMOb. • The parameter X.25 Options is set to BKUP.

Call Security

Range:	DISABLE, ENABLE
Default:	DISABLE
Description:	Specifies whether or not security is used before the port is detected as being up for ports used as a backup port (for Link Backup): • DISABLE: Outgoing and incoming calls are allowed. • ENABLE: Outgoing calls are enabled: incoming calls are terminated. ■ **Note** This parameter is valid only when the Link Backup Option has been implemented.

*Protection Level

Range:	NONE, CP_ONLY, FULL_DCP
Default:	NONE
Description:	Specifies how Data Connection Protection is implemented for this port. • NONE: The feature is turned off. • CP_ONLY: Connection protection only • FULL_DCP: Full data and connection protection ■ **Note** This parameter is valid only when the Data Connection Protection Option has been purchased for this node.

Reconnection Timeout

Range:	1 to 128
Default:	2
Description:	Specifies how many seconds the Data Connection Protection feature waits between reconnection attempts. ■ **Note** This parameter is valid when the Data Connection Protection Option has been implemented.

Reconnection Tries Limit

Range:	0 to 127
Default:	4
Description:	Specifies the number of times that the Data Connection Protection feature attempts to reconnect before clearing the call. If a zero (0) is entered, there will be no attempt to reconnect. ■ **Note** Valid only when the Data Connection Protection Option has been purchased for this node.

Facility Subscription Control

Range:	NONE, FCN_ON, FCN_OFF, TCN_ON, TCN_OFF, DBITMOD, CUGIA, REDIRECT, BCUG_ON, BCUGOA, BCUG_OFF
Default:	NONE

Facility Subscription Control *(continued)*

<table>
<tr><td>Description:</td><td>Flow Control Negotiation (FCN), Throughput Control Negotiation (TCN) and D-bit Modification (DBITMOD) are part of the facilities defined (in the X.2 standard) for data networks . They are facilities which can be turned on or off for a network subscriber.

The FCN, TCN and DBITMOD parameters can be implemented alone or in combination. For instance, you can use FCN_ON, TCN_OFF, and DBITMOD concurrently.

• NONE: Subscription to facilities not enforced.
• FCN_ON: Flow Control Negotiation enabled. Packet and Window size negotiation facilities in an inbound call are allowed. Packet and Window size facilities are always included in outbound calls and call accepted/connected when this parameter is set.
• FCN_OFF: Flow Control Negotiation disabled. Inbound calls containing Packet and Window size facilities are cleared. Packet and Window size facilities are not present in outbound calls and calls accepted/connected when this parameter is set.
• TCN_ON: Throughput Class Negotiation enabled. The throughput class negotiation facility is always included in outbound calls and call accepted/connected when this parameter is set. The facility is passed onward to the destination in the call packet transparently and does not alter the handling of the SVC data within the node.
• TCN_OFF: Throughput Class Negotiation disabled. Inbound calls containing the throughput class negotiation facility are cleared. The throughput class negotiation facility is not present in outbound calls and call accepted/connected when this parameter is set.
• DBITMOD: D-bit Modification Facility enabled. This facility sets the D-bit to 1 in every data packet traversing this port. Setting the D-bit to 1 enables packet delivery acknowledgment from the remote end. (When the D-bit is set to its default, 0, acknowledgment comes from the intermediary node.)
• CUGIA: Closed User Group Incoming Access enabled. This facility checks the CUG of incoming calls but allows incoming access from addresses that do not belong to the CUG.
• REDIRECT: Call Redirection enabled. This facility redirects inbound calls to a disabled or busy port to other ports. Alternate ports are defined by X.25 addresses in the Call Redirection table on the node which originated the call.
• BCUG_ON: Subscription to Bilateral Closed User Group facility enabled.
• BCUGOA: Subscription to Bilateral Closed User Group with Outgoing Access facility enabled.
• BCUG_OFF: Subscription to Bilateral Closed User Group facility disabled.

BCUG_ON, BCUGOA, and BCUG_OFF are mutually exclusive and can be enabled only on Access ports.</td></tr>
</table>

Facility Subscription Control *(continued)*

Description: (Continued)	• BCUG_OFF: Subscription to Bilateral Closed User Group related facilities disabled. **■ Note** BCUG_ON, BCUGOA, and BCUG_OFF options are mutually exclusive, and may be enabled only on Access ports. Some combinations of above options are allowed (e.g. FCN_ON+TCN_ON).

Alarm Priority

Range:	NETWORK, ACCESS
Default:	NETWORK
Description:	Specifies the severity level of LINK UP and LINK DOWN alarms: • NETWORK: Severity HIGH alarms are generated. • ACCESS: Severity LOW alarms are generated.

Charging Information Subscription Control:

Range:	NO, YES
Default:	NO
Description:	Specifies whether Charging Information has to be sent even without requesting. • NO: Charging Information will not be sent without Request. • YES: Charging Information will be sent.

NUI Verification Timer:

Range:	5 to 180
Default:	60
Description:	Specify the NUI verification timer in seconds. The call is cleared if timer expires.

Max NUI Violations:

Range:	0 to 100
Default:	10
Description:	The maximum number of successive NUI verification failures an X.25 DTE can tolerate when making verification attempts through X.25 port.

Action Type for NUI Violations:

Range:	NONE, DISC, DEGR, LOCK
Default:	NONE
Description:	This specifies the course of action to be taken if the NUI violations exceed the configured threshold count. This parameter is effective only if the X25 options parameter is set to CNUI. • NONE - No action is taken. • DISC - All connections on the port are broken. • DEGR - Port is busied-out for one minute then it is re-enabled. • LOCK - All connections on the port are broken and the port is disabled. Operator intervention is required to enable the port.

Line Idle Mode:

Range:	FLAG, MARK
Default:	FLAG
Description:	Specify one of these line idle mode options: • FLAG - Flag fill between frames • MARK - Mark idle between frames

Conformance Control Options:

Range:	NONE, CHKFAC
Default:	NONE
Description:	Select any of the following conformance control options: • NONE - no option specified • CHKFAC - Checking of facility codes enabled. **■ Note** Some of these options can be combined.

Address Translation Options:

Range:	NONE, DEDO, DEGO, REGO, REGSO, INGO, SAGO, INGI, REGI, SRGI, CUDR, DADA, DAGA, IADD
Default:	NONE
Description:	Select any of these address translation options: • NONE - no option specified **Outbound Call Processing:** • DEDO - delete called address • DEGO - delete calling address • REGO - replace calling address with configured Port Address • REGSO - replace calling address with configured Port Address plus Inbound Subaddress obtained from the Inbound Call Translation Table entry where Private Network Address matches the entire calling address • INGO - replace calling address with configured Port Address and retain original calling subaddress • SAGO - strip calling address, but retain subaddress **Inbound Call Processing:** • INGI - replace calling address with configured Port Address and retain original calling subaddress • REGI - replace calling address with configured Port Address • SRGI - select route from the Calling Address Translation Table by replacing the called address with the Private Network Address where the Inbound Calling Address matches the beginning of the calling address This option can not be summed with CUDR. • CUDR - CUD based Routing: The CUD string (configured in the CUD based Address Translation Table) will be searched in the CUD of the incoming call packet. If found, the called address will be replaced by the address configured in the CUD based Address Translation Table. This option can not be summed with SRGI. **Call Accept Processing:** • DADA - delete called address in inbound/outbound call accept • DAGA - delete calling address in inbound/outbound call accept • IADD - copy called and calling addresses from call request into outbound call accepted/connected **■ Note** Some of these options can be combined.

*Number of One Way Incoming SVC Channels:

Range:	0 to 4096
Default:	0
Description:	Specifies the number of logical channels used in One Way Incoming Switched Virtual Circuits. The total number of PVC, One Way Incoming, One Way Outgoing and Two Way SVC channels should be kept as small as possible and consistent with needs.

*Starting One Way Incoming SVC Channel Numbers:

Range:	0 to 4096
Default:	0
Description:	This is the starting logical channel number for the One Way Incoming Switched Virtual Circuits on this link. Not used if the number of One Way Incoming SVCs = 0.

*Number of One Way Outgoing SVC Channels:

Range:	0 to 4096
Default:	0
Description:	Number of logical channels used in One Way Outgoing Switched Virtual Circuits. The total number of PVC, One Way Incoming, One Way Outgoing and Two Way SVC channels should be kept as small as possible and consistent with needs.

*Number of One Way Outgoing SVC Channel Numbers:

Range:	0 to 4095
Default:	1
Description:	This is the starting logical channel number for the One Way Outgoing Switched Virtual Circuits on this link. Not used if the number of One Way Outgoing SVCs = 0.

Window Subtractor

Range:	0 to 63
Default:	0
Description:	Specifies the point in the receive window that the layer 3 acknowledgment is to be sent when there are not any packets to send in the reverse direction. The acknowledgment is sent when the number of packets equivalent to the W Packet Window minus the Window Subtractor has been received. If the W packet Window is 32 and the window subtractor is 8, the layer 3 acknowledgment is sent once 24 packets have been received. Setting the Window Subtractor to a non-zero value when INL or INL+INLB are set has no impact on the functionality of the routing loop detection feature of INL. It only effects functionality when the layer 3 acknowledgment is sent. If INL is specified and the subtractor is zero, the router uses the previous setting of 2. If INL+ INLB is specified and the subtractor is zero, the router will send an Acknowledgment for every packet received. This is also what occurs if INL nor INLB are not specified and the subtractor is zero. You should increase the value of the subtractor when you are using high speed end-to-end connections or when path delays are unusually high. This sends the acknowledgements sooner so the remote window stays open and the remote node can continue to send data without being stopped (waiting for an acknowledgement). The "Window Subtractor" Value is dependent on the "W" (packet) window setting and interacts with many other settings and factors such as the speed of the line, the "K" (frame) window setting, circuit propagation delay, etc. Tuning can result in CPU utilization savings and higher throughput. ■ **Note** Refer to the following table of Recommended Window Settings.

Recommended Window Settings

Annex G/X.25 Window Guidelines

Link Description	Recommended Window Settings		Recommended Window Subtractor
	K (Frame)	W (Packet)	
8 Mbps Serial	63	30	25
4 Bps Serial	30	20	15
2 Mbps Serial	30	20	7
E1	30	20	15
1536 Kbps Serial	25	15	7
T1	30	20	15
512 Kbps	15	10	4
256 Kbps	10	7	4
128 Kbps	10	7	4
64 Kbps	10	7	4
64 Kbps	10	7	4

These recommendations were arrived at in a controlled environment. In links with long delays adjustments may be required. A general rule would be to be bring the Window Subtractor value close to or equal with the "W' Packet window. This effectively allows the acknowledgments to be sent out faster accommodating the added delay.

The new Window Subtractor parameter is downward compatible with previous releases. It can be set independently at one end of the link without effecting the remote node that may not have this parameter. In addition to the recommendations in the table above the following two parameters should be always be set as shown below:

- Data queue upper threshold = 15
- Data queue lower threshold = 4

■Note

The Vanguard 7300 W Packet Window parameter's default has been changed from 2 to 7.

Best Path Routing

Introduction

The 6500 Series uses a best-path algorithm to calculate the best path through the network.

Arriving at the Effective Load Number

To arrive at the Effective Load Number, the algorithm considers the following factors:

- The number of logical channels in use
- Port speed
- Priority of eligible links
- Eliminates links with 0 (zero) priority

The link with the lowest load number is the optimal link and is used to forward the call.

The following table shows the algorithm:

Best Path Algorithm

Load Number	=	$\frac{(80{,}000)(\text{Port Priority})(\text{Logical Channels in use} + 1)}{\text{Port Speed}}$

where Port Priority = the priority configured in the Route Selection Table.

Choosing Port Priority

When choosing port priority in the Route Selection table, enter a value that represents the number of node links to the destination if that route is selected. This can be changed for special circumstances. For example, if two ports go to the same destination with the same number of links, but one route is tariffed at a higher rate, this route would be given a lower priority so that it is less likely to be used.

■Note

The higher the priority number the lower the priority. For example, a port with a priority number of 2 has a higher priority than a port with a priority of 3. Also, a port with a priority of 0 (zero) is a backup port. Calls are not normally routed to a backup port unless all others to a specific destination are down.

Periodic SVC Billing

Introduction

Periodic SVC Billing lets you generate billing records at regular intervals, for SVCs of long duration, without waiting for the SVC to clear.

Navigating the CTP

You can generate billing records by configuring the SVC Billing Record Timer parameter. This parameter is available when you select the **Node** menu (from the **Configure** menu) from the CTP, as shown in Figure 2-7.

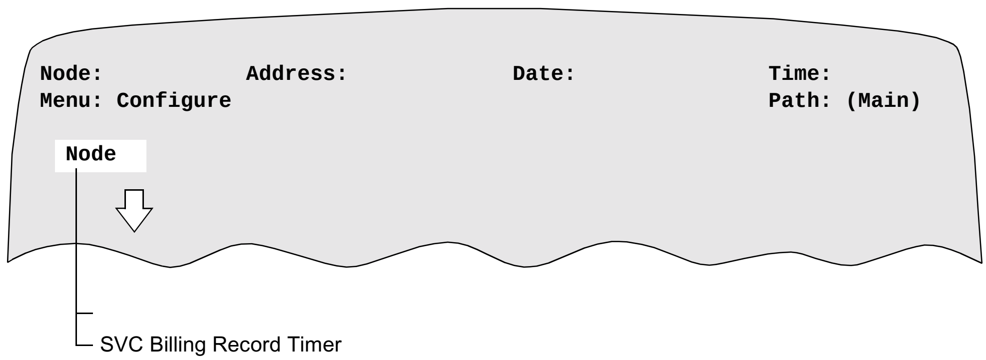

Figure 2-7. Configure Node Menu

Configuring the SVC Billing Record Timer

Follow these steps to configure the SVC Billing Record Timer.

Step	Action	Result
1	Select **Configure** from the CTP.	The Configure menu appears.
2	Select **Node**.	The Node menu appears. Move through the list until SVC Billing Record Timer (minutes) appears.
3	Select **SVC Billing Record Timer (minutes)**.	You are prompted to enter a value that is within a given range.
4	Enter a value.	
5	Boot the node with a warm or cold boot, or boot the Table and Node Record. ■ **Note** When a Node boot is executed, the node itself is restarted and reinitialised with the configuration for the node record. When a Table and Node Record boot is executed, the node is only reinitialised with the new values. The node is not restarted.	Changes to the parameter take effect.

Parameters

This table shows the SVC Billing Record Timer parameter. You must perform a Node boot, or a Table and Node Record boot, for changes to this parameter to take effect.

SVC Billing Record Timer

Range of values:	0 to 65535
Default value:	0
Description:	Specifies the interval at which billing records are gathered and printed. This applies to all SVCs in the node that have the Billing parameter turned on. ■ **Note** A value of 0 indicates that the SVC Periodic Billing feature is disabled. This means that the Billing Records are generated only after the SVC is cleared.

Configuring X.25 Options to Prevent Routing Loops

Introduction

Vanguard nodes can prevent routing loops by using the call packet in a unique application.

What is a Routing Loop?

When several nodes are connected in a network configuration, several paths may exist between any two points on that network. If the Route Selection Table is inadvertently misconfigured so that a call is forwarded through several nodes and back to its originating point, a Routing Loop exists. These loops prevent calls from being successfully completed.

Enabling Loop Detection

You enable Loop Detection when you set the parameter X.25 Options in the X.25 Port Record to Internodal Link (INL).

When a call is made over a link configured for INL, the node places an anti-loop code (CCITT type D facility, default 200 decimal, C8 hex) in the call packet's facility field. The node's number is also appended to the facility.

■ **Note**
You can change the anti-loop code by changing the parameter Hop Count module Code in the Node record.

How the Call Packet Field Works When a Call Arrives

When a call arrives, the node checks the content of the anti-loop facility for the presence of its own node number and operates as described in this table:

If...	*Then...*
The node detects its own node number	The call is cleared with cause code 13 (decimal), diagnostic code 133 (decimal). This notifies the originating VanguardMS node that a routing loop has occurred and that it should try an alternate path.
The node's own node number is not present in the call	The node adds its own node number in the facility and routes the call based on settings in the routing table. ■ **Note** All Vanguard Product nodes in the network must use the same anti-loop facility code (i.e. the parameter Hop Count facility Code in all the nodes must have the same value).
A call is routed to an X.25 link that is not configured with X.25 Options = INL	The anti-loop facility is deleted. This ensures that the facility is not sent to a non-Vanguard device.

Configuring an X.25 Port for Suppression of Call Rerouting

How It Works

You would enable the Suppression of Call Rerouting CSK if you want a port that is down not to reroute incoming calls to an alternate destination. When Suppression of Call Rerouting is enabled, incoming calls are cleared back to the originator.

The Suppression of Call Rerouting CSK only effects ports that are configured as Access Ports. (To configure a port as a Access Port, you must enable the AP option in the X.25 Option parameter.)

Enabling the CSK

Follow these steps to enter this CSK:

Step	Action	Result
1	Select **Configure** from the CTP Main menu.	The Configure menu will appear.
2	Select **Software Key Table** from the Configure menu.	The Software Key Table Configuration screen will appear.
3	Press Return to access the Key Value field and enter this CSK number: **ECR94XYW5K9ZN72QT7B4**	The message **Storing updated record in configuration memory** appears.
4	Perform a Node boot to implement your changes.	

Limiting Calls Between Ports

Introduction

In some applications, you may want to limit calls between ports. You can use the Closed User Group (CUG) feature to configure ports to receive calls only from specified ports in the network and to reject calls for all other ports.

Implementing CUG

Implementing the CUG feature is a two-part process:

1) To enable Closed User Group, set a Port Record parameter.

- For X.25 ports, X.25 Options = CUGF
- For PAD ports, Terminal Control = CUG

2) To specify Closed User Group membership:

The parameter CUG Membership (in the Port Record for PAD ports and X.25 ports) must identify at least one closed user group for which the port or channel is a member. A port can be a member of up to eight CUGs.

Call Initiation

This table identifies what happens when a call is initiated from a CUG port:

Step	Action
1	The CUG identifier is placed in the CUG field, when the call is initiated from a terminal attached to a CUG port.
2	A port configured for a CUG checks the facility field of all incoming calls to see if it contains a CUG identifier.
3	The call is rejected if the field does not contain a CUG identifier.
4	The module is checked against the called port's CUG Membership list, if the identifier is found. The call is accepted if there is a match between the CUG identifier and the CUG membership list. The call will be cleared if there is no match.
5	Ports that are not members of any CUG ignore the CUG facility in incoming calls. This means that a port that is a member of a CUG can make calls to ports that are not members of any closed user group (the parameters X.25 Options and Terminal Control are not set to CUG).

CUG Incoming Access

A CUG port will accept incoming calls from other user groups if the CUGIA option in the Call Subscription Facility parameter is enabled. The CUGIA works with these specifications:

- Ports can belong to one or more CUGs and can receive incoming calls from other DTEs belonging to these subscribed CUGs.
- Ports can receive incoming calls from DTEs not belonging to any CUG (open part of the network).
- Ports can receive incoming calls from other DTEs belonging to different CUGs (a different CUG is one which is not subscribed to at this node) with Outgoing Access (CUGOA) capability.

D-bit Modification

Introduction

The D-bit on an X.25 data packet is the signalling bit used to acknowledge packet delivery. If you want to make sure that data packets are being delivered to the remote end of an X.25 connection, you can enable the DBITMOD facility in the Facility Subscription Control parameter available from the X.25 Port Record.

How It Works

The D-bit on a data packet is used to acknowledge packet delivery. It can be set to either 0 or 1. When set to 0, acknowledgment of a packet is sent from the intermediary node. When set to 1, acknowledgment of a packet is sent only when it reaches the remote end.

Most modern terminal application can set the D-bit on data packets to 1. However, if you have an older terminal application that cannot set the D-bit, it can be set on data as it travels through a port on A Vanguard Product with the D-bit Modification facility.

■ Note

Enabling the D-bit Modification facility may slow down the data transfer rate. Because only a limited amount of data can be sent across a network without acknowledgment, the data transfer rate may slow (if window closure occurs).

D-bit Modification Facility

When the D-bit Modification Facility is enabled on a port, it sets the D-bit on every packet that goes through the port.

The type of data (X.25 or non-X.25) determines whether you enable the D-bit Modification Facility access (receiving) port or the network (sending) port. When X.25 data is transmitted, the D-bit Modification Facility can be set for either the access port or the network port. However, when non-X.25 data is transmitted, it must go through a PAD before it can enter the X.25 network, the D-bit modification facility must be set on the network port.

Figure 2-8 shows the D-bit used with X.25 data:

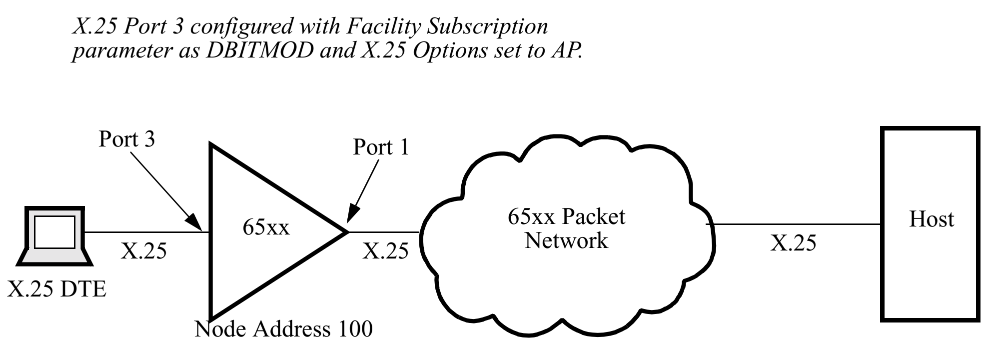

Figure 2-8. D-Bit Modification With X.25 Data

Figure 2-9 shows the D-bit modification facility used with data that must be processed by a PAD before it can enter the X.25 network:

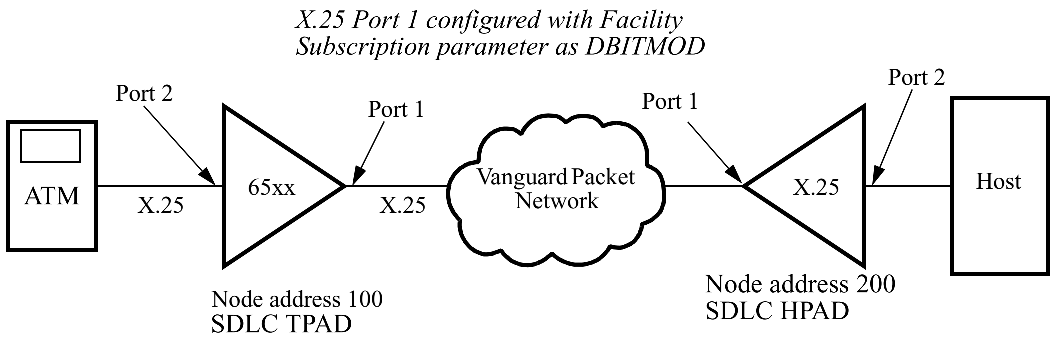

Figure 2-9. D-Bit Modification With Non-X.25 Data

Call Redirection

Introduction

If you want an X.25 port to redirect incoming calls when it is busy or disabled, you must configure it for Call Redirection.

How It Works

The node that places an incoming call must redirect the call. Otherwise, it will be cleared.

This table identifies how to configure a port for Call Redirection.

Step	Action
1	Set the X.25 Options parameter to INL (in the X.25 port record) on the port that receives the call. (See “X.25 Options” on page 40.)
2	Set the Call Subscription Facility to REDIRECT (in the X.25 port record) on the port that originates the call. (See “Facility Subscription Control” on page 49.)
3	Configure the Call Redirection Table for the port originating the call. For more information on how to configure the Call Redirection Table, see “Call Redirection Table”.

■**Note**

Call Redirection is limited to a network consisting of Vanguard devices only. It will not function across third party X.25 equipment, public networks or Hunt groups.

Call Redirection Table

When you configure a port for Call Redirection, inbound calls are sent to alternate X.25 addresses as they are specified in the Call Redirection Table. The Call Redirection Table should be configured on the port that the call originates from.

The Call Redirection Table supports wildcarding. Although, both the primary and redirection addresses may contain wildcard characters, the length of a redirection address cannot exceed the length of the primary address.

This table shows six redirection addresses with wildcard characters in them and the new addresses that incoming call would be directed to:

Original Address	Redirection Address	New Address
99010001	9802	9802
	9802*	98020
	9802**	980200
	9802***	9802000
	9802****	98020001
	9802*******	98020001

Call Facility Manipulation for Inbound Calls

Introduction

When a call enters the node and when it leaves on the link to which it is forwarded, the basic routing function is checked by processing the call for facilities. Facilities are placed in call requests to ask for enhanced services that the network or the destination might provide.

Facility Checking

These facilities are checked during inbound call processing:

- Packet size negotiation
- Window size negotiation
- Closed User Group (CUG)
- Reverse charging
- Fast Select
- Network User Identification (NUI)

Facilities not listed below remain in the Call Request Packet without modification and are passed to the destination.

Packet Size Negotiation

This table describes the packet size negotiation environment for X.25:

If...	*Then...*	*Result*
The Call Request Packet contains the Packet Size Negotiation facility	The size requested is checked.	Only packet sizes of 128, 256, 512, or 1024 bytes are allowed. Also, the parameter Maximum Negotiated Packet Size determines the maximum packet size that the X.25 link is allowed to negotiate.
The incoming Packet Size Negotiation requests a packet size larger than the maximum	The node responds with a packet size equal to the size in the parameter Maximum Negotiated Packet Size.	
The incoming Packet Size Negotiation requests a packet size less than 128 bytes	The call is changed to 128 bytes.	

Parameter Settings for Maximum Negotiated Packet Size

The parameter Maximum Negotiated Packet Size sets the maximum X.25 layer 3 data packet size at which an FRMR is sent. This table lists the parameter settings and maximum frame sizes.

Parameter Setting Frame Size	Maximum
128 + packet header	128 + frame header
256 + packet header	256 + frame header
512 + packet header	512 + frame header
1024 + packet header	1024 + frame header

The frame header is either 2 bytes (if normal sequencing is configured) or 3 bytes (if extended sequencing is configured) in length. The packet header is either 3 bytes (if normal sequencing is configured) or 4 bytes (if extended sequencing is configured) in length. Selecting 128 allows 256 + headers because a CALL packet may be 256 bytes.

Window Size Negotiation

If the Call Request Packet contains the Window Size Negotiation facility, the range requested is checked. Ranges can be 1 to 7 on ports running normal window sequencing and 1 to 15 on ports running extended window sequencing. If the requested window size is greater than 7 (for normal sequencing) or 15 (for extended sequencing), it is changed to 7 or 15 respectively.

Closed User Groups

The Closed User Group (CUG) feature lets you configure ports to receive calls only from specified ports in the network and to reject calls for all other ports. Refer to Limiting Calls Between Ports on page 62.

Reverse Charging

If the parameter Facilities to Bar in Inbound Calls is set to REV (bar reverse charging), incoming calls with Reverse Charge Facility are rejected. Otherwise, the facility is passed transparently to the outbound channel.

Fast Select

Fast Select is not processed during the inbound processing phase. It is passed transparently to the outbound channel.

Network User Identification (NUI)

NUI support can be passive or active. Passive NUI support allows calls with the NUI facility to pass without checking the facility’s contents. Active NUI support checks the contents of the NUI facility and acts on the call based on the results of the check. All X.25 ports can support passive or active NUI.

Passive NUI Support

When the X.25 Options port parameter is not set to NUI, it is configured for passive NUI support. Calls are passed without the NUI facility’s contents being checked. The NUI facility is passed to the destination unchanged and the destination equipment checks for valid users.

Example of Passive NUI Support

A typical example of this is where the destination is the port on a PDN to which the Vanguard device is attached. The PDN is configured for NUI checking and passwords and account names are maintained by the PDN. To operate in this manner, the X.25 Options port parameter must not enable NUI.

Passwords and account name format are not specifically defined by CCITT recommendations. For this type of arrangement, valid password and account names must be determined by the PDN to which the node is attached. They are used in the facility field of calls going to the PDN.

Active NUI Support

When the X.25 Options port parameter is set to NUI, it is configured for active NUI support. A call entering the node has a password in the facilities section of the call and the node is configured to check the password against a similar set stored in the node. If there is no match, the call is cleared.

To support this, configure the NUI/Password Table with the appropriate passwords and account names. Account names are not used in NUI checking; they are used if a billing record is to be created. By doing NUI validation at the point of attachment, unauthorized calls are cleared before they enter the network.

Bilateral Closed User Group (BCUG)

BCUG options are available in the parameters Facilities to Bar in Outbound Calls and Facilities to Bar in Inbound Calls (in the X.25 Port record). You must specify these parameters when the link is connected to a Digital Data Network (DDN).

Datagram (DGRAM)

Datagram options are available in the parameters Facilities to Bar in Outbound Calls and Facilities to Bar in Inbound Calls (in the X.25 Port record). You must specify these parameters when the link is connected to a DDN.

Call Facility Manipulation for Outbound Calls

Introduction

After address processing, the facilities are processed.

- Packet size negotiation
- Window size negotiation
- Closed User Group (CUG)
- Reverse Charging
- Fast Select
- Network User Identification (NUI)
- Throughput Class Negotiation

These facilities are checked during outbound call processing. Any facilities not mentioned are left intact in the Call Request Packet.

Packet Size Negotiation

If the Facilities to Add to Outbound Calls parameter specifies PACK, packet size negotiation is added to the outbound Call Request. The parameter P Packet Size (in the X.25 Port Record) specifies the value to be negotiated.

Window Size Negotiation

If the parameter Facilities to Add to Outbound Calls parameter specifies WIND, window size negotiation is added to the outbound Call Request. The parameter W Packet Window (in the X.25 Port record) specifies the value to be negotiated.

CUG

CUG can be supported actively or passively:

- Passive Support: The default setting of the X.25 port allows a call with the CUG facility to pass without checking its contents.
- Active Support: When the parameter X.25 Options is set to CUG, the port checks the contents of the CUG facility and acts on the call. The action depends on the setting of the parameter CUG Membership parameter. If the parameter Facilities to Delete from Outbound Calls is set to CUG, the CUG facility is removed from the call after any checking is done.

CUG with Outgoing Access (CUGOA)

The X.25 Closed User Group with Outgoing Access (CUGOA) facility enables the DTE to belong to one or more closed user groups, and to originate virtual calls to DTEs in the open part of the network and to DTEs belonging to other CUGs with the incoming access capability. Once the DTE has subscribed to the CUGOA facility, The Closed User Group with Outgoing Access Selection facility can be used on a per virtual call basis.

This facility is used by the calling DTE in the call request packet to specify the closed user group selected for a virtual call, and to indicate that outgoing access is also needed. The CUGOA facility can be received by a DTE only if the network supports it and the DTE has subscribed to the CUGIA (Closed User Group with Incoming Access) facility.

The Terminal Control parameter (under the PAD Port Record) contains a new value: CUGOA. When Terminal Control is set to CUGOA, the DTE:

- Can belong to one or more closed user groups
- Can originate virtual calls to DTEs in the open part of the network
- Can originate virtual calls to DTEs belonging to other CUGs with the incoming access capability.

■ Note

A remote DTE can receive a CUGOA setting only if it is supported by the network and if that DTE has subscribed to the Closed User Group with Incoming Access facility.

Reverse Charging

If the parameter Facilities to Bar From Outbound Calls is set to REV (bar reverse calls), a call with the request for reverse charging included in the packet is cleared.

Fast Select

If the parameter Facilities to Bar From Outbound Calls is set to FAST, the call is cleared if the fast select facility is in the Call Request Packet. If the parameter is not set to FAST and if the facility is in the Call Request, the facility is passed transparently.

NUI

If the parameter Facilities to Delete from Outbound Calls is set to the NUI, the Network User Identification is removed from the Call Request. If the parameter is not set to NUI, this facility is passed transparently.

Throughput Class Negotiation

If the parameter Facilities to Delete from Outbound Calls is set to THRO, this facility is removed from the Call Request. If the parameter is not set to THRO, the facility is passed transparently.

BCUG

When an X.25 link is connected to a DDN, the parameters Facilities to Bar in Outbound Calls and Facilities to Bar in Inbound Calls must be set to the BCUG.

Datagram (DGRAM)

When an X.25 link is connected to a DD), the parameters Facilities to Bar in Outbound Calls and Facilities to Bar in Inbound Calls must be set to the DGRAM.

Link Address Negotiation for Dial On Demand

Introduction

This section describes Link Address Negotiation for Dial On Demand.

What Is It?

X.25 support for Vanguard products includes dynamic link addressing for Dial On Demand on nodes connected to an X.25 network. This means that you can configure your Vanguard device to negotiate the DCE or DTE link addressing at both ends of a link.

How It Works

As illustrated in Figure 2-10, each time a DOD link is brought up on a node configured with the Link Address Negotiation feature, the two nodes trying to establish the link begin an exchange of SABMs and replies to establish proper link addressing and make a connection. You can configure one or both ends of a link for negotiation. However, if only one end of the link is configured for negotiation, that node resets its link address to complement the node at the other end of the link after a brief exchange of SABMs and replies.

If both ends of a link are configured for negotiation, a series of exchanges occurs before the nodes settle on complementary link addresses.

This negotiation process may change each time a link is established between the two nodes.

Example

Figure 2-10 shows an example of a DOD application in which Node B negotiates link addressing with Node C in order to bring up a new link.

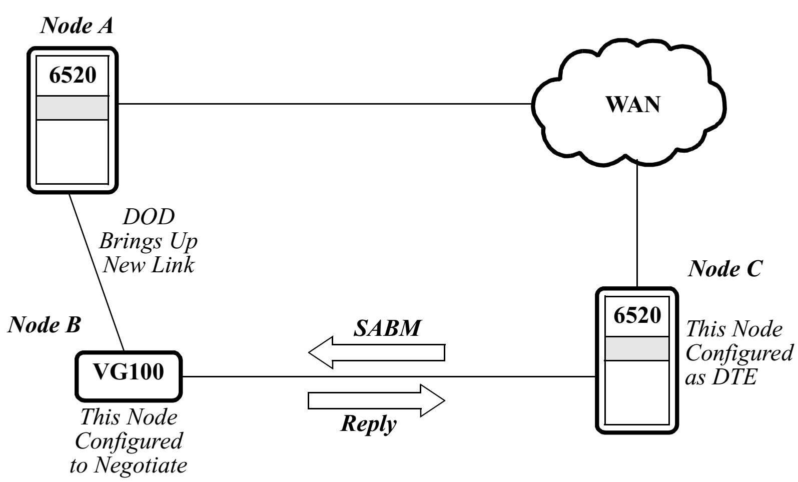

Figure 2-10. How DOD Negotiate Feature Works

Node B, configured for negotiation, determines that Node C has a DTE link address, and configures itself to a DCE link address to establish the link.

Configuring the Negotiate Link Address Feature

This table identifies how to configure Link Address Negotiation.

Step	*Action*	*Result*
1	Select **Configure from the CTP Main menu.**	The Configure menu appears.
2	Select **Port** from the Configure menu.	The Port Configuration record appears.
3	Configure the Port Number you want to use and define the Port Type as X.25.	You are prompted to fill in the next parameter.
4	At the Link Address: prompt, type in **Negotiate**.	This sets the port configuration for the node to negotiate the link address each time a link is being established.
5	Perform a Port boot to implement your changes.	

Chapter 3
Configuring Call Translation Functions

Overview

Introduction

This Chapter describes how to configure the X.25 Calling translation functions on Vanguard products and includes:

- The “Inbound Call Translation Table Record” section on page 3-2.
- The “Outbound Call Translation Table Record” section on page 3-5.
- The “Configuring the REGSO Option” section on page 3-9.
- The “Calling Address Translation Table Record” section on page 3-16.
- The “Call Redirection Table” section on page 3-21.

Inbound Call Translation Table Record

Introduction

The Inbound Call Translation Table Record specifies how the node translates calls received from a PDN. This record contains parameters that translate inbound calling subaddresses that match this table entry.

What You See in This Record

Figure 3-1 shows the Inbound Call Translation Table Record.

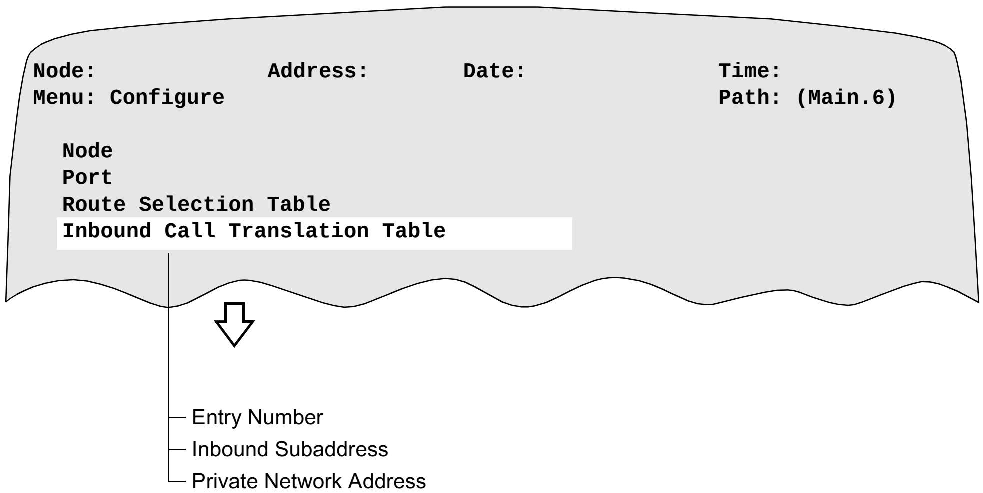

Figure 3-1. Inbound Call Translation Table

Before You Begin

Before you can configure parameters, you must log on to the local node's control terminal port.

Configuration Guidelines

When you configure the Inbound Call Translation Table Record:

- No blank address values are permitted.
- No duplicate address values are permitted.
- If there are entries in this table, then at least one X.25 link should exist.
- An X.25 port must have X.25 Option = PDN to use the Inbound Call Translation Table.

Accessing the Inbound Call Translation Table Record

To access the Inbound Call Translation Table record:

Step	Action	Result
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **Inbound Call Translation Table** from the Configure menu.	The Inbound Call Translation Table and its parameters appear. A prompt appears asking you to configure the next parameter.
3	Enter the parameter values.	
4	Press **<ESC>** to return to the Configure menu after you have configured all the parameters.	
5	Perform a Table and Node Record boot.	The changes you make will be saved.

Inbound Call Translation Table Record Parameters

Introduction

This section describes the Inbound Call Translation Table parameters.

Parameters

Configure these parameters from the Inbound Call Translation Table Record:

Entry Number

Range:	1 to 64
Default:	1
Description:	Identifies the particular Inbound Call Translation Table entry being configured by the other parameters in the record. ■ **Note** You can not modify this value.

Inbound Subaddress

Range:	0 to 3 digits
Default:	(blank)
Description:	Specifies the subaddress contained in an incoming call from another network, usually a PDN. This address is translated into a Private Network Address before the call is forwarded. The variable subaddress length is determined by the length of the Subaddress in the X.25 Port record. ■ **Note** Use the space bar to blank the parameter value.

Private Network Address

Range:	0 to 15 digits
Default:	(blank)
Description:	Value of this parameter replaces the entire called address if the subaddress of the incoming called address matches the value of the Inbound Subaddress (previous parameter). ■ **Note** The Inbound Subaddress (previous parameter) is not appended to this private network address. ■ **Note** Use the space bar to blank the parameter value.

Outbound Call Translation Table Record

Introduction

The Outbound Call Translation Table Record specifies how the node translates calls sent to a PDN. This record contains parameters that translate outbound calling subaddresses that match the entry for this table.

What You See in This Record

Figure 3-2 shows the Outbound Call Translation Table Record.

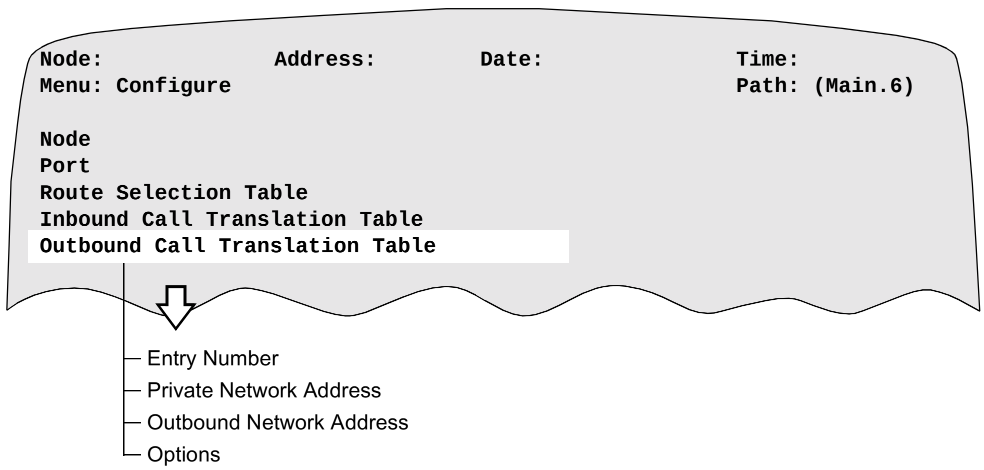

Figure 3-2. Outbound Call Translation Table

Before You Begin

Before you can configure parameters, you must log on to the local node’s control terminal port.

Configuration Guideline

An X.25 port must have the X.25 Option parameter set to PDN to make use of the Outbound Call Translation Table.

Accessing the Outbound Call Translation Table Record

Follow these steps to access the Outbound Call Translation Table record:

Step	*Action*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **Outbound Call Translation Table** from the Configure menu.	The Outbound Call Translation Table and its parameters appear. A prompt appears asking you to configure the next parameter.
3	Enter the parameter values.	
4	Press **<ESC>** to return to the Configure menu after you have configured all parameters.	
5	Perform a Table and Node Record boot.	The changes you make will be saved.

Outbound Call Translation Table Record Parameters

Introduction

This section describes the Outbound Call Translation Table Record parameters.

Parameters

Configure these parameters from the Outbound Call Translation Table Record:

Entry Number

Range:	1 to 64
Default:	1
Description:	Identifies the particular Outbound Call Translation Table being configured by the other parameters in the record. ■ **Note** You can not modify this value.

Private Network Address

Range:	0 to 15 digits
Default:	(blank)
Description:	Specifies the Private Network Address that is contained in an outbound call to another network, usually a PDN. The Private Network Address is translated into a Public Network Address before the call is forwarded. Do not include the subaddress in this parameter. ■ **Note** Use the space bar to blank the parameter value.

Outbound Network Address

Range:	0 to 15 digits
Default:	(blank)
Description:	Specifies a new called address, if the outgoing PDN called address matches the value of the Private Network Address. ■ **Note** Any subaddress will be appended unless CUD is used. ■ **Note** Use the space bar to blank the parameter value.

Options

Range:	NONE, OLDA
Default:	NONE
Description:	Specifies options for outbound call address translation: • NONE: Do nothing. • OLDA: Insert private network address into outbound Call User Data (CUD) field starting at the fifth byte of the CUD after the protocol ID. This address can be a maximum of 12 digits. If it is longer, the least significant digits are deleted. When the X.25 Options parameter (in the X.25 Port record) is set for CUD and PDN, the network address and the subaddress are included in the CUD.

Configuring the REGSO Option

REGSO Access

You access the REGSO option as part of the X.25 Port Record through either the CTP or through an SNMP manager. This section describes how to configure the option.

Configuration Procedure

These tables explain how to configure the REGSO option.

Steps to Configure REGSO

Step	Action	Result
1	Set the X.25 Options field to REGSO in an X.25 Port record.	The REGSO option is selected.
2	Configure the Inbound Call Translation Table Size in the Node Record.	The table size is determined.
3	Configure a translation table entry.	A private network address is uniquely associated with a public subaddress. ■ **Note** Be sure that the private network address is a full address.

Setting REGSO Option

This table describes how to configure the X.25 Record for REGSO.

Step	Action	Result
1	Select **Configure** from the Main menu.	The Configure menu appears.
2	Select **Port** from the Configure menu.	The Port Configuration menu appears along with a prompt.
3	Enter the number of the port you want to configure, and press Return.	The prompt appears to enter information about the port type.
4	Select **X.25** as the port type.	The X.25 Port Record appears.
5	Enter **REGSO** in the X.25 Options field.	Configures the X.25 node to replace calling addresses in outgoing call packets.

Setting the Table Size

This table describes how to set the number of records in the Inbound Call Translation Table. REGSO requires one table entry per private network address.

Step	*Action*	*Result*
1	Select **Configure** from the Main menu.	The Configure menu appears on the screen.
2	Select **Node Record** from the Configure menu.	The Node Record appears.
3	Enter a value, in the range 1 to 1000, in the Inbound Call Translation Table Size field.	The table size is entered.
4	Reboot the node.	The table size is configured.

Adding an Address

This table describes how to configure an entry in the Inbound Call Address Translation Table.

Step	*Action*	*Result*
1	Select **Configure** from the Main menu.	The Configure menu appears.
2	Select **Inbound Call Translation Table**.	The Inbound Call Translation Table Configuration screen appears.
3	Enter an unused table entry value	A table entry form appears.
4	Enter both: • An Inbound Subaddress, of 0 to 3 digits (decimal) • Private Network Address, of 0 to 15 digits (decimal)	The message **Storing updated record in configuration memory** appears. The new table entry is configured.

Example of Inbound Call Translation Table Configuration Screen

Figure 3-8 shows the Inbound Call Address Translation Table screen. The compound Selection entry, 6.4, is equivalent to entering 6, then 4. This example shows table entry 30.

```
#Enter Selection: 6.4


Inbound Call Translation Table Configuration


ATTENTION
---------
As the maximum size of the Inbound Call Translation Table
has been increased to 1000, another method for choosing an entry
has been introduced.

* An entry can be chosen EITHER by its entry number
  OR by specifying either the Public Sub-address or Private Network address
that the entry already contains. If an entry matching the Public Sub-ad-
dress or Private Network address exists then the entry number will be dis-
played.

* If more than one entry exists with the specified Public Sub-address or
Private Network address, the entry number of the first match will be dis-
played with a '*'. Entering '>' will display the other matching entries
one by one.
```

```
Entry Number: 1/
Entry with Sub-Address:
Entry with Private Network Address: 10098

Entry Number: 30/ :
[30] Inbound Subaddress: 98/
[30] Private Network Address: 10098/
```

Figure 3-3. Inbound Call Translation Table Configuration Screen

Configuring Mnemonic Calls

Introduction

To make a call using a mnemonic, you enter:

- The configured mnemonic code instead of the X.28 Call command
- The network address
- The subaddress or group subaddress
- Call facilities
- User data

Required Parameters

You can establish mnemonic calls only if you have properly configured the parameters in these two records:

Mnemonic Table:

In the node where the call is originating, you must configure a Mnemonic Table entry for each X.25 address number to be called. That entry must include the Mnemonic (the parameter Mnemonic Name) and the destination address (the parameter Call Parameters).

Route Selection Table:

In the same node, you *must* configure a corresponding entry in the Route Selection Table representing the destination address (the parameter Address) that is in the Mnemonic Table entry.

■ **Note**

The mnemonic "CTP" is reserved for the control terminal port (default subaddress 98) in each node. BCST is reserved as the mnemonic for the Broadcast module (default subaddress 95).

Example of Mnemonic Addressing

Figure 3-10 is a simple example of mnemonic addressing. In Node 100, the terminal at Port 4 is about to make a Mnemonic Call to the terminal at Port 3, Node 200. The configuration records and parameters that pertain to mnemonic addressing are shown for Node 100.

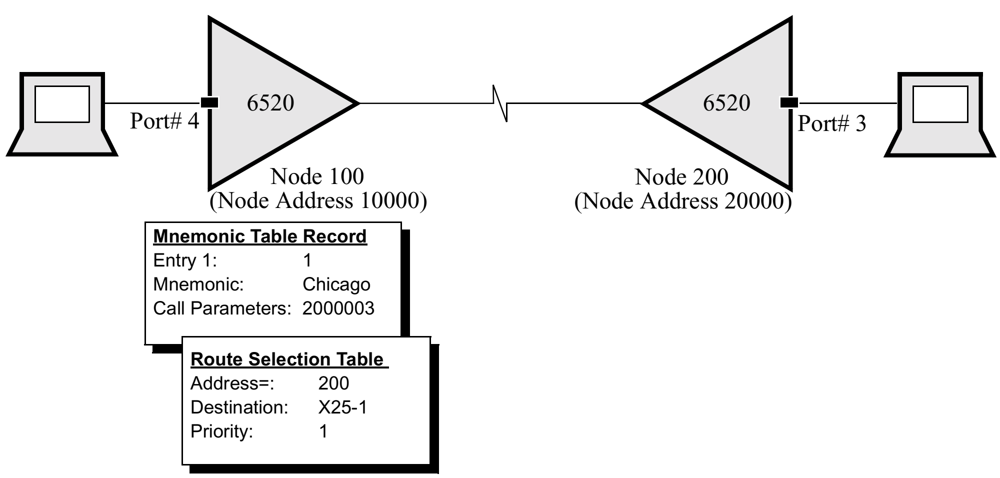

Figure 3-4. Mnemonic Addressing Example

Searching for and Deleting an Address

Address Search

This table describes how you can search for an Inbound Call Address Translation Table.

Step	*Action*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **Inbound Call Translation Table.**	The Inbound Call Translation Table Configuration (Figure 3-9) appears.
3	At the **Entry Number:** prompt, press the ESC key.	This prompt appears: **Entry with Subaddress:**
4	Enter the Inbound Subaddress for which you are searching a Private Network Address.	• The entry number of the match appears. If there is more than one matching entry, an asterisk appears next to the entry number. • When you press the Return key, the Inbound Subaddress that you input appears. • When you press the Return key again, the matching Private Network Address appears. You can also use the private network address to get the Inbound Subaddress. You can only search one entry at a time. Press the ESC key to return to search mode.
	If...	***Then...***
	You enter an incorrect subaddress	This error message appears: **Entry with Sub-Address: XXX not found**

Screen in Search Mode

Figure 3-9 shows the Inbound Translation Table Configuration in search mode.

```
#Enter Selection: 6.4


        Inbound Call Translation Table Configuration


             ATTENTION
             ---------
As the maximum size of the Inbound Call Translation Table
has been increased to 1000, another method for choosing an entry
has been introduced.

* An entry can be chosen EITHER by its entry number
  OR by specifying either the Public Sub-address or Private Network address
that the entry already contains. If an entry matching the Public Sub-ad-
dress or Private Network address exists then the entry number will be dis-
played.

* If more than one entry exists with the specified Public Sub-address or
Private Network address, the entry number of the first match will be
displayed with a '*'. Entering '>' will display the other matching entries
one by one.
```

```
Entry Number: 1/
Entry with Sub-Address:
Entry with Private Network Address: 10098

Entry Number: 30/ :
[30] Inbound Subaddress: 98/
[30] Private Network Address: 10098/
```

Figure 3-5. Inbound Call Translation Table Configuration in Search Mode

Deleting an Address

This table describes how to delete an Inbound Call Address Translation Table entry.

Step	Action	Result
1	Select **Delete Record** from the Main menu.	The Delete Record appears on the screen.
2	Select **Inbound Call Translation Table.**	The Inbound Call Translation Table screen appears. The **Entry Number:** prompt appears.
3	Enter the number for the entry you want deleted.	This message appears: **Proceed y/n:** Once you enter **y**, this message appears: **Record deleted.**

Calling Address Translation Table Record

Introduction

This record contains parameters that are required when configuring an X.25 link for SRGI+PDN (when the parameter X.25 Options = SRGI in the X.25 Port Record).

The Calling Address Translation Table Record specifies how the node translates calls received from a PDN.

What You See in This Record

Figure 3-6 shows the Calling Address Translation Table Record.

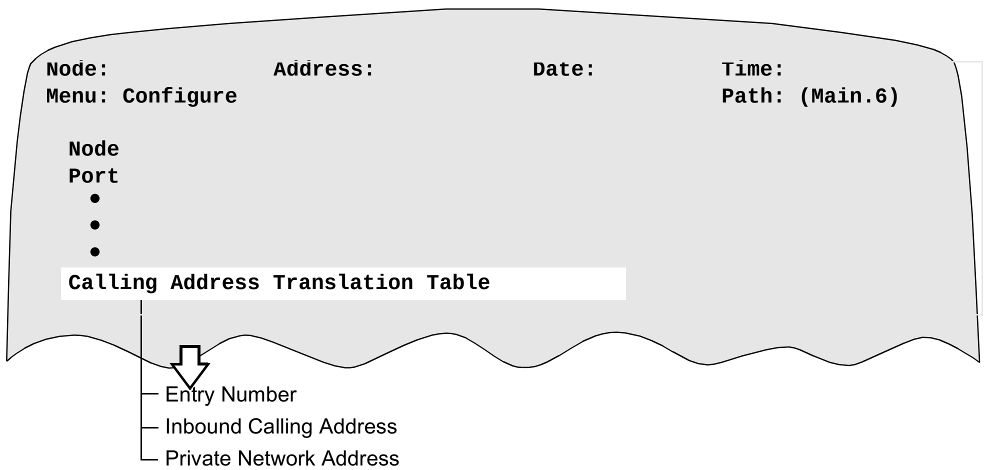

Figure 3-6. Calling Address Translation Table Record

Before You Begin

Before you can configure parameters, you must log on to the local node's control terminal port.

Accessing the Calling Address Translation Table Record

Follow these steps to access the Calling Address Translation Table record:

Step	Action	Result
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **Calling Address Translation Table** from the Configure menu.	The Calling Address Translation Table and its parameters appear. A prompt appears asking you to configure the next parameter.
3	Enter the parameter values.	
4	Press **<ESC>** to return to the Configure menu after you have configured all parameters.	
5	Perform a Table and Node Record boot.	The changes you make will be saved.

Calling Address Translation Table Record Parameters

Introduction

This section describes the Calling Address Translation Record parameters.

Parameters

Configure these parameters from the Calling Address Translation Table Record:

Entry Number

Range:	1 to 64
Default:	1
Description:	Identifies the entry being configured by the rest of the parameters in the record. ■ **Note** You can not modify this parameter.

Inbound Calling Address

Range:	0 to 15 digits
Default:	(blank)
Description:	Specifies the inbound calling address, which the private network address (specified in the next parameter) replaces before the call is forwarded. ■ **Note** Use the space bar to blank the parameter value.

Private Network Address

Range:	0 to 15 digits
Default:	(blank)
Description:	Specifies the private network address that replaces the inbound called address (specified in the previous parameter). ■ **Note** Use the space bar to blank the parameter value.

CUD Based Address Translation Table

Introduction

Call User Data (CUD) routing can be configured on an X.25 port, if the Address Translation Option parameter is set to CUDR, to resolve CUD address information. This updates the called address, of the incoming Call packet from the network, before routing it to its final destination.

Configuration

Complete these steps to configure the CUD Based Address Translation Table:

Step	*Action*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **CUD based Addr Translation Table** from the Configure menu.	The CUD based Addr Translation Table menu appears as shown in Figure 3-7.
3	Press **<ESC>** to return to the Configure menu after you have configured all parameters.	

What You See In This Record

Figure 3-7 shows the CUD based Addr Translation Table menu.

```
Node:              Address:            Date:         Time:
Menu:: CUD based Addr Translation Table              Path: (Main.6.3)

  CUD String
  Called Address
```

Figure 3-7. CUD based Addr Translation Table

Parameters

You must configure these parameters in the CUD based Addr Translation Table.

CUD String

Range	1 to 64 alphanumeric characters
Default	(Blank)
Description	Specifies the sub-string to search in the CUD for the incoming call for translating it into Called address. For searching from index in the CUD the name can be specified as: **(7)DADADIFUBBBB** It will skip 7 characters of the CUD and match DADAIFUBBBB in the CUD starting at Position 8. ■ **Note** Use the space bar to blank this field.

.

Called Address

Range	0 to 15 decimal digits
Default	(blank)
Description	Enter the X.25 Address which will be inserted for called address of incoming X.25 call packet if the configured CUD string is matched in the CUD of the incoming X.25 Call packet. ■ **Note** Use the space bar to blank this field.

Call Redirection Table

Introduction

This section describes the Call Redirection Table Record parameters. Any parameter with an asterisk (*) requires a Node boot; changes to other parameters require a Table and Node Record boot. For more information on configuring a network port for Call Redirection, see "Call Redirection Table" on page 21.

What You See In This Record

Figure 3-8 shows the Call Redirection Table menu.

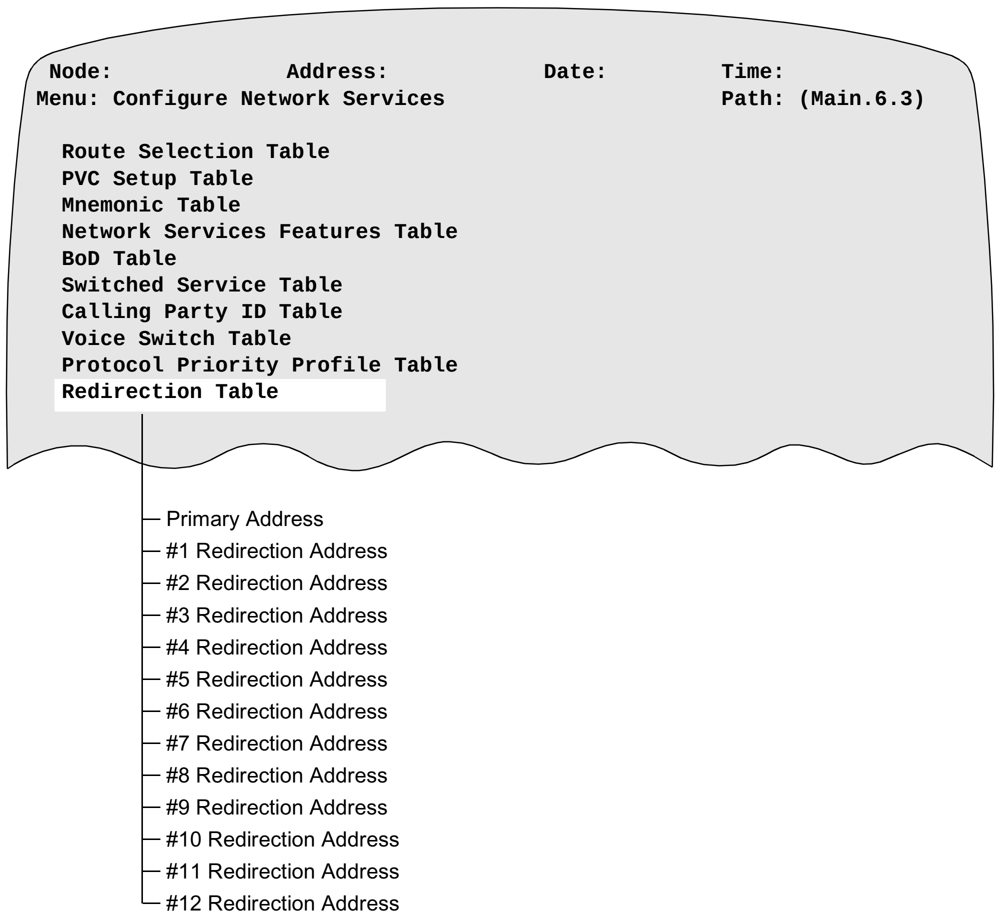

Figure 3-8. Call Redirection Table

Accessing the Call Redirection Table Record

Follow these steps to access the Call Redirection Table record:

Step	*Action*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **Configure Network Services** from the Configure menu.	The Configure Network Services menu appears.
3	Select **Call Redirection Table** from the Configure Network Services menu.	The Call Redirection Table appears.
4	Press **<ESC>** to return to the Configure menu after you have configured all parameters.	

Call Redirection Table Parameters

Introduction

This section describes the Call Redirection Table Record parameters

■ **Note**
In Vanguard products, six Call Redirection Tables are possible. In the Vanguard 6520 and Vanguard 6560, 12 Tables are possible.

Parameters

You must configure these parameters in the Call Redirection Table.

Primary Address

Range	0-15 decimal digits
Default	blank
Description	Specifies the primary address from which calls are redirected. If the destination has subscribed to REDIRECT, calls made to this address are redirected to any of the address against this entry in the Redirection Address fields. ■ **Note** The primary address can contain wildcard (*) characters. Use space character to blank field.

#1-#12 Redirection Address

Range	0-15 decimal digits
Default	blank
Description	Specifies the alternate address to which calls are redirected. If the destination has subscribed to REDIRECT, calls made to the primary address are redirected to the redirection addresses. To prevent all calls being redirected to the first alternative address in the table, the table is scanned each time a call is redirected and the call is redirected to a different address each time. ■ **Note** A redirection address cannot contain more characters than the primary address. It can contain wildcard (*) characters. Use space character to blank field.

Chapter 4
Statistics

Overview

This chapter describes how to access Detailed X.25 Port Statistics and T1/E1 Interface Statistics, and defines their screen components.

Detailed Port Statistics provide detailed information about a specified port and illustrates the effectiveness with which that port is operating. The T1/E1 Interface Statistics provide detailed information about each interface.

Before You Begin

Before you can access and use the statistics, you log on to the local node's Control Terminal Port. Refer to the *Vanguard Configuration Basics Manual* for information on using the CTP.

Accessing the Detailed Port Statistics

Introduction

This section describes how to access the Detailed Port Statistics screens.

Detailed Port Statistics

Use this procedure to access Detailed Port Statistics:

Step	Action	Result
1	Select **Status/Statistics** from the CTP Main menu.	The Status/Statistics menu appears.
2	Select **Detailed Port Stats**.	You are prompted to specify a particular port type.
3	Specify a port type.	A series of screens appears that are specific to the type of port (PAD or X.25). Examples of the X.25 screens are shown in Figure 4-1 through Figure 4-4.
4	Scroll through a series of screens for one port.	You are prompted to display the detailed port statistics for the next port.

Port Statistics Screens

Once you have accessed Port Statistics, you are presented with a series of up to four sequential display screens. These pages describe each screen and provide complete descriptions for each parameter displayed.

Port Statistics Screen

What You See in The First Screen

Figure 4-1 shows the first screen of the X.25 Detailed Port Statistics.

```
Node:           Address:                Date:           Time:
 Detailed X.25 Port Statistics:         Port 1 Page:  1 of  5
 Port Number: 1            Port Type:  X25           Port Status: Down
 Port Speed:  336000      Port State: Disc. Phase    Link Address: DCE
 Port Utilization In:   0% Port Utilization Out:   0%
 Call Summary:
              SVC     PVC
  Maximum:    0       0
  Current:    0       0
 Data Summary:          Last Statistics Reset:    1-JAN-1995  0:00:00
              IN         OUT                               IN         OUT
  Characters: 0          0              Characters/sec: 0          0
  Packets:    0          0              Packets/sec:    0          0
  Frames:     0          0              Frames/sec:     0          0
  Number of Packets Queued: 0
 Interface Summary:  T1-1       Channel 2
  Channel State: Normal

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

Figure 4-1. Example of Detailed X.25 Port Statistics, First Screen

Description of Terms — First Screen

Screen 1 of the Detailed X.25 Port Statistics screen contains this information:

Screen Term	*Tells You...*
Port Number	Number of the port
Port Type	Type of port
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 the Port Speed is 0, and the Clock=Ext, but clocking is not being received from attached device.
Port State	There are six possible port states that may appear. These 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.

Screen Term	***Tells You...*** *(continued)*
Port Utilization: In/Out	Percentage of port bandwidth in use
Call Summary	Maximum/Current (SVC/PVC): • Number of SVCs and PVCs currently using the port and the maximum number since the last reset
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
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.
Channel State	When T1/E1 daughtercard is installed. Indicates the conditions generating status for the T1/E1 channel associated with this port.

What You See in the Second Screen

Figure 4-2 shows the second screen of the X.25 Detailed Port Statistics.

```
Node:               Address: Date:      Time:
Detailed X25 Port Statistics: Port 1          Page:  2 of 5

Physical Summary:
Overrun Errors: 0     Underrun Errors: 0     CRC Errors: 0
Non-Octet Aligned: 0      Frame Length Err:0
Unknown DLCI Err: 0       Last Unknown DLCI: 0


Frame Summary:
        IN    OUT     IN         OUT
Info    0      0      RR       0        0
RNR     0      0      REJ      0        0
SABM    0      23     DISC     0        0
DM      0      0      UA       0        0
FRMR    0      0
Packet Summary:
                    IN OUT           IN   OUT
Data                 0 0     Receiver Ready 00
Receiver Not Ready   0 0     Reject Packet00
Call Request         0 0     Call Accept0 0
Clear Request        0 0     Clear Confirm00
Interrupt Request    0 0     Interrupt Conf.00
Reset Request        0 0     Reset Confirm00
Restart Request      0 0     Restart Confirm00
```

Figure 4-2. Example of Detailed X.25 Port Statistics, Second Screen

Screen Terms

Screen 2 of the Detailed X.25 Port Statistics contains this information:

Screen Term	Tells You...
Physical Summary	Number of Overrun, Underrun, and 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: Indicates the number of errors detected by Cyclic Redundancy Check (CRC) since last node boot or reset of statistics. Indicates that a frame received contains one or more corrupted bits. • Non-Octet Aligned: Indicates an invalid frame that is not divisible by eight. • Frame Length Errors: Indicates the number of frames received with length less than five characters. • Unknown DLCI Err: Indicates the number of frames received with DLCI for which no station is configured. • Last Unknown DLCI: Indicates the last unknown DLCI received in a frame.
Frame Summary	Summary of each frame being sent and received over the port since the last node, port, or statistics reset.
Packet Summary	Summary of each packet being sent and received over the port.

What You See In The Third Screen

Figure 4-3 shows the third screen of the X.25 Detailed Port Statistics.

```
 Node:              Address:Date:       Time:
Detailed X25 Port Statistics: Port 1    Page:  3 of 5

  Last inbound LCN: 0
  Inbound processing status: Processed OK, call passed to ROUT

                      Last Inbound Call, before processing:
    Called Address:
    Calling Address:
    Facilities:
    CUD:

                       Last Inbound Call, after processing:
    Called Address:
    Calling Address:
    Facilities:
    CUD:

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

Figure 4-3. Example of Detailed X.25 Port Statistics, Third Screen

Screen Terms

Screen 3 of the Detailed X.25 Port Statistics screen contains this information:

Screen Term	***Tells You...***
Last Inbound LCN	Logical channel number over which the last inbound call was processed
Inbound Processing Status	Describes how the last inbound call was handled. Examples include: • Process OK • Call Passed to ROUT • Failed Processing • Call Cleared
Last Inbound Call, before processing	Called Address, Calling Address, Facilities, and CUD of the last inbound call *before* it was processed
Last Inbound Call, after processing	Called Address, Calling Address, Facilities, and CUD of the last inbound call *after* it was processed

What You See In The Fourth Screen

Figure 4-4 shows the fourth screen of the X.25 Detailed Port Statistics.

```
 Node:              Address Date:       Time:
Detailed X25 Port Statistics: Port 1    Page:  4 of 5

  Last Outbound LCN: 0
  Outbound processing status: Processed OK, call transmitted

                      Last Outbound Call, before processing:
    Called Address:
    Calling Address:
    Facilities:
    CUD:

  Last Outbound Call, after processing:
    Called Address:
    Calling Address:
    Facilities:
    CUD:

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

Figure 4-4. Example of Detailed X.25 Port Statistics, Fourth Screen

Screen Terms

The fourth Detailed X.25 Port Statistics screen contains this information:

Screen Term	*Tells You...*
Last Inbound LCN	Logical channel number over which the last inbound call was processed
Inbound Processing Status	Describes how the last inbound call was handled. Examples include: • Process OK • Call Passed to ROUT • Failed Processing • Call Cleared
Last Inbound Call, before processing	Called Address, Calling Address, Facilities, and CUD of the last inbound call *before* it was processed
Last Inbound Call, after processing	Called Address, Calling Address, Facilities, and CUD of the last inbound call *after* it was processed

The fifth detailed X.25 Port Statistics screen displays with Release 6.1 or greater.

```
Press any key to continue (ESC-exit, 'N'-next sect, 'S'-skip to station)
...

 Node: 340_QUAD  Address: 200                 Date:  8-MAR-2002  Time:
11:05:53
 Detailed X.25 Port Statistics: Port 3                        Page:  5 of  5
 Monitor control signals on port 01 for 1 change (type: SW56K) on  22-APR-
1998

 Number of      Input            Output
 changes   NIS BPV DL C+ C-  RS LL CL IDL CLK        State      Time
 ========= ================  ================   ===============   ========
    1        L   H  H  H  H   H  H  H   H   H   Connected     03:33:19
    2        H   H  H  H  H   H  H  H   H   H   Connected     03:33:20
    3        H   L  H  H  H   H  H  H   H   H   Connected     03:33:23
    4        H   H  H  H  H   H  H  H   H   H   Connected     03:33:24
```

Figure 4-5. Example of Detailed X.25 Port Statistics, Fifth Screen

T1/E1 Interface Statistics

Introduction

This section describes the menus and statistics calculated for the T1/E1 Interface.

Detailed T1/E1 Interface Statistics

Figure 4-6 is an example of a Detailed T1/E1 Interface Statistics screen. Screen terms are described in the table.

```
Node:           Address:                Date:           Time:
Detailed T1/E1 Interface Statistics                      Page:  1 of  9

Interface Type: E1 - 2
Time Since Last Stats Reset:  8-FEB-2036    1:24:12
Alarm State: NONE
Channel State: NORMAL | NORMAL | NORMAL
Line Error Count:
24 Hour Totals
  LES    LCV    PCV    CSS     ES    BES    SES   SEFS    UAS
    0      0      0      0      0      0      0      0      0
Current 15 Minutes Interval Time Elapsed in Current Interval:  0
  LES    LCV    PCV    CSS     ES    BES    SES   SEFS    UAS
    0      0      0      0      0      0      0      0      0
 Press any key to continue ( ESC to exit ) ...
```

Figure 4-6. Sample Detailed Interface Statistics Screen - Page 1

Screen Term	Description
Alarm State	Indicates conditions generating alarms for the T1 and E1 Interfaces. For T1: • None: Normal Operation • Red: Loss of signal • Yellow: Reception of RAI/Yellow alarm • Blue: Reception of AIS/Alarm Indication Signal • Line Loop back: TELCO test • Payload Loop back: TELCO test • POWER ON: This state is the starting state after the unit is powered up and before line activity is detected. For E1: • NONE: Normal Operation • LOS: Loss of Signal (Red) • FAS: Frame Alignment Signal • LOF: Loss of Frame • RAI: Reception of RAI/Yellow alarm (Yellow) • RAI+E: Reception of RAI with constant FEBE errors • AIS: Reception of Alarm Indication Signal (Blue) • POWER ON: This state is the starting state after the unit is powered up and before line activity is detected
Channel State 1st, 2nd, 3rd	Indicates the current state of the channel: • NORMAL: Normal operation: T1/E1 line is up • DOWN: T1/E1 line is down or unavailable, or has no time slots • TELCO Loop: Channel is placed in remote loopback by carrier • L3 Loop: Channel is placed in remote loopback by remote unit or BERT test equipment • L2 Loop: Channel is placed in local loopback

15 Minutes Statistics Screen

Figure 4-7 is an example of a T1/E1 15 Minutes Statistics screen which displays statistics for various errors. Screen terms are described in the table.

```
 Node:          Address:              Date:          Time:
 Detailed T1/E1 ISDN Interface Statistics
Interface Type: E1 - 2
                       Page:  2 of  9
Interval:   LES    LCV    PCV    CSS     ES    BES    SES   SEFS    UAS
00:15         0      0      0      0      0      0      0      0      0
00:30         0      0      0      0      0      0      0      0      0
00:45         0      0      0      0      0      0      0      0      0
01:00         0      0      0      0      0      0      0      0      0
01:15         0      0      0      0      0      0      0      0      0
01:30         0      0      0      0      0      0      0      0      0
01:45         0      0      0      0      0      0      0      0      0
02:00         0      0      0      0      0      0      0      0      0
02:15         0      0      0      0      0      0      0      0      0
02:30         0      0      0      0      0      0      0      0      0
02:45         0      0      0      0      0      0      0      0      0
03:00         0      0      0      0      0      0      0      0      0

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

Figure 4-7. Sample Detailed Interface Statistics 15 Minutes Stats Screen

:

Screen Term	Indicates...
Interval	The time period for which error count statistics are calculated.
LES	Line Error Seconds count
LCV	Line Coding Violation count
PCV	Path Coding Violation count
CSS	Controlled Slip Seconds count
ES	Errored Seconds count
BES	Bursty Errored Seconds count
SES	Severely Errored Seconds count
SEFS	Severely Errored Framing Seconds count
UAS	Unavailable Seconds count
For details regarding the error types, refer to appropriate parameters in the "Configuring the T1/E1 Interface" section in Chapter 2.	

Chapter 5
Troubleshooting with Delay Path Tracing

Overview

This chapter describes the Delay Path Tracing feature, a diagnostic test used for reporting circuit transit delay in the path associated with a selected SVC network connection.

Introduction

Delay Path Tracing measures the round-trip delay of a connection incurred on the networking levels to an accuracy expected to be within 40 milliseconds of the actual delay.

Operation With Traffic Priority

Delay Path Tracing operates with the Traffic Priority feature. The delay packet is injected into the specified connection's data queue. Traffic priority treats the delay packet the same as other data packets belonging to this priority queue.

How You Use Delay Path Tracing

You can use the results of delay path tracing to:

- Isolate the source of delay to a particular node and link combination.
- Determine whether circuit transit delay is due to network congestion or latencies in the host computer or terminal equipment.
- Determine the exact path that a given call travels.
- Give the measured delay along each hop of the path, in addition to the delay for the entire path traced.

Software Release Requirements

Every network node must have Release 4.0 software or higher to allow the Delay Path Tracing to function.

If...	*Then...*
Any network node does not have Release 4.0 or higher	a) Links that do not support delay tracing return the delay packet before the destination is reached. b) The Delay Module records the reason for the returning Response Packet, and the test report shows delay only on a partial path.
Any 3.X nodes are internal to a 4.X/5.X network	The delay path trace works, but the 3.X nodes do not report anything back to the source node.
Adjacent 4.X/5.X nodes span a 3.X set of nodes	Reports from the 4.X/5.X node record the transit delay across the 3.X nodes, as well as their own delay times.
6500 Series release 3.X nodes separate destination nodes	Only partial delays and path traces are reported.

Limitations

Delay Path Tracing does not:

- Report any delay experienced at the connection's serial protocol, except for the Delay application itself.
- Include delays at the application protocol level on the source and destination nodes.

Network Restrictions

Delay Path Tracing can be used only on:

- Vanguard networks with Delay service because of the non-standard Call Set Up facilities allowing tracing of specific virtual circuits.
- Network links that use the MX25, X.25, XDLC, and FRI-DTE with the Delay option specified.

Only delay that occurs at all the intermediate nodes and at the network level of the source and destination nodes is measured.

Default for Delay Path Tracing

The default for Delay Path Tracing specifies that ports on a 4.X/5.X node do not allow delay tracing.

To change the default and allow Delay Path Tracing, you must:

- Specify the links between nodes where Delay Path Tracing will run.
- Turn on the Delay Path Tracing option.

If the end node does not support the delay trace facility, the Delay facility is missing from an intermediate link.

The last Vanguard node should not allow the delay facility to pass through to the non-Vanguard equipment.

■ Note
When connecting to a non-VanguardMS product, do not turn on delay.

To Enable Delay Path Tracing

To enable Delay Path Tracing on X.25 and Frame Relay Annex G:

For...	***From the Configuration Menu...***
X.25	Select the X.25 Port, Select X.25 Options.
Frame Relay Annex G	Configure the FRI Station to set the X.25 options for Delay Path Tracing.

Menu Example

Figure 5-1 on the following page shows how to access the FRI Station Record and configurable parameters.

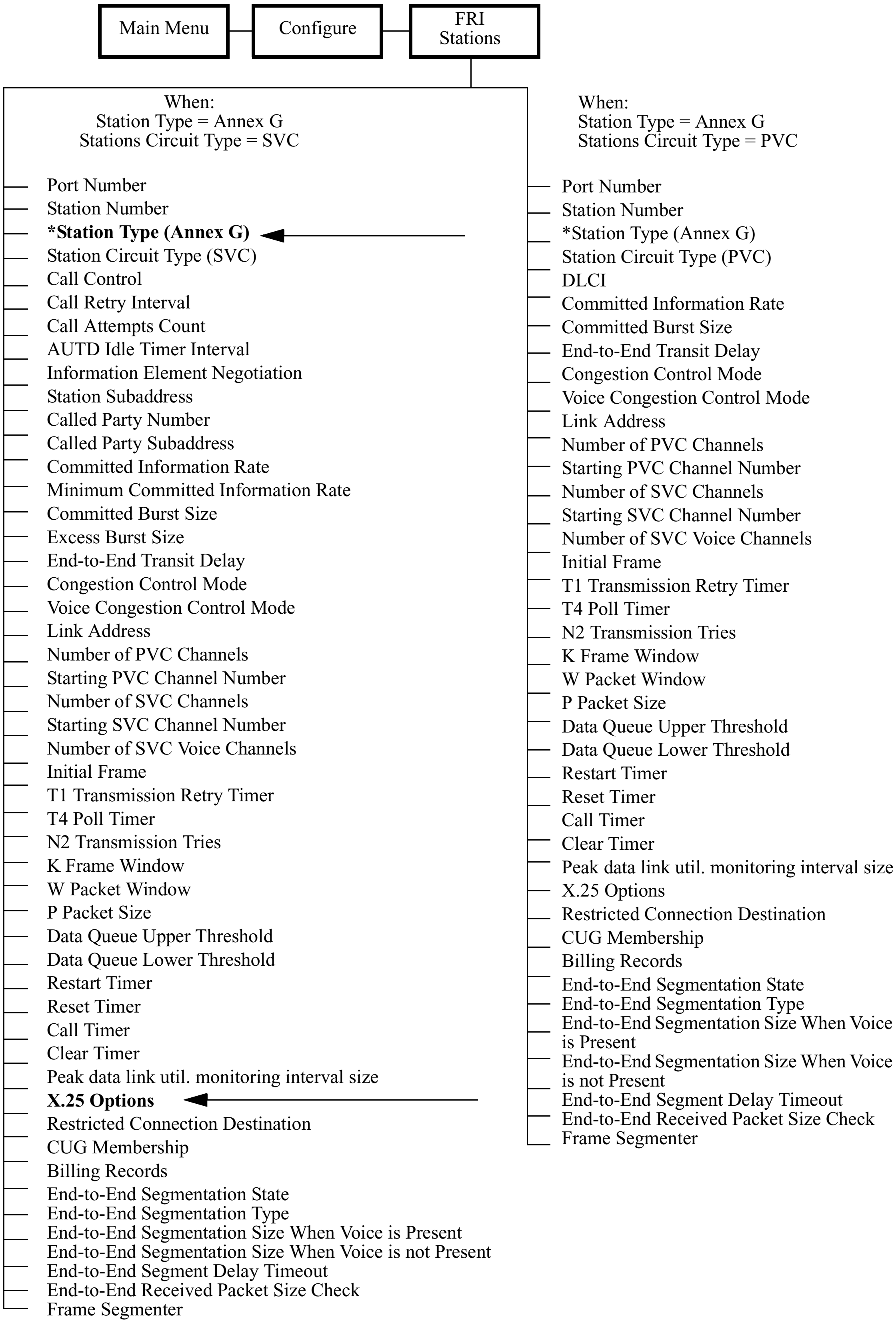

Figure 5-1. Configuration Example

How Delay Path Tracing Works

Introduction

Delay Path Tracing involves these processes:

- Call setup
- Delay data transfer

What Happens During Call Setup

Call Setup confirms that delay tracing can occur on the selected SVC using the exchange of Call Request and Call Accept packets.

Stage	Process	Result
1	The source node sends a Call Request packet.	• Informs nodes that delay processing can occur on this connection. • Sets the Node Context for future reference when Delay Data packets arrive. • Informs each node (with Delay Path Trace facility) that Delay Tracing packets will pass through the selected connection.
2	The end node and intermediate nodes respond with a Call Accept packet and a modified Delay Path Trace facility code.	• Sets the Delay facility to acknowledge that Delay Data packets will be processed. • Remote Vanguard node insert a delay trace facility acknowledgment in the Call Accept packet to be sent back to the source node. • Each 4.X/5.X node is ready to process delay test data as well as user data, during data transfer phase.

What Happens During Delay Data Transfer

When you select Delay Tracing, packets are injected into the data stream at a rate you specify. Each node forwards the delay packet along the SVC path to reach the remote node.

Delay data transfer involves this processes:

Stage	Process	Result
1	Establishes the path and link information	a) The source node issues a Resource Request packets to identify the remote nodes and to discover the available resources. b) The remote nodes respond to the source node with a Resource Response packet, which includes the name of the remote node, link number, and specific SVC (possibly station number).
2	Performs periodic delay testing	a) The source node issues Delay Request packets to gather static information about the nodes and links involved in the path. b) The Delay Response packets are issued to create a delay event at the source node for round trip timing. c) Each intermediate node returns the following to the source node: • Node name • Link number • Resource strings for inbound/ outbound data transfer • A flag indicating if the packet came from the end node d) The Delay module then periodically sends delay measurement packet requests. e) Each intermediate node immediately returns Response packets, and the request is forwarded to the downstream nodes. (See Figure 5-2.) f) The source node tracks the time between the transmission of the delay measurement request packets and arrival of responses from each intermediate and end node.

Example of Forwarding Delay Requests

Figure 5-2 shows Delay Requests being to the next node in the path. Each node responds to the source node with the delay data specific to its node.

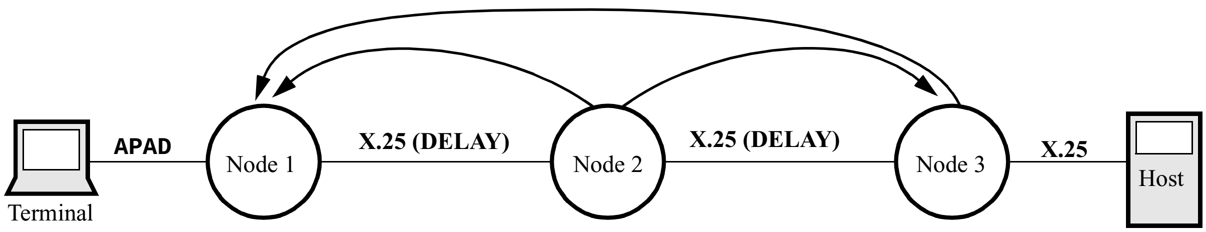

Figure 5-2. Delay Path Tracing Request/Response Packet Exchange

Relation of Delay Path Tracing to Protocol Events

Figure 5-3 shows how Delay Path Tracing processes, such as call setup and periodic delay testing, map to a sequence of resource and delay trace packet protocol events.

How the Modified Q Packet Functions in Delay Path Tracing

Figure 5-3 also highlights the function played by Q packets in delay path tracing. A Q packet is normally used to exchange information between two X.25 endpoints and is not often passed during normal data transfer.

To enable delay trace measurement, a modified Q packet is used to convey information about the selected connection. Data encapsulation of Q packets preserves application Q-bit data signalling and allows transmission of Delay Path Tracing data diagnostic information.

Within a network, encapsulation is added to every Q packet at the point of entry. The encapsulation is removed before it is forwarded to a node resource or to a networking link that does not have the Delay option turned on. Encapsulation on the Q packet allows identification of a normal user Q packet or a delay trace Q packet.

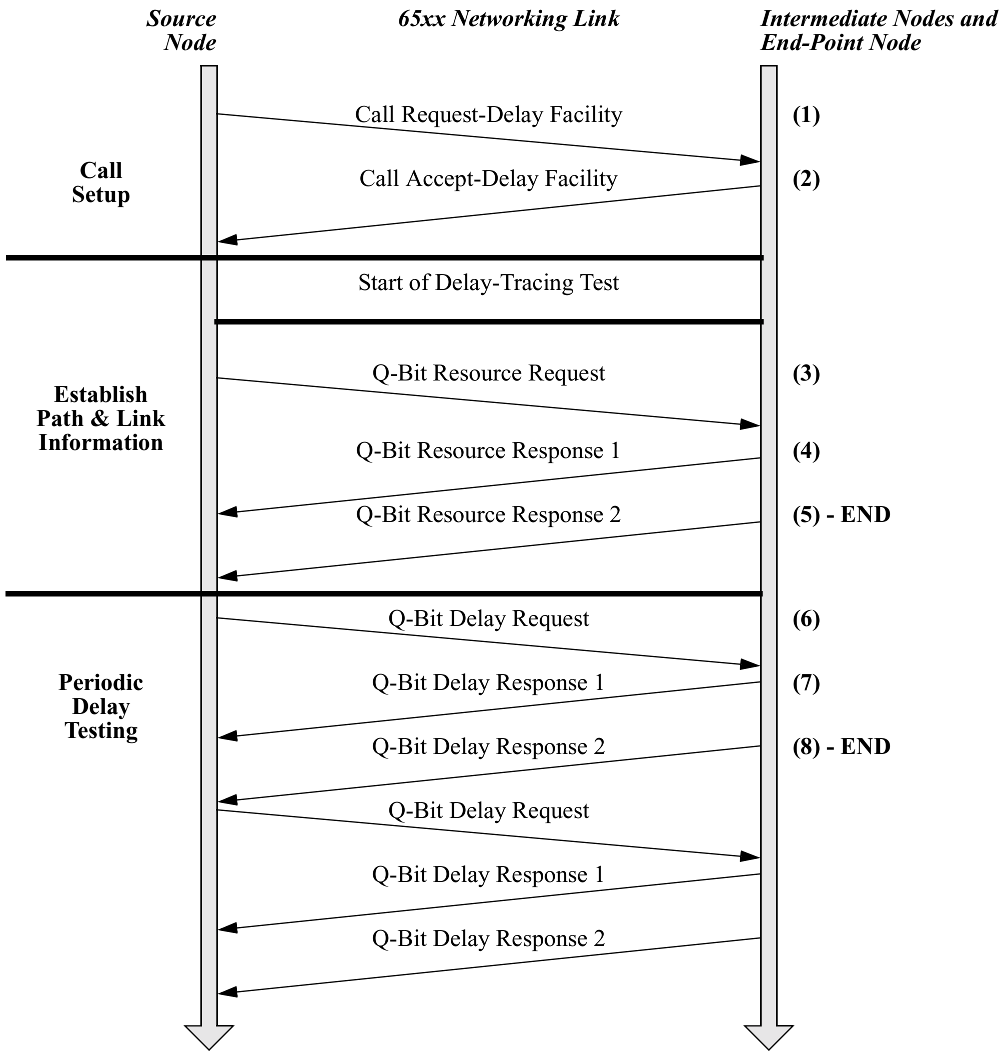

Figure 5-3. How Delay Path Tracing Processes Relate To Protocol Events

Delay Path Tracing Processes and Protocol Events

The relationship between delay path tracing processes and protocol events as shown in Figure 5-3 is described as:

Stage	Protocol Event	Result
1	Call Request — Delay Facility issued by source node	a) Includes the Delay facility. b) Each node in the network checks for the presence of this facility and, if detected, then responds to Q packets.
2	Call Accept — Delay Facility issued by end network node	a) Indicates that a remote node responded to the Call Request. b) Delay tracing can run on this SVC.
3	Q-Bit Resource Request	a) Tells all nodes along the path to respond with the network resource information for the link associated with the current call.
4	Q-Bit Resource Response issued by intermediate Nodes	a) Includes the node name, link resource names, and indication that the node is an intermediate node in this connection.
5	Q-Bit Resource Response issued by end node	a) Includes the node name, link resource names, and an indication that this node is the last in this connection.
6	Q-Bit Delay Request	a) Informs each node to send a response packet back to the source node. b) Each node forwards the request to the next node in the network.
7	Q-Bit Delay Response - forwarded by intermediate nodes	a) The source node receives Q-Bit Delay Response. b) The source node time stamps the arrival of these packets. c) The source node compares packet arrival time with the time that the Request was sent out.
8	Q-Bit Delay Response - forwarded by the intermediate nodes	a) The source node receives Q-Bit Delay Response. b) The source node time stamps arrival of the packet. c) The source node compares the time against the time the request was sent out. Arrival of this end node packet invalidates any others that arrive out of sequence from other nodes in the path.

Function of Network Node Interface in Delay Path Tracing

The network node interface, source nodes, intermediate nodes, and end nodes each perform certain roles and functions in the delay path tracing process.

Stage	Functional Role
1	Each node responds to the Request Delay Path packets sent to it by forwarding requests to the next downstream 4.X/5.X node.
2	The remote node responses are directed back to the source node for processing of delay data.
3	The Delay Request acts as an event trigger for the source node, logging the time of arrival of the delay trace response packets.

Function of Source Node in Delay Path Tracing

The source node controls the type of protocol that is run between itself and the endpoint using an exchange of Resource Requests and Resource Responses.

Stage	Functional Role
1	The source node sends the initial Resource Request.
2	The remote nodes respond to the source node with this information: • Name of the remote node • Link number • Specific SVC (possibly station number)
3	The source node receives and logs the preceding responses until the End Node Resource Response arrives at the source node.
4	The source node sends the Delay Trace Request.
5	The source node receives the Delay Responses from the remote nodes until the End Node Delay Response arrives.
6	The source node compares the Delay Response time stamp with the Delay Request time stamp to calculate the round trip delay from the source to each node on the delay trace path.

Function of Intermediate Nodes in Delay Path Tracing

The intermediate nodes serve these functions in delay path tracing:

Stage	Functional Role
1	Each intermediate node relays the delay resource request packet and Delay Trace Request packet to the next node in the SVC path.
2	Delay resources for the node are sent back to the source node in the resource response packet.
3	When the source node receives the delay request packet, the node responds immediately with a delay response packet and a timing event for round trip delay measurement, including current link speed.

Function of End Nodes in Delay Path Tracing

The end nodes serve these functions in Delay Path Tracing:

Stage	Functional Role
1	The end node Resource Response defines the number of nodes in the delay trace path by counting the delay resource test packets.
2	The end node processes the Resource Request and Delay Response test packets exactly as in the intermediate node.
3	The end node sends the Resource Request and Delay Response test packets to the source node; after which the end node does not expect to receive packets from other nodes.

Delay Measurement Test

Delay Measurement Test

Delay Measurement Test (formally called Delay Path Test, prior to 5.3 software) measures a round trip delay from a source connection to a destination connection.

Proper Syntax

Before running a Delay Measurement Test, you need to find the connection points proper syntax.

Syntax example: PAD-6, LCON-1, FRA-2S1, and SDLC-3S1

Proper syntax can be found within the nodes statistics:

Step	*Action*	*Result*
1	Select **Status/statistics** for the Control Terminal Port (CTP) Main Menu.	The menu for **Status/statistics** displays.
2	Select **Network Service Stats** from the **Status/statistics** Menu	The **Network Service Stats** menu displays.
3	Select: **SVC Call Summary** or **PVC Call Summary** **e.g. ATPAD-3, X25-4, FRI-3s4**	■ **Note** The SVC or PVC you are testing must be connected to perform the test.

■ **Note**

The network links along the trace path should have the delay option assigned. For example, X.25 and FR Annex G have a parameter called X.25 Options. For more information on this parameter See “X.25 Options” on page 40.

Accessing Delay Path Tracing

Introduction

Delay Path Tracing is accessible from the Diagnostics menu.

Limitations for NMS Users

Delay and Path Trace menus are not currently supported by a network management system (NMS).

NMS users must open a terminal emulation window and log on to the CTP to use the Delay and Path Trace commands.

Menu Selections to Enable Delay Path Tracing

These selections, which are accessible from the Diagnostics menu screen, support delay path tracing:

- Start Delay Measurement
- Stop Delay Measurement
- Display Delay Summary

Accessing the Diagnostics Menu

Use this procedure to access the Diagnostics menu:

Step	*Action*	*Result*
1	Select **Diagnostics** from the CTP Main menu.	The Diagnostics menu appears.
2	Enter a selection number.	The requested screen appears.

Screen Example

Figure 5-4 shows an example of the Diagnostics menu screen.

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

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

Figure 5-4. Diagnostics Menu

Function of the Delay Sub-facility

The Delay subfacility interrogates the adjacent connection to determine:

- If the adjacent link is a networking link.
- If the Delay option is enabled.
- Misconfiguration of a 4.X/5.X node (if Link Delay turned ON, and if end node is 3.X.

When you turn on the delay option at the outgoing link, the Delay subfacility:

- Is added to every call packet originating at a node.
- Applies to every transit call that comes in from a networking link with the Delay option disabled.

Start Delay Measurement

Use this procedure to start Delay Path Tracing measurement:

Step	Action	Result/Description
1	Log on to the CTP where the endpoint of the call resides.	An endpoint is either: a) a local resource of the node that does not have the Delay feature enabled. b) a virtual circuit on a networking link or station.
2	Specify the name of one of the two endpoints in the connection.	
3	See "Start Delay Measurement Parameters" in this table for details on individual input parameters. Then enter the values for each input parameters.	Once the input has been entered, the remaining portion of the screen displays as shown in Figure 5-5 .

Start Delay Measurement Parameters

The Start Delay Measurement parameters control the setup. Real time statistics are displayed on the screen for the measured delay for a particular trace.

Channel to Trace

Range:	5 to 16 alphanumeric characters
Default:	(blank)
Description:	Specifies the name of the connection to be traced. Use the space bar to blank field.

Time Between Test Packets

Range:	2 to 60
Default:	5
Description:	Specifies the number of seconds between test packets.

Duration in Minutes

Range:	1 to 9999
Default:	10
Description:	Specifies the duration of the test in minutes.

Start Delay Measurement Diagnostics Screen

Figure 5-5 shows an example of Start Delay Measurement Diagnostics screen.

```
Channel to Trace:                    /MX25-2S4(15)
Time between test packets (sec.): 5/20
Duration in minutes: 10/
----------------------------------------------------------
Node:           Address:                  Date:            Time:
Menu: Start Delay Measurement             Path: (Main.12.6)  Page 1 of 1

START TIME:                @                        STATUS: RUNNING
STOP TIME:                                          PACKETS SENT: 1
CURRENT PATH: END-TO-END

PATH TRACE
MX25-2S4(15)   [TORONTO]   X25-1 (23)     @ 80000
M25-2 (23)     [BOSTON]    X25-3 (12)     @ 80000
X25-2(23)      [CHICAGO]   X25-3 (12)     @ 80000
X25-2 (23) [NEWYORK]       X25-3 (12)     @ 80000

Last Measured Round Trip Delay: 143 ms @ 8:23:32      PACKETS SENT: 7

Continue to run test in background after exit (Y/N)?__

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

Figure 5-5. Start Delay Measurement Diagnostics Screen

Start Delay Measurement Diagnostics Screen Terms

The Start Delay Measurement Diagnostics screen contains this information:

Screen Term	***Tells You...***
START TIME	Time when the test was initiated.
STOP TIME	Time when the test is completed or aborted. This field is blank if the test is still running.
STATUS	• RUNNING: Test is in progress. • STOPPED: Test is complete. • ABORTED: Test is stopped due to: – Call cleared – Test packets lost, or – User command.
PACKETS SENT	Current count of the number of delay test packets sent since test began.
CURRENT PATH	• END-TO-END: The endpoint is a local resource in the Release 4.0 or later node. • PARTIAL: The endpoint is not a local resource *but* is an intermediate *or* end node that terminates with a network resource (PDN, foreign host, or 3.X network).
PATH TRACE	• Shows the path of the connection: • The first line shows the name of the end resource. • The next line lists all the various network connections that the call passes through. • The last item shows the name of the connection that leaves the last Release 4.X/5.X node.
Last Measured Round Trip Delay	This field is continually updated in real-time with the current network round trip delay and the current time as the delay packets are returned from the destination node.
Continue to run test in background?	Responding with either a **Y** or **N** causes the CTP to return to the diagnostics menu. However, a **Y** response allows the test to run in background (even if you log off the CTP) until the specified duration expires.

Running A Delay Measurement Test

Running a Delay Measurement Test

Follow these steps to run a delay measurement test:

Step	Option	Action
1	Connect to the node you are performing the test from.	Choose the Source or Destination connection from the statistics SVC or PVC Call Summary screen.
2	Begin the test from the nodes connection point.	**Diagnostics->Start Delay Measurement-> Channel to trace** (Enter the current connections syntax from the call summary screen.) • Time between test packets: 5 sec • Duration in minutes: 10 (Enter a time in minutes to run the test 1-9999) **Begin Delay Test**
3	The test results continually update to the screen.	By pressing **ESC**, you are given the option to allow the test to run in the background, or you can cancel the test completely.
4	To stop a test that is running in the background.	Choose **Diagnostics->Stop Delay Measurement**
5	A delay summary screen is also provided for viewing at any time.	Choose **Diagnostics->Display Delay Summary.**

Terminating Delay Path Tracing Measurement

Introduction

A delay test may be terminated by the:

- Operator
- System

Effect of Test Termination

When a delay test is terminated, test results remain in memory:

- Until the node is booted.
- You start another test that overwrites the data.

Operator-initiated Test Termination

You can terminate a delay test in two ways:

- Press the ESC key within the Start Delay menu.
- Use the Stop Delay measurement menu.

Use this procedure to stop a delay test that is running:

Step	Action	Result
1	From the Diagnostics Menu, select Stop Delay Measurement.	The Stop Delay Measurement screen appears, shown in Figure 5-6, detailing a numbered list of the active connections traced. (If a delay trace slot is not actively performing a delay trace, the connection field for that particular field shows “NONE.”)
2	To stop a specific currently active SVC, enter a selection numbered 1 through 5. Or: To stop all currently traced SVCs, enter selection number 6.	The message Delay Trace on xxxx stopped (1 through 5) appears. The message ALL delay trace connections stopped (6).

Stop Delay Measurement Screen

Figure 5-6 shows an example of the Stop Delay Measurement screen.

```
Node:               Address:          Date:               Time:
Menu: Stop Delay Measurement          Path: (Main.12.7)   Page 1 of 1


Active Connections Traced:


   MX25-21S3 (66)
   PAD-6
   FRI-5S2 (15)
   BSC3270-1S6
   NONE
   ALL




Select Connection to Stop: 0/2


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

Figure 5-6. Stop Delay Measurement Screen

System-initiated Termination Test

The system terminates a delay test under the following conditions:

- The call is cleared on the monitored link for any reason, including the case where the call is taken down due to link or node failure but rerouted to a different link by DCP.
- The first delay packet to gather path and resource information is not returned properly.
- One or more of the delay measurement packets are lost in the network, and the number of times that this occurs on this test exceeds 10.

Delay Path Tracing Measurement Reporting

Introduction

The Display Delay Summary screen reports on a node-by-node basis the delay between each node on the patch from source to destination, as well as an overall end-to-end delay.

Examples of Display Delay Summary Screen

Figures 5-7 and 5-8 represent a report that is displayed for a network consisting of six or more nodes.

For networks with fewer than six nodes, the data on the two pages is combined and displayed on one screen.

```
Node:              Address:           Date:                 Time:
Menu: Display Delay Summary           Path: (Main.12.8)     Page 1 of 2

START TIME:               @             STATUS: RUNNING
STOP TIME:                @             PACKETS SENT: 1234
CURRENT PATH: END-TO-END

PATH TRACE:
MX25-2S4(15) [TORONTO]   X25-1 (23)     @ 80000
M25-2 (23)   [BOSTON]    X25-3 (12)     @ 80000
X25-2(23)    [CHICAGO]   X25-3 (12)     @ 80000
X25-2 (23)   [NEWYORK]   X25-3 (12)     @ 80000
X25-2 (23)   [WASH01]    X25-3 (12)     @ 80000
X25-2 (23)   [WASH02]    X25-3 (12)     @ 80000
X25-2 (23)   [RALEIGH]   X25-3 (12)     @ 80000
X25-2 (23)   [BUFFALO]   X25-3 (12)     @ 9600
X25-23 (10)  [ALBANY]    X25-17 (23)    @ 80000
X25-18 (04)  [PITTSB]    X25-10 (05)    @ 80000
X25-23 (12)  [TOLEDO]    X25-22 (03)    @ 80000
X25-11 (06)  [CORNING]   PAD-6

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

Figure 5-7. Display Data Summary Screen, First Page

```
Node:                   Address:          Date:              Time:
Menu: Display Delay Summary               Path: (Main.12.8)   Page 2 of 2

START TIME:               @                   STATUS: RUNNING
STOP TIME:                @                   PACKETS SENT: 1234

                          MEASURED DELAY (ROUND TRIP):
NODE                  MINIMUM (ms)                MAXIMUM        AVG (ms)
TORONTO-BOSTON        82 @ hh:mm:ss               150 @ hh:mm:ss    110
BOSTON-CHICAGO        5 @ hh:mm:ss                112 @ hh:mm:ss    110
CHICAGO-NEWYORK       45 @ hh:mm:ss               132 @ hh:mm:ss    110
NEWYORK-WASH01        12 @ hh:mm:ss               112 @ hh:mm:ss    110
WASH01-WASH02         19 @ hh:mm:ss               198 @ hh:mm:ss    110
WASH02-RALEIGH        36 @ hh:mm:ss               156 @ hh:mm:ss    110
RALEIGH-BUFFALO       31 @ hh:mm:ss               235 @ hh:mm:ss    110
BUFFALO-ALBANY        19 @ hh:mm:ss               349 @ hh:mm:ss    110
ALBANY-PITTSB         23 @ hh:mm:ss               234 @ hh:mm:ss    110
PITTSB-TOLEDO         43 @ hh:mm:ss               313 @ hh:mm:ss    110
TOLEDO-CORNING        23 @ hh:mm:ss               131 @ hh:mm:ss    110
End-End Delay         820 @ hh:mm:ss              282 @ hh:mm:ss    350

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

Figure 5-8. Display Delay Summary Screen, Second Page

Display Delay Summary Screen

The Display Delay Summary screen contains this information:

Screen Term	Tells You...
START TIME	Time when test is initiated.
STOP TIME	Time when test is completed. This field is blank if the test is still running.
STATUS	Current process status of trace: • RUNNING: Delay trace still in progress and the following statistics are intermediate results only. • STOPPED: The following test results are the completed statistic on this trace. • ABORTED: Test is stopped due to: – Call cleared – Test packets lost, or – User command.
PACKETS SENT	Current count of the number of delay test packets sent from the time of the start of the test.

Screen Term *(continued)*	***Tells You...***
CURRENT PATH	• END-TO-END: The destination node echoed the delay packet, with a local resource string. • PARTIAL: The destination node returned a networking resource string (X.25, MX25, FRI).
PATH TRACE	• Virtual Circuit path from source to destination node, listing: • All the intermediate nodes • The link • Station • LCN number
MEASURED DELAY (ROUND TRIP)	• Lists the measured round trip delay between nodes that the specified trace passes through. • Highlights nodes that are performing poorly, such as those with higher than normal delay or lower link speeds compared to the rest of the nodes in the delay trace path.

Chapter 6
Logical Channel Number Maps

Overview

CCITT Recommendation X.25 defines the Logical Channel Number (LCN) to be a 12-bit binary number that ranges from 0 to 4095 (decimal). In many instances, these 12 bits are broken into an 8-bit LCN with a range of 0 to 255 (decimal) and a 4-bit Logical Channel Group Number (LCGN) with a range of 0 to 15 (decimal).

LCGN

Figure 6-1 shows how the 4-bit LCGN is formed from the most significant bits of the 12-bit number:

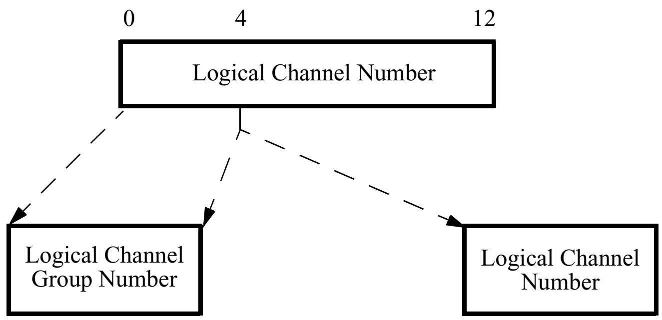

Figure 6-1. Forming the LCGN

8 + 4 Bit Logical Channel Number Mapping

When configuring channels on Vanguard X.25 links, you may need to map the 12-bit full channel number to the equivalent 4-bit Logical Channel Group Number plus the 8-bit Logical Channel Number. This table indicates this mapping.

12-Bit Logical Channel Number																
8-Bit	***4-Bit Logical Channel Group Number***															
LCN	***0***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***
0	0	256	512	768	1024	1280	1536	1792	2048	2304	2560	2816	3072	3328	3584	3840
1	1	257	513	769	1025	—	—	—	—	—	—	2817	3073	3329	3585	3841
2	2	258	514	770	—	—	—	—	—	—	—	—	3074	3330	3586	3842
3	3	259	515	—	—	—	—	—	—	—	—	—	—	3331	3587	3843
4	4	260	—	—	—	—	—	—	—	—	—	—	—	—	3588	3844
5	5	—	—	—	—	—	—	—	—	—	—	—	—	—	—	3845
6	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
255	255	511	767	1023	1279	1535	1791	2047	2303	2559	2815	3071	3327	3583	3839	4095

Chapter 7
X.25 Facility Codes

Overview

This chapter describes the packet types and formats commonly found with the X.25 protocol.

X.25 Packet Header

Figure 7-1 shows the X.25 packet header.

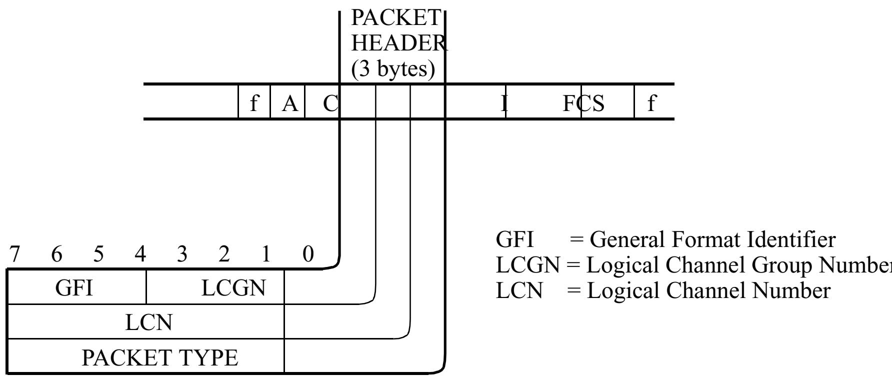

Figure 7-1. X.25 Packet Header

■Note

The Packet Header may contain an extra octet when the numbering is Modulo 128. The GFI format is:

Bit Number	7	6	5	4	
	Q	D	0	1	sequence numbering Modulo 8
	Q	D	1	0	sequence numbering Modulo 128

where 0 = 1 indicates X.29 Data Packet

D = 1 indicates Delivery Confirmation in Call and Data Packets

Packet Type Formats

This table describes the packet types:

Packet Type		*Service*		*Encoding*								*Hex*
From DCE to DTE	*From DTE to DCE*	*SVC*	*PVC*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*0*	
Call Set-Up and Clearing												
Incoming Call	Call Request	X		0	0	0	0	1	0	1	1	0B
Call connected	Call Accepted	X		0	0	0	0	1	1	1	1	0F
Clear Indicator	Clear Request	X		0	0	0	1	0	0	1	1	13
DCE Clear Confirmation	DTE Clear Confirmation	X		0	0	0	1	0	1	1	1	17
Data and Interrupt												
DCE Data	DTE Data (Modulo 8)	X	X	P (R)			M	P(S)			0	xx
DCE Data	DTE Data (Modulo 128)	X	X	P (S)							0	xx
				P (R)							M	xx
DCE Interrupt	DTE Interrupt	X	X	0	0	1	0	0	0	1	1	23
DCE Int. Confirmation	DTE Int. Confirmation	X	X	0	0	1	0	0	1	1	1	27
Flow Control and Reset												
DCE RR	DTE RR (Modulo 8)	X	X	P (R)			0	0	0	0	1	x1
DCE RNR	DTE RNR (Modulo 8)	X	X	P (R)			0	0	1	0	1	x5
	DTE REJ (Modulo 8)	X	X	P (R)			0	1	0	0	1	x9
DCE RR	DTE RR (Modulo 128)	X	X	0	0	0	0	0	0	0	1	01
				P (R)							0	xx
DCE RNR	DTE RNR (Modulo 128)	X	X	0	0	0	0	0	1	0	1	03
				P (R)							0	xx
	DTE REJ (Modulo 128)	X	X	0	0	0	0	1	0	0	1	09
				P (R)							0	xx
Reset Indication	Reset Request	X	X	0	0	0	1	1	0	1	1	1B
DCE Reset Confirmation	DTE Reset Confirmation	X	X	0	0	0	1	1	1	1	1	1F
Restart												
Restart Indication	Restart Request			1	1	1	1	1	0	1	1	FB
DCE Restart Confirmation	DTE Restart Confirmation	X	X	1	1	1	1	1	1	1	1	FF

***Packet Type** (continued)*		**Service**		**Encoding**								**Hex**
From DCE to DTE	***From DTE to DCE***	***SVC***	***PVC***	***7***	***6***	***5***	***4***	***3***	***2***	***1***	***0***	
Diagnostic												
Diagnostic		X	X	1	1	1	1	0	0	0	1	F1
Registration												
	Registration Request			1	1	1	1	0	0	1	1	F3
Registration Confirmation				1	1	1	1	0	1	1	1	F7

Packet Types

These tables show various packet types:

	7	6	5	4	3	2	1	0
Octet 1	0Dfs				LCGN			
2	LCN							
3	0	0	0	0	1	0	1	1
4	Calling DTE Address Length				Called DTE Address Length			
	DTE Address(es)							
					0	0	0	0
	0	0	Facilities Length (<109 Bytes)					
	Facilities							
	Call User Data							

Call Request/ Indication Packet

	7	6	5	4	3	2	1	0
Octet 1	0Dfs				LCGN			
2	LCN							
3	0	0	0	0	1	1	1	1
4	Calling DTE Address Length				Called DTE Address Length			
	DTE Address(es)							
					0	0	0	0
	0	0	Facilities Length (<109 Bytes)					
	Facilities							
	Call User Data Fast Select							

Call Accepted/ Connected Packet

	7	6	5	4	3	2	1	0
Octet 1	00fs				LCGN			
2	LCN							
3	0	0	0	1	0	1	1	1

	7	6	5	4	3	2	1	0
Octet 1	00fs				LCGN			
2	LCN							
3	0	0	1	0	0	0	1	1

Clear Confirmation Packet

Interrupt Packet

	7	6	5	4	3	2	1	0
Octet 1	00fs				LCGN			
2	LCN							
3	0	0	1	0	0	1	1	1

Interrupt Confirmation Packet

	7	6	5	4	3	2	1	0
Octet 1	QD01				LCGN			
2	LCN							
3	P(R)			M	P(S)			0
	User Data							

Data Packet (Modulo 8)

	7	6	5	4	3	2	1	0
Octet 1	00fs				0	0	0	0
2	0	0	0	0	0	0	0	0
3	1	1	1	1	0	0	0	1
4	Diagnostic Code							
	Diagnostic Explanation							

Diagnostics Packet

	7	6	5	4	3	2	1	0
Octet 1	QD10				LCGN			
2	LCN							
3	P(S)							0
4	P(R)							M
	User Data							

Data Packet (Modulo 128)

fs = 01 for normal (Modulo 8) sequencing

fs = 10 for extended (Modulo 128) sequencing

	7	6	5	4	3	2	1	0
Octet 1	0	0	0	1	LCGN			
2	LCN							
3	P(R)			0	0	0	0	1

Receiver Ready (RR) Packet
(Modulo 8)

	7	6	5	4	3	2	1	0
Octet 1	0	0	0	1	LCGN			
2	LCN							
3	P(R)			0	0	1	0	1

Receiver Not Ready (RNR) Packet
(Modulo 8)

Octet	7	6	5	4	3	2	1	0
1	0	0	1	0	LCGN			
2	LCN							
3	0	0	0	0	0	0	0	1
	P(R)							0

Receiver Ready (RR) Packet
(Modulo 128)

Octet	7	6	5	4	3	2	1	0
1	0	0	1	0	LCGN			
2	LCN							
3	0	0	0	0	0	1	0	1
4	P(R)							0

Receiver Not Ready (RNR) Packet
(Modulo 128)

Octet	7	6	5	4	3	2	1	0
1	0	0	0	1	LCGN			
2	LCN							
3	P(R)			0	1	0	0	1

Reject Packet
(Modulo 8)

Octet	7	6	5	4	3	2	1	0
1	0	0	1	0	LCGN			
2	LCN							
3	0	0	0	0	1	0	0	1
4	P(R)							0

Reject Packet
(Modulo 128)

Octet	7	6	5	4	3	2	1	0
1	00fs				LCGN			
2	LCN							
3	0	0	0	1	1	0	1	1
4	Resetting Cause							
5	Diagnostic Code							

Reset Packet

Octet	7	6	5	4	3	2	1	0
1	00fs				LCGN			
2	LCN							
3	0	0	0	1	1	1	1	1

Reset Configuration Packet

	7	6	5	4	3	2	1	0
Octet 1	00fs				0	0	0	0
2	0	0	0	0	0	0	0	0
3	1	1	1	1	1	0	1	1
4	Restarting Cause							
5	Diagnostic Code							

Restart Packet

	7	6	5	4	3	2	1	0
Octet 1	00fs				0	0	0	0
2	0	0	0	0	0	0	0	0
3	1	1	1	1	1	1	1	1

Restart Confirmation Packet

fs = 01 for normal (Modulo 8) sequencing

fs = 10 for extended (Modulo 128) sequencing

	7	6	5	4	3	2	1	0
Octet 1	00fs				0	0	0	0
2	0	0	0	0	0	0	0	0
3	1	1	1	1	0	0	1	1
4	Calling DTE Address Length				Called DTE Address Length			
	DTE Address(es)							
					0	0	0	0
	0	Registration Length						
	Registration							

Registration Packet

	7	6	5	4	3	2	1	0
Octet 1	00fs				0	0	0	0
2	0	0	0	0	0	0	0	0
3	1	1	1	1	0	1	1	1
4	Cause							
5	Diagnostic							
6	Calling DTE Address Length				Called DTE Address Length			
	DTE Address(es)							
					0	0	0	0
	0	Registration Length						
	Registration							

Registration Confirmation Packet

7	6	5	4	3	2	1	0

Octet								
1	0Dfs				LCGN			
2	LCN							
3	0	0	0	1	0	0	1	1
4	Clear Cause							
5	Diagnostic Code							
	Calling DTE Address Length				Called DTE Address Length			
	DTE Address(es)							
					0	0	0	0
	0	0	Facilities Length (<109 Bytes)					
	Facilities							
	Call User Data							

Clear Request/ Indication Packet

fs = 01 for normal (Modulo 8) sequencing

fs = 10 for extended (Modulo 128) sequencing

Coding for Clearing

This table shows the coding for clearing cause field in clear indication packet:

Clearing Cause	***7***	***6***	***5***	***4***	***3***	***2***	***1***	***0***	***HEX***	***DEC***
DTE Originated	0	0	0	0	0	0	0	0	00	0
DTE Originated (refer to Note)	1	x	x	x	x	x	x	x	xx	
Number Busy	0	0	0	0	0	0	0	1	01	1
Out of Order	0	0	0	0	1	0	0	1	09	9
Remote Procedure Error	0	0	0	1	0	0	0	1	11	17
Reverse Charge Acceptance Not Subscribed	0	0	0	1	1	0	0	1	19	25
Incompatible Destination	0	0	1	0	0	0	0	1	21	33
Fast Select Not Subscribed	0	0	1	0	1	0	0	1	29	41
Invalid Facility Request	0	0	0	0	0	0	1	1	03	3

Access Barred	0	0	0	0	1	0	1	1	0B	11
Local Procedure Error	0	0	0	1	0	0	1	1	13	19
Network Congestion	0	0	0	0	0	1	0	1	05	5
Not Obtainable	0	0	0	0	1	1	0	1	0D	13
RPOA Out Of Order	0	0	0	1	0	1	0	1	15	21

■ **Note**
When bit 7 is set to 1, the bits represented by x are those included by the remote DTE in the Clearing or Restarting Cause field of the Clear or Restart Request packets, respectively.

Cng for Resetting

This table shows the coding for resetting cause field in the reset packet:

Coding for Resetting Cause Field in Reset Packet

Clearing Cause	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*0*	*HEX*	*DEC*
DTE Originated	0	0	0	0	0	0	0	0	00	00
	1	x	x	x	x	x	x	x	xx	
Out of Order	0	0	0	0	0	0	0	1	01	1
Remote Procedure Error	0	0	0	0	0	0	1	1	03	3
Local Procedure Error	0	0	0	0	0	1	0	1	05	5
Network Congestion	0	0	0	0	0	1	1	1	07	7
Remote DTE Operational (PVC)	0	0	0	0	1	0	0	1	09	9
Network Operational (PVC)	0	0	0	0	1	1	1	1	0F	15
Incompatible Destination	0	0	0	1	0	0	0	1	11	17
Network Out Of Order	0	0	0	1	1	1	0	1	1D	29

Standard For Diagnostic Codes

This table shows the standard diagnostic codes in clear, reset, and restart indication, registration confirmation, and diagnostic packets.

Refer to X.25 Recommendation for details.

Diagnostic	*HEX*	*DEC*
No Additional Information	00	0
Invalid P(S)	01	1
Invalid P(R)	02	2
Packet Type Invalid	10	16
Other Types (Note 1)	xx	16
Packet Not Allowed	20	32
Unidentifiable Packet	21	33
Call On One-way Logical Channel	22	34
Invalid Packet Type on a PVC	23	35
Packet on an unassigned Logical Channel	24	36
Reject not subscribed to	25	37
Packet too short	26	38
Packet too long	27	39
Invalid GFI	28	40
Restart, or Registration, with non-zero in bits 0-3, 8-15	29	41
Packet type not compatible with facility	2A	42
Unauthorized interrupt confirmation	2B	43
Unauthorized Interrupt	2C	44
Unauthorized Reject	2D	45
Timer Expired	30	48
For Incoming Call	31	49
For Clear Indication	32	50
For Reset Indication	33	51
For Restart Indication	34	52
Call Set-Up, Clearing or Registration Problem	40	64
Facility/Registration Code not allowed	41	65
Facility Parameter not allowed	42	66
Invalid Called Address	43	67
Invalid Facility/Registration length	45	69
Incoming Call barred	46	70
No Logical Channel available	47	71
Call collision	48	72

Diagnostic *(continued)*	***HEX***	***DEC***
Duplicate facility requested	49	73
Non-zero address length	4A	74
Facility not provided when expected	4C	76
Invalid CCITT-specified DTE facility	4D	77
Miscellaneous	50	80
Improper cause code from DTE	51	81
Not aligned octet	52	82
Inconsistent Q-bit setting	53	83
International Problems	70	112
Remote network problem	71	113
International protocol problem	72	114
International link out of order	73	115
International link busy	74	116
Transit network facility problem	75	117
Remote network facility problem	76	118
International routing problem	77	119
Temporary routing problem	78	120
Unknown called DNIC	79	121
Maintenance action	7A	122
Reserved for Public-Network-Specific Information	80	--
Other types (refer to the next table for details)	8x	--

6500^{PLUS} Specific Diagnostic Code Messages

The following table shows diagnostic code messages for the 6500^{PLUS}.

Diagnostic	*HEX*	*DEC*
Call limit reached on intermediate node	80	128
Call limit reached on destination node	81	129
No LCN available on node that is not the call destination	82	130
Call disconnected by Control Terminal Port	83	131
Link failure in intermediate node	84	132
Routing loop detected	85	133
Call passed through too many nodes	86	134
Received Restart at Level 3	9A	154
Received DISC at Level 2	9C	156
Received DM at Level 2	9D	157
Received SABM at Level 2	9E	158
Received FRMR at Level 2	9F	159
Received invalid N(R). Transmit FRMR.	A0	160
Received unsolicited F Bit. Transmit FRMR	A1	161
Received unknown command. Transmit FRMR.	A2	162
Received unknown response. Transmit FRMR.	A3	163
Received I field too long for L1. Transmit FRMR.	A4	164
No response after N2 tries. Transmit SABM.	A5	165
Received frame of incorrect size. Transmit FRMR.	AE	174
Address error, sent FRMR	AF	175
Source Port is in Busy Out State	B0	176
Destination Port is in Busy Out State	B1	177
Diag_Reconn-Rejected	B2	178
Invalid Call Request	B3	

A

Alarm Priority 2-51, 2-52
Autocall Mnemonic
  parameter 2-12

B

BKUP
  setting 2-6

C

Call Facility 2-66, 2-69
Call Security 2-48
Call Setup 5-4
Call Timer 2-38
Clear Timer 2-39
Configuration
  inbound call translation table 3-2
  outbound call translation table 3-5
  PVC broadcast output table 3-16
  X.25 Port
    guidelines 2-6
  X.25 Port Record 2-5
Configuring
  Outbound Call Address Translation 3-9
  T1/E1 Interface 2-15
Connection Type 2-6
  EMDC 2-6
  EMRI 2-6
  SIMPv guidelines 2-6
  X.25 Port 2-30
Control signals
  summary 1-7
control signals
  DIMO 1-15
  DIMS 1-8
  port disabled 1-8
CUD 2-45
  setting 2-6
CUG 2-47
  entering a value 2-6
  membership 2-47
CUG (See Closed User Group)
  identifier 2-62

D

Data Connection Protection 2-48
Data Queue Lower Threshold 2-37
Data Queue Upper Threshold 2-37
DCP 2-48
Delay Data Transfer 5-5
Delay option 5-13

D (Continued)

Delay Path Tracing 5-1
  accuracy 5-1
  call setup 5-4
  configuration 5-12
  delay sources 5-1
  measured delay 5-1
  network congestion 5-1
  network node interface 5-9
  process 5-4
  Processes and Protocol Events 5-8
  Q packets 5-6
  restricted network use 5-2
  Software Release Requirements 5-1
  version requirements 5-1
Detailed Port Statistics 4-2
Detailed Port Stats
  X.25 4-2
Diagnostics Menu 5-12
DIMOv
  guidelines 2-6
DIMs 1-8

F

Facilities
  to add to Outbound Calls 2-39
  to bar in Inbound Calls 2-40
  to bar in Outbound Calls 2-40
  to delete from Outbound Calls 2-39
Facility
  bilateral closed user group 2-70
  datagram 2-68, 2-70
  fast select 2-67, 2-70
  inbound calls 2-66
  network user identification 2-67, 2-70
  outbound calls 2-69
  packet size negotiation 2-66, 2-69
  reverse charging 2-67, 2-70
  throughput class negotiation 2-70
  window size negotiation 2-67, 2-69
Facility Checking 2-44
Facility Codes 2-44
Facility Subscription Control 2-49
Features
  CUG 2-62
FRA Station Parameters
  Traffic Priority 2-18, 2-19, 2-20, 2-21, 2-22, 2-23, 2-24, 2-25, 2-26, 2-27
Frame Sequence Counting 2-34

H

Hop Count Facility Code 2-60
How Delay Path Tracing Works 5-4

I

Idle Disconnect Timer 2-47
setting 2-6
Inbound call translation table
configure 3-2
Inbound Calling Address 3-4, 3-18
Inbound/Outbound Call Translation Tables
guidelines 3-2

K

K Frame Window 2-35

L

LAN Connection
table record 2-11
LAN Forwarder Type
parameter 2-12
Limitations 5-2

M

Maximum Negotiated Packet Size 2-36
Maximum Number of Autocall Attempts
parameter 2-12
Mnemonic
Table
specifying Billing Printer Mnemonic 2-6
Mnemonic Name
parameter 2-14
Mnemonic Table Record 3-12
Modified Q Packet 5-6

N

N2 Transmission Tries 2-34
Network address 3-7
Network Restrictions 5-2
Number of Prefix Address Digits
stripped from Outgoing Calls 2-46
Number of Prefix Address Digits stripped from
Incoming Calls 2-46
Number of PVC Channels 2-32
Number of Routing Digits in Call User Data 2-45
Number of Subaddress Digits in X.25 Address 2-47
Number of SVC Channels 2-32

O

OLDA option 2-6
Operator-initiated Test Termination 5-17
Options 3-8
Outbound call translation table
configure 3-5
Outbound Translation Table 2-6

P

Packet Sequence Counting 2-35

P (Continued)

Packet size 2-36
Parameters
Hop Count Facility Code 2-60
PDN 2-6
setting 2-6
Port address 2-6, 2-46
Port Statistics 4-1
examples 4-2
Private Network Address 3-7, 3-18
Private network address
appending a subaddress 3-4
Protection Level 2-48
PVC broadcast output table
configure 3-16
PVC Channels 2-32
range guidelines 2-6

R

Reconnection Tries Limit 2-49
REGI
setting 2-6
REGO
setting 2-6
Remote Connection ID
parameter 2-12
Request/Response Packet Exchange 5-6
Reset Timer 2-38
Restricted Connection Destination 2-46
Route Selection Table 3-12
Routing
best path 2-57
best path algorithm 2-57

S

SIMPv
guidelines 2-6
Starting SVC Channel Number 2-33
Statistics
T1/E1 4-10
Statistics menu
Port Statistics 4-1
SVC channels 2-32, 2-33
range guidelines 2-6
SVC network connections 5-1
System-initiated Termination Test 5-18

T

T1 Transmission Retry Timer 2-33
guidelines 2-6
T1/E1
statistics 4-10
T1/E1 Interface
configuring 2-15
statistics 4-10

T (Continued)

T4 Poll Timer
  guidelines 2-6
Test Termination 5-17
Threshold 2-37
Timer 2-38, 2-39
Traffic Priority 5-1
  delay packet 5-1

W

W Packet Window 2-36
Window 2-35, 2-36
  size guidelines 2-6
Window Settings
  Annex G/X.25 2-56
Window Subtractor Parameter 2-55

X

X.25 D Bit
  data transfer rate 2-63
  modification facility 2-63
  X.25 Port Record 2-63
X.25 options 2-40
  INL and PDN 2-6
X.25 Port Record
  configure 2-5