Vanguard Managed Solutions

Vanguard Applications Ware
Basic Protocols

Bandwidth Management

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Unpublished - rights reserved under the copyright laws of the United States.

Notice (continued)

Proprietary Material

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

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

Part No. T0108, Rev J
Publication Code: DS
First Printing: June 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. Bandwidth Management Features

Chapter 2. Tables and Records Used to Manage Bandwidth

Chapter 3. Bandwidth Management Statistics

Index

About This Manual

Overview

Introduction

This manual covers features you use to manage bandwidth when using Vanguard devices.

Audience

This manual is intended for users of the Vanguard products.

What's in This Manual?

This table describes the information found in this manual.

Title	***Describes***
Chapter 1- Bandwidth Management Features	The functionality of bandwidth management features, including theory of operation, advantages, support, examples, and limitations.
Chapter 2 - Tables and Records Used in Managing Bandwidth	The tables, records, configuration guidelines, and parameters you use to configure Vanguard bandwidth management features. Many of these features share common menus and are, therefore, grouped together.
Chapter 3 - Statistics	Statistics calculated for the bandwidth management features.

Related Documentation

All documentation is provided on the Vanguide CD-ROM and the Vanguard Managed Solutions web site.

Part Number	***Includes:***
T0100	IP and LAN Feature Protocols
T0101	SNA Feature Protocols
T0102	Serial Feature Protocols
T0103	Multi-Service Feature Protocols
T0104	Multimedia Feature Protocols
T0106	Vanguard Applications Ware Basic Protocols

About This Manual (continued)

Vanguide CD-ROM

The Vanguide CD-ROM contains all Vanguard documentation available at the time of release. The Vanguide CD-ROM is shipped with each Vanguard product. To order an additional copy of the Vanguide CD-ROM, please contact your Vanguard Managed Solutions's representative.

Worldwide Web

Check the Vanguard Managed Solutions web site for the latest documentation:

http://www.vanguardms.com/documentation

Chapter 1
Bandwidth Management Features

Overview

Introduction

This manual describes Vanguard features used to manage bandwidth.

What Is Bandwidth Management?

The term *Bandwidth Management* refers to a number of Vanguard features used to efficiently pass various kinds of traffic between nodes. These features operate and interoperate at many levels. For example, using Bandwidth Management features, you can:

- add additional temporary dial lines triggered by congestion and queue states.
- influence the processing of traffic packets themselves.
- monitor specific ports for failure and configure backup routes.
- efficiently route traffic over several paths.
- assign priority to ports.
- assign priority classes and percentage of bandwidth to specific protocols.

Features in this Manual

These features function as part of Bandwidth Management:

Feature	***Reference***	***Description***
Dial SVCs	page 1-7	Provides Dial SVC support for IP traffic over X.25 by activating when there is data to send and deactivating once all the data has been sent. This allows you to send LAN data over an X.25 Public or Private Data Network via an X.25 SVC, and only pay for the time the X.25 WAN connection is actually in use.
Dial on Demand	page 1-8	Allows LAN-to-LAN Remote Access customers to use dial connections to connect PCs on one remote Vanguard-attached LAN to other PCs/Servers on another Vanguard-attached LAN. It also provides On Demand access to all the services available on that LAN, without burdening any Server. Dial on Demand links can also provide a dial up connection between PCs and a front end processor that supports X.25 switched connections using RFC 877.

Feature	***Reference***	***Description** (continued)*
Bandwidth on Demand (BoD)	page 1-14	Allows you to activate additional incremental Wide Area Bandwidth for IP traffic, on a packet-by-packet basis, when congestion thresholds are exceeded on the primary SVC.
Load Balancing	page 1-14	Provides BoD dial functionality activating additional lines when needed by triggering either of these configurable congestion measurement methods: • Queue length: Triggers parallel SVC activation based on LAN Connection queue overflow, provided that SVC is not also congested. • Port utilization: Triggers parallel SVC activation based on actual usage of the port as compared to high and low usage thresholds, link speed, and packet size.
Switched Services Link Backup	page 1-20	Switched Services Link Backup functionality provides backup routing to monitored ports in case these ports fail.
Load Sharing	page 1-25	Lets you route calls destined for a particular node over two links instead of one to reduce congestion and maintain a reasonable throughput level. You can specify up to eight port destinations and priorities for each entry in the Route Selection Table.
Alternate Routing	page 1-26	Enables you to route calls over alternate links when the preferred link is unavailable.
Data Connection Protection	page 1-28	Data Connection Protection (DCP) lets you recover lost data packets and reroute calls around failed network links. All PAD and X.25 ports can use DCP when it is enabled.
Traffic Priority	page 1-31	Allows you to assign a priority class to a user port. Then, the network port protocol stack uses the priority class to determine the order in which user ports transmit data packets for X.25 and Frame Relay Annex G traffic. Besides prioritizing traffic between SVCs, you can assign priority to the various forwarders such as Source Route, Transparent Bridge, IPX, or IP. The WAN Adapter uses these forwarders to determine the order that frames are sent from the WAN Adapter to the network port within a virtual circuit.

Feature	***Reference***	***Description** (continued)*
Time of Week Dial Filtering	page 1-39	Lets you disable an ISDN port's incoming and outgoing dialing for a specified time period. You configure a set of intervals to define the day, time, and duration during which dialing applications cannot access the port. The maximum configurable duration is one week.
Protocol Priority	*Protocol Priority Manual* (Part Number T0100-09)	The Protocol Priority feature provides prioritization of traffic for various protocols so that WAN bandwidth is shared effectively between them. Protocol Priority allows you to classify and service different traffic streams over a WAN link/connection by assigning a priority level and percentage of bandwidth.
Data Compression	*Frame Data Compressor Manual* *(*Part Number T0103-04)	The Frame Data Compressor is a Network Services feature that improves throughput across a WAN link and reduces overall WAN bandwidth usage. When you configure data compression for any virtual circuit between two Vanguard endpoints, frames are compressed prior to transfer and decompressed upon receipt. The Frame Data Compressor operates on the payload portion of each frame. Payload refers to everything excluding the X.25 or Frame Relay header.
Quality of Service	*Quality of Service Manual (Part Number* T0100-10)	Related to Bandwidth Management, Quality of Service is the performance of user/ application traffic through networks intended to provide end-to-end service with respect to service availability, throughput, delay, jitter, and packet loss.

Before You Begin

Before you can configure the parameters described in this chapter, you must log on to the local node's Control Terminal Port. Refer to the *Vanguard Basic Configuration Manual* (Part Number T0113) for more information.

Switched Virtual Circuits (SVCs)

Introduction

Vanguard devices support four types of switched virtual circuits:

- Permanent SVCs
- On Demand SVCs
- Dial on Demand SVCs
- Parallel SVCs (Bandwidth on Demand)

What is an SVC?

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

Permanent SVCs

A Permanent SVC is a LAN Connection SVC that becomes active after it is configured and remains operational until you deactivate it.

On Demand SVCs

On Demand SVCs support IP traffic over X.25 by activating when there is data to send and deactivating once all the data has been sent. This allows you to send LAN data over an X.25 Public or Private Data Network (PDN) via an X.25 SVC, and to pay only for the time the X.25 WAN connection is actually in use.

Dial on Demand (DoD) SVCs

DoD SVCs extend On Demand SVC connection options to support IPX and asynchronous traffic in addition to IP.

Parallel SVCs (Bandwidth on Demand)

Bandwidth on Demand (BoD) provides additional wide area bandwidth for IP traffic. BoD becomes active when traffic exceeds congestion limits on the primary SVC.

Switched Virtual Circuit (SVC) Examples

Typical Applications

This section describes typical SVC applications.

Example 1

This application depicts a network for a large hotel chain. It demonstrates the most common application of RFC877/1356 with On Demand SVCs. An AS/400 that needs to connect to up to 2000 branch sites over an X.25 PDN. All LAN Connections (LCONS) between the AS/400 and Vanguards are RFC877 encapsulated. Dotted lines denote On Demand SVCs. On Demand SVCs are used on a transaction basis where users are billed accordingly. Permanent SVCs are used only where warranted because of other serial traffic needs.

In this network, as shown in Figure 1-1, it is possible to have other LAN connections using VanguardMS proprietary encapsulations between branch sites using Vanguard Routers.

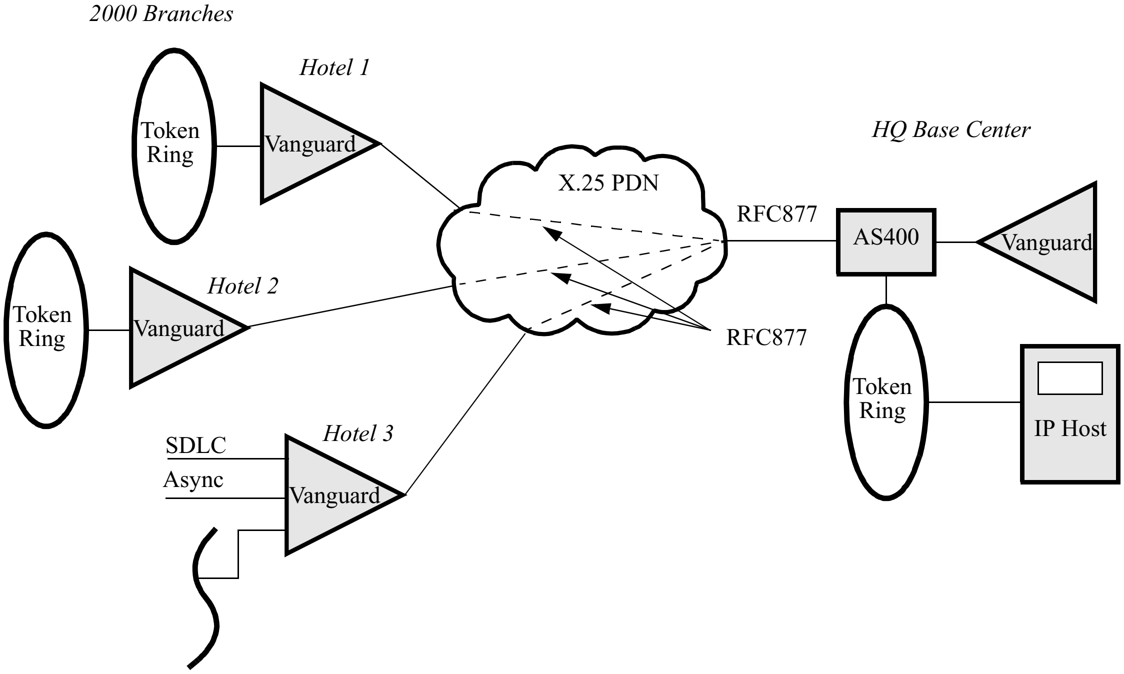


Figure 1-1. On Demand SVCs in an X.25 PDN Using RFC877

Example 2

This example, shown in Figure 1-2, is a network for a package shipping company using an X.25 PDN network, RFC877/1356 encapsulation, and On Demand SVCs. The headquarters has another network that must connect to as many as to 1200 branch sites.

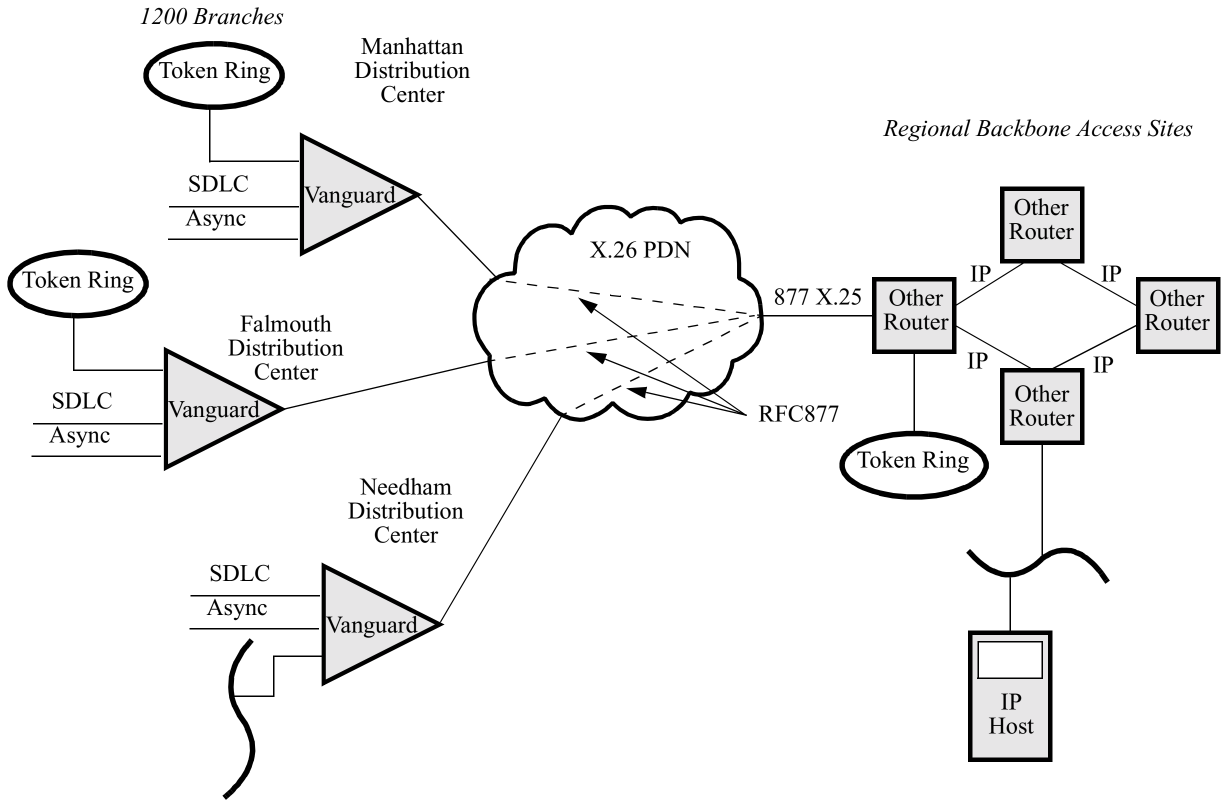


Figure 1-2. On Demand SVCs in an X.25 PDN Using RFC877

On Demand SVCs

Introduction

On Demand SVCs support IP traffic over X.25 by activating when there is data to send and deactivating once all the data has been sent. This allows you to send LAN data over an X.25 Public or Private Data Network via an X.25 SVC, and pay only for the actual X.25 WAN connection usage.

Activating an On Demand SVC

An On Demand SVC stays inactive until there is IP data to send over that WAN link. Data on the local node triggers the need to establish the SVC or an incoming call request from a remote node to establish the SVC activates the SVC. The SVC stays active as long as there is IP data remaining to be sent. Once the data is sent, the SVC is deactivated. The SVC remains inactive until this process is repeated.

Activation and Deactivation

The criteria for activating and deactivating On Demand SVCs are:

- All LCONs configured for RFC 877 encapsulation are On Demand by default.
- LCONs configured for Codex Proprietary encapsulation can be On Demand or Permanent and are created during initialization.

If an initial call request fails either because of a collision or a clear message received from the remote node, the Vanguard device attempts to bring the call up for the configured maximum number of retries. Upon completion of retries, the data queues are flushed and call establishment stops.

If the Vanguard device goes into a congestion state while waiting for the SVC to come up (is flooded by the local IP forwarder), it executes the congestion handling algorithm as it does on Permanent SVCs. Once the congestion clears, the Vanguard returns to its normal steady state operation.

Configuration Considerations

These configuration considerations apply to On Demand SVCs:

- The LAN Forwarder Type should be configured for static routing when using On Demand SVCs.
- RIP advertisements should be disabled for a ROUT LCON configured as On Demand. Otherwise, RIP advertisements activate and deactivate the SVCs every 60 seconds, thus defeating the On Demand functionality. Router Interfaces at both ends of this link should have Static Routes configured.

Making Dial SVCs Appear Permanent

Router-type LAN Connections in RFC 877 encapsulation format use On Demand SVCs by default. SVCs that are On Demand by default have a configurable Idle Timer parameter that specifies a period of inactivity after which the SVC becomes inactive. In the On Demand-Idle Out mode, the SVC activates and deactivates as stated in the preceding Activation and Deactivation section. By entering a zero Idle Timer entry, the On Demand SVC functions in non-Idle Out mode. The SVC activates the same way, but when there is no more data to be sent, the link remains active because of the zero Idle Timer entry and functions as a Permanent SVC.

Dial on Demand SVCs

Introduction

Dial on Demand SVCs are an extension to On Demand SVC functionality. Dial on Demand SVCs extend Vanguard WAN connectivity options to support IPX and asynchronous traffic in addition to IP. This occurs over switched networks using:

- PSTN modems
- ISDN links
- Switched 56 lines

Dial on Demand links can also provide a dial up connection between PCs and a front end processor that supports X.25 switched connections using RFC 877.

Features

Dial on Demand SVCs offer these features:

- Ability to initiate or receive Dial calls from other Vanguard devices.
- Serial port access call activation (SLIP, RFC 877 or 1490).
- Ability to configure routes to optimize Dial link cost in a mixed Lease and Switched network.

Dial on Demand Uses

Dial on Demand links are useful in situations like these:

- You need access to, or from, branches as soon as possible and are awaiting leased connections to be set up by the carrier. Dialed connections are available much faster at most remote sites.
- You want to mix in asynchronous traffic at the remote office site to gain access to a terminal server or front end processor at another site.
- You want to install a Brouter/Router network, using permanent connections (leased line, Frame Relay, or X.25), but a portion of your networking traffic does not warrant the expense of a permanent connection.

■ **Note**

Generally, depending on the tariff for dialed versus leased connections, two to eight hours of dial connection usage is the breakeven point compared with leased line tariff.

Advantages

These advantages apply to the Dial on Demand feature:

- Dial on Demand SVCs allow LAN-to-LAN Remote Access users to use dial connections when connecting PCs on a remote Vanguard-attached LAN to other PCs/Servers on another Vanguard-attached LAN. This allows access to the services available on the other LAN, in an “On Demand” fashion, without burdening any server.
- Dial on Demand SVCs activate a dial link prior to establishing the SVC; the On Demand SVCs do not.

Platform Support

The Dial on Demand feature is supported for all Vanguard products.

Configuration Considerations

These configuration considerations apply to the Dial on Demand feature:

- Avoid configuring Serial protocols over dial links. This results in the Dial link being activated to send overhead information over the WAN.
- External modems only are supported. You cannot use the Integral Service modem as a Dial on Demand port.

Support

Dial on Demand SVCs support:

- IPX and Asynchronous traffic, in addition to IP.
- X.25 switched networks using:
  - External PSTN dial modem.
  - An ISDN terminal adapter.
  - Switched-56 device.

DoD SVC Examples

Example

Figure 1-3, when PC1, which is attached to a Vanguard router through LAN1, needs access to information on Server1, connected to LAN 2, over a modem dial link, the Vanguard device activates a dial connection using either DTR or V.25 bis signalling. After the session has ended, the call is terminated.

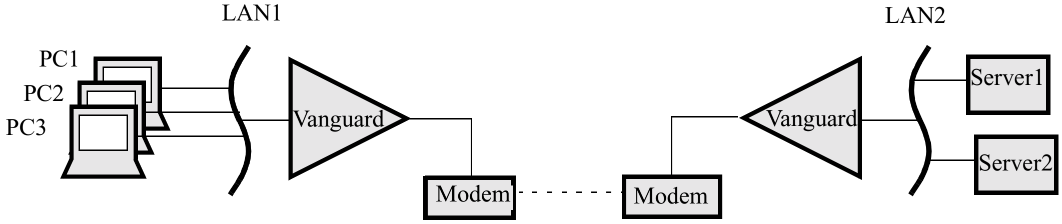


Figure 1-3. Dial on Demand Connection

Typical DoD Application

The application shown in Figure 1-4 is a typical example of Dial On Demand. A LAN Connection is required for the Dial on Demand SVC. Note that the dial port can be part of the same LANView as another network port. The DoD link is configured for use when Node D needs to access Network 10.0.0.0.

When Node D receives a packet destined to network 10.0.0.0 from Node C, whose next hop (or interface address) is configured as 12.0.0.3, Node D activates a dial connection and data is transferred.

■Note

In this example, you must configure the dial port for nodes D and C using BKUP in the X.25 Option parameter and DIMOv for the Connection type. You must also configure the Switched Services Table. A sample configuration for this application appears in the next section.

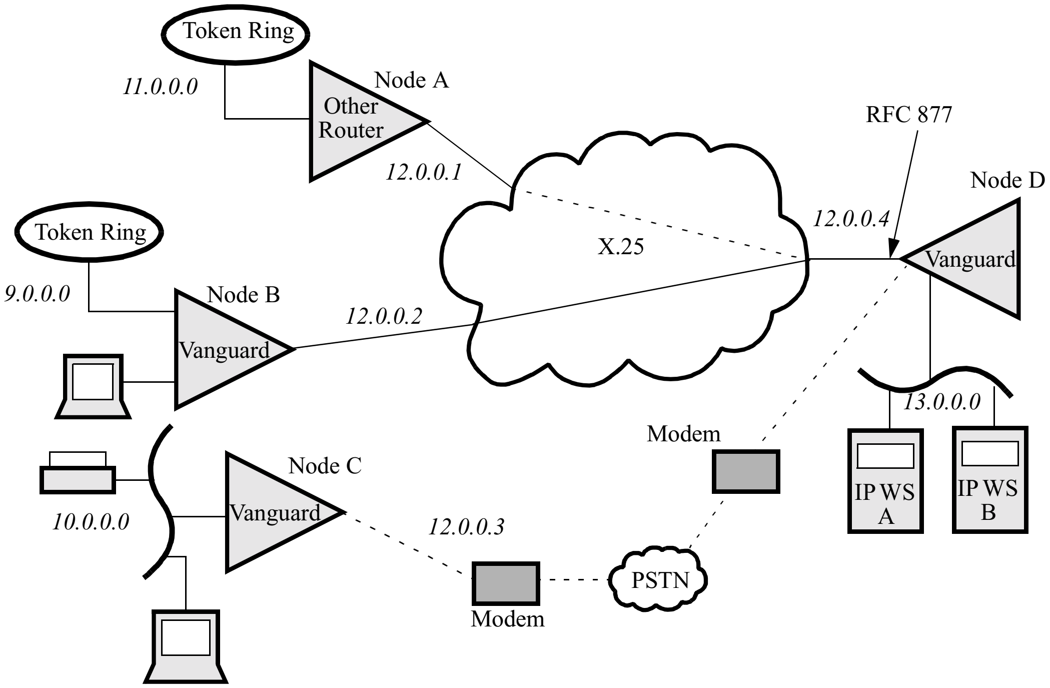


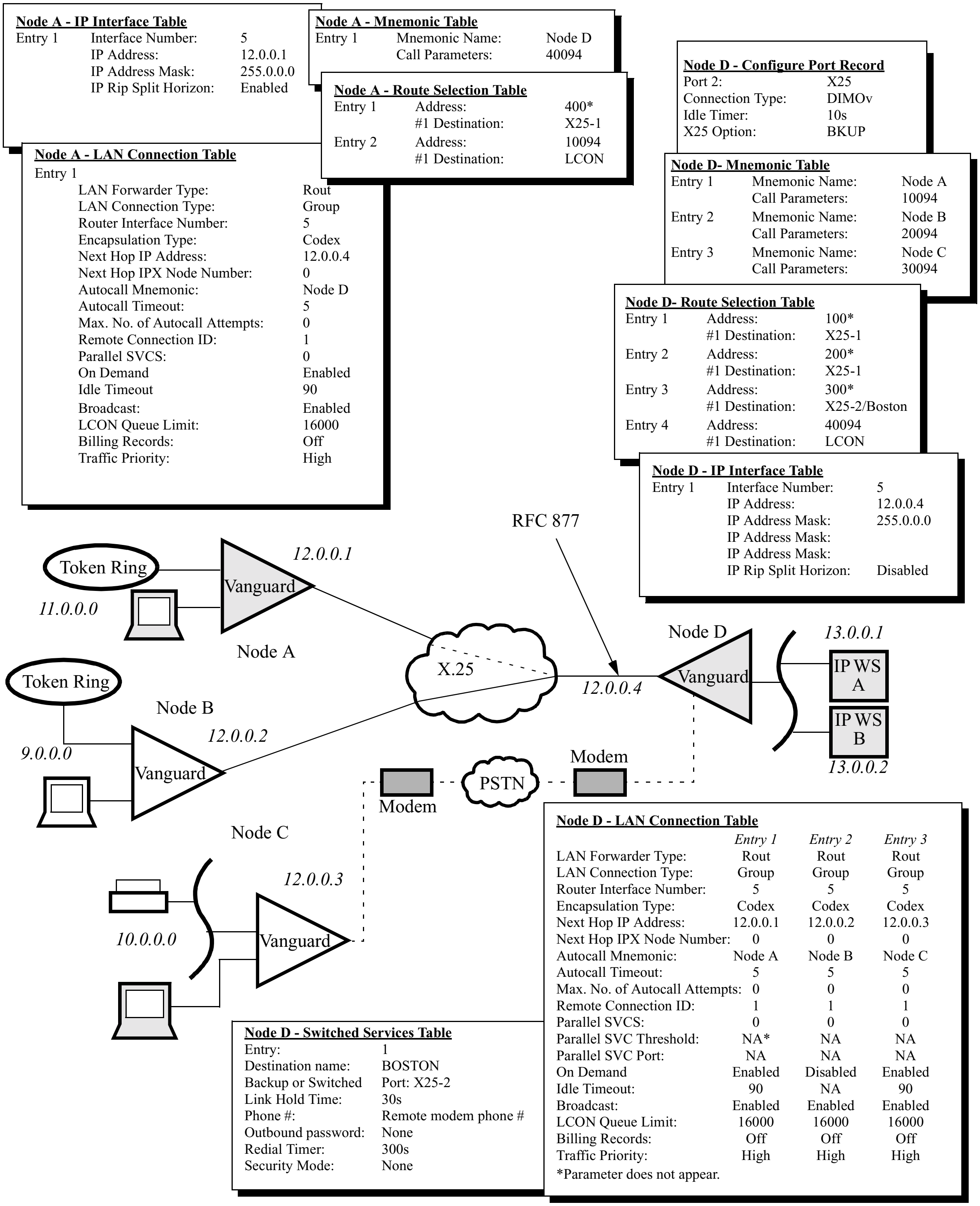
Figure 1-4. Sample Dial on Demand Connection

Typical DoD Configuration

Figures 1-5 and 1-6 depict configuration of the DoD application example described below. Figure 1-5 shows configuration of Nodes A and D (shaded gray). Figure 1-6 shows configuration of Nodes B and C (shaded gray).

The following application shows a typical example of DoD. A LAN Connection is required for the DoD SVC. Note that the dial port can be part of the same LANView as another network port. The DoD link is configured to be used when Node D needs to access Network 10.0.1.0.

When Node D receives a packet destined to network 10.0.1.0 off Node C, whose next hop (or interface address) is configured as 12.0.0.3, Node D activates a dial connection and data is transferred.



Node A - IP Interface Table

Entry 1	Interface Number:	5
	IP Address:	12.0.0.1
	IP Address Mask:	255.0.0.0
	IP Rip Split Horizon:	Enabled

Node A - Mnemonic Table

Entry 1	Mnemonic Name:	Node D
	Call Parameters:	40094

Node A - Route Selection Table

Entry 1	Address:	400*
	#1 Destination:	X25-1
Entry 2	Address:	10094
	#1 Destination:	LCON

Node A - LAN Connection Table

Entry 1	
LAN Forwarder Type:	Rout
LAN Connection Type:	Group
Router Interface Number:	5
Encapsulation Type:	Codex
Next Hop IP Address:	12.0.0.4
Next Hop IPX Node Number:	0
Autocall Mnemonic:	Node D
Autocall Timeout:	5
Max. No. of Autocall Attempts:	0
Remote Connection ID:	1
Parallel SVCS:	0
On Demand	Enabled
Idle Timeout	90
Broadcast:	Enabled
LCON Queue Limit:	16000
Billing Records:	Off
Traffic Priority:	High

Node D - Configure Port Record

Port 2:	X25
Connection Type:	DIMOv
Idle Timer:	10s
X25 Option:	BKUP

Node D- Mnemonic Table

Entry 1	Mnemonic Name:	Node A
	Call Parameters:	10094
Entry 2	Mnemonic Name:	Node B
	Call Parameters:	20094
Entry 3	Mnemonic Name:	Node C
	Call Parameters:	30094

Node D- Route Selection Table

Entry 1	Address:	100*
	#1 Destination:	X25-1
Entry 2	Address:	200*
	#1 Destination:	X25-1
Entry 3	Address:	300*
	#1 Destination:	X25-2/Boston
Entry 4	Address:	40094
	#1 Destination:	LCON

Node D - IP Interface Table

Entry 1	Interface Number:	5
	IP Address:	12.0.0.4
	IP Address Mask:	255.0.0.0
	IP Address Mask:	
	IP Address Mask:	
	IP Rip Split Horizon:	Disabled

Node D - Switched Services Table

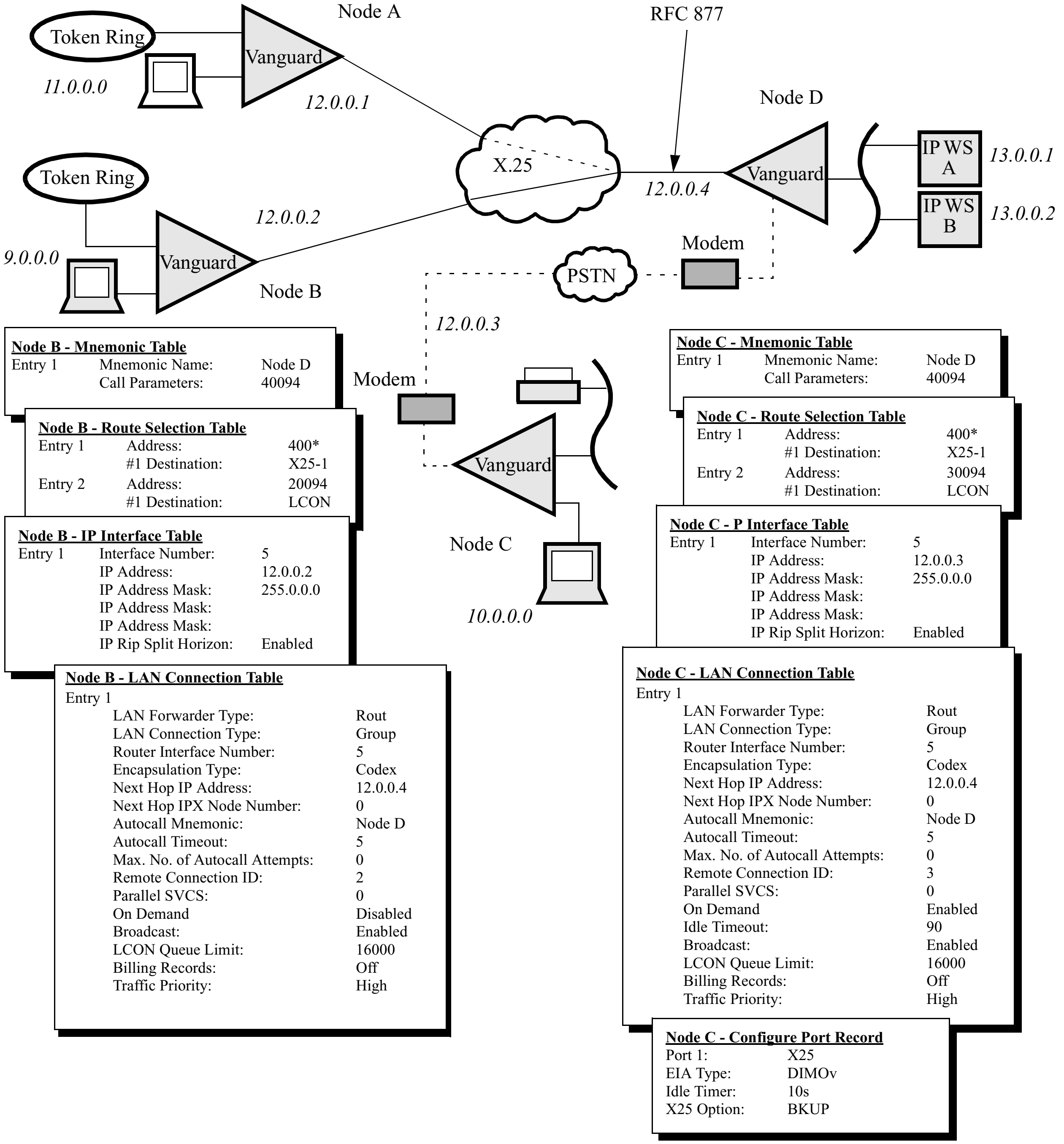
Entry:	1
Destination name:	BOSTON
Backup or Switched	Port: X25-2
Link Hold Time:	30s
Phone #:	Remote modem phone #
Outbound password:	None
Redial Timer:	300s
Security Mode:	None

Node D - LAN Connection Table

	Entry 1	*Entry 2*	*Entry 3*
LAN Forwarder Type:	Rout	Rout	Rout
LAN Connection Type:	Group	Group	Group
Router Interface Number:	5	5	5
Encapsulation Type:	Codex	Codex	Codex
Next Hop IP Address:	12.0.0.1	12.0.0.2	12.0.0.3
Next Hop IPX Node Number:	0	0	0
Autocall Mnemonic:	Node A	Node B	Node C
Autocall Timeout:	5	5	5
Max. No. of Autocall Attempts:	0	0	0
Remote Connection ID:	1	1	1
Parallel SVCS:	0	0	0
Parallel SVC Threshold:	NA*	NA	NA
Parallel SVC Port:	NA	NA	NA
On Demand	Enabled	Disabled	Enabled
Idle Timeout:	90	NA	90
Broadcast:	Enabled	Enabled	Enabled
LCON Queue Limit:	16000	16000	16000
Billing Records:	Off	Off	Off
Traffic Priority:	High	High	High

*Parameter does not appear.

Figure 1-5. Dial on Demand Configuration (Nodes A and D)



Node B - Mnemonic Table

Entry 1	Mnemonic Name:	Node D
	Call Parameters:	40094

Node B - Route Selection Table

Entry 1	Address:	400*
	#1 Destination:	X25-1
Entry 2	Address:	20094
	#1 Destination:	LCON

Node B - IP Interface Table

Entry 1	Interface Number:	5
	IP Address:	12.0.0.2
	IP Address Mask:	255.0.0.0
	IP Address Mask:	
	IP Address Mask:	
	IP Rip Split Horizon:	Enabled

Node B - LAN Connection Table

Entry 1

LAN Forwarder Type:	Rout
LAN Connection Type:	Group
Router Interface Number:	5
Encapsulation Type:	Codex
Next Hop IP Address:	12.0.0.4
Next Hop IPX Node Number:	0
Autocall Mnemonic:	Node D
Autocall Timeout:	5
Max. No. of Autocall Attempts:	0
Remote Connection ID:	2
Parallel SVCS:	0
On Demand	Disabled
Broadcast:	Enabled
LCON Queue Limit:	16000
Billing Records:	Off
Traffic Priority:	High

Node C - Mnemonic Table

Entry 1	Mnemonic Name:	Node D
	Call Parameters:	40094

Node C - Route Selection Table

Entry 1	Address:	400*
	#1 Destination:	X25-1
Entry 2	Address:	30094
	#1 Destination:	LCON

Node C - P Interface Table

Entry 1	Interface Number:	5
	IP Address:	12.0.0.3
	IP Address Mask:	255.0.0.0
	IP Address Mask:	
	IP Address Mask:	
	IP Rip Split Horizon:	Enabled

Node C - LAN Connection Table

Entry 1

LAN Forwarder Type:	Rout
LAN Connection Type:	Group
Router Interface Number:	5
Encapsulation Type:	Codex
Next Hop IP Address:	12.0.0.4
Next Hop IPX Node Number:	0
Autocall Mnemonic:	Node D
Autocall Timeout:	5
Max. No. of Autocall Attempts:	0
Remote Connection ID:	3
Parallel SVCS:	0
On Demand	Enabled
Idle Timeout:	90
Broadcast:	Enabled
LCON Queue Limit:	16000
Billing Records:	Off
Traffic Priority:	High

Node C - Configure Port Record

Port 1:	X25
EIA Type:	DIMOv
Idle Timer:	10s
X25 Option:	BKUP

Figure 1-6. Dial on Demand Configuration (Nodes B and C)

Link Address Negotiation for Dial On Demand

Introduction

This section describes the Link Address Negotiation enhancement to the Dial On Demand feature.

What Is It?

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

How It Works

As shown in Figure 1-7, 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 Set Asynchronous Balanced Mode messages (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 occur 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 1-7 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.

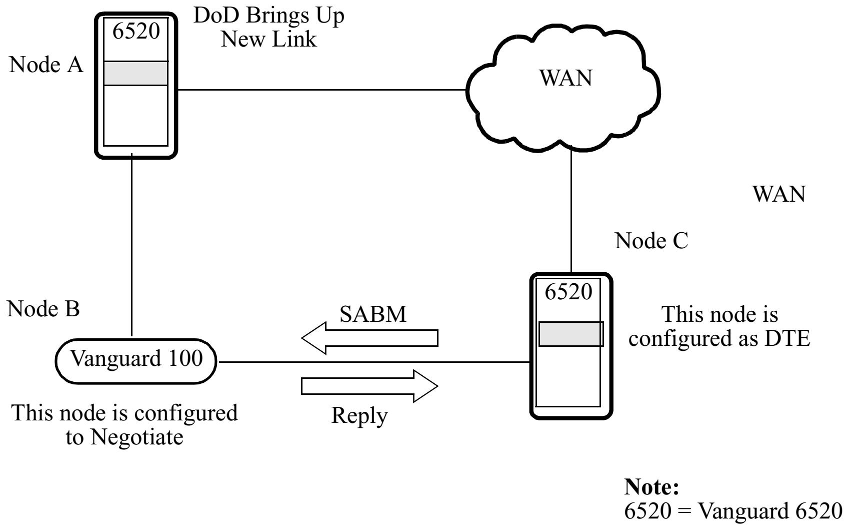


Figure 1-7. How DoD Negotiate Feature Works

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.

Bandwidth on Demand and IP Load Balancing

What Is Bandwidth on Demand?

Bandwidth on Demand (BoD) refers to the ability to activate additional incremental Wide Area Bandwidth for IP traffic, on a packet-by-packet basis, when congestion thresholds are exceeded on the primary SVC. This incremental bandwidth can be:

- Additional X.25 SVCs on the same or a different physical port.
- An external dial modem, ISDN-terminal adapter or Switched-56 device connected to a different physical port.

A parallel SVC is an LCON configured as attached to the same router interface as a primary SVC in the local router and the same next hop address as the primary SVC in the remote router.

How BoD Works

When a configured threshold of congestion is reached on a primary SVC, a BoD or *parallel* SVC can be activated. Vanguard nodes queue up and transmit packets over the parallel SVC, until congestion ceases on the primary link. Once congestion on the primary link ceases, packets queued to the parallel SVC are redirected to the primary SVC.

If parallel SVCs stay idle for longer than the configured idle time, they are terminated.

Example

You can use BoD to activate a secondary link when a primary link is congested. In the example shown in Figure 1-8, the ISDN link provides the on demand connection.

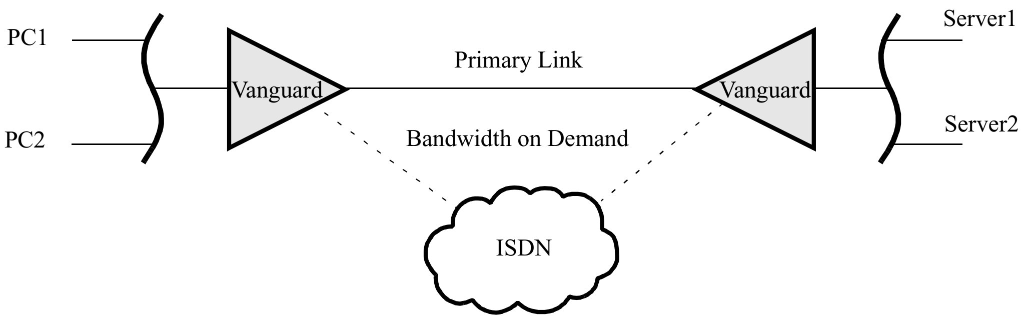


Figure 1-8. Bandwidth on Demand Connection

What Is IP Load Balancing?

BoD functionality can be triggered by either of two configurable congestion measurement methods:

- *Queue length*: Triggers parallel SVC activation based on LAN Connection queue overflow, provided that SVC is not also congested.
- *Port utilization*: Triggers parallel SVC activation based on actual usage of the port as compared to high and low usage thresholds, link speed, and packet size.

Queue length and port congestion are explained further next:

Queue Length (THRESHOLD value)

With congestion based on the queue overflow scheme, the LCON tries to keep the primary link full. Overflow of the primary link triggers activation of a secondary link, usually with higher speed. Once the overflow condition subsides, the secondary link deactivates and all traffic switches back immediately to the primary link. This can result in oscillation: The secondary link bounces between activation and deactivation rapidly, attempting to keep the primary link filled while keeping the secondary active only as long as necessary.

Port Utilization (PORT_CONGEST value)

You can also activate and deactivate BoD parallel SVCs based on port utilization. In this scheme, additional bandwidth is brought up when utilization on the primary link crosses a configured threshold. Congestion status on the primary link is constantly monitored and compared to factors such as link speed, number of packets, and number of bytes of the receiving packet to activate and deactivate the secondary link more gradually. Once two links are in use, IP traffic is “load balanced” over the two SVCs. In balancing IP traffic, other contributing traffic, such as serial protocols, is taken into account so that it is not choked by the IP traffic, and vice versa.

■ **Note**

> You can find these settings in the Parallel SVC Trigger Mechanism parameter in the LAN Connection Table parameters in the Configure menu. See the “LAN Connection Table Parameters” section in Chapter 2.

Advantages

BoD is useful when you have an average need for 56/64K line speeds, but you have occasional peak time periods where you must double or triple available bandwidth to improve response time.

If you occasionally require more than 56/64K throughput, you pay only for the connection time used by the temporary second link.

Features

BoD functionality offers:

- Congestion-activated, additional, incremental Wide Area Bandwidth for IP.

  This can be:

  - Additional X.25 SVCs on a different physical port than the primary link.
  - An external dial modem, ISDN-terminal adapter, or SW-56 device connected to a different physical port than the primary link.

■ **Note**

> An additional X.25 SVC can be activated on the same port as the primary link if you are measuring congestion using the queue length threshold method instead of port utilization method.

Call Establishment Process

Criteria for activating a parallel SVC is congestion based, as measured by queue length (the number of data bytes either queued, or transmitted and awaiting acknowledgment) or port utilization (WAN port congestion, detected, and signalled by the networking port). First, the Vanguard tries to transfer new packets over the primary SVC. If the LCON queue of the primary SVC exceeds the configured congestion threshold, the data is queued to go over a parallel SVC. All new packets get queued to the parallel SVC(s) until the congestion threshold goes below the configured level on the primary SVC.

When congestion is based on queue length, up to three parallel SVCs to the same next hop destination can be defined in addition to the primary SVC to that destination. With congestion based on port utilization, only one parallel SVC is possible.

After congestion has gone below the threshold on the primary SVC, one of the following occurs:

- *Queue Length Congestion*: All new packets are queued to go over the primary SVC immediately, with the parallel SVC being deactivated. The parallel SVC is allowed to idle out based on the Idle Timeout configuration in the LAN Connection. If the primary SVC has its Idle Timeout configured for either zero or greater than 90 seconds, the parallel SVC times out after 90 seconds.
- *Port Utilization Congestion*: New packets are balanced between the two links to gradually off-load the second SVC based on your Network Services BoD Table parameter configuration. This prevents oscillation between one and two links if, for example, your traffic is bursty in nature.

Traffic Priority

Congestion handling is supported at the individual SVC level and *not* at the Group level. If one of the SVCs of a LAN Connection Group is congested, other SVCs within the LAN Connection Group are uneffected. Refer to Traffic Priority on page 1-31 for more information.

■Note

The priority of a parallel SVC is always the same as the primary SVC.

BoD Examples

Typical BoD Application

Figure 1-9 shows a typical example of BoD via parallel SVCs.

Here, when the primary On Demand link between Node C and Node D is congested, Node D brings up a parallel SVC (BOLD dashed) to Node C, connected to the same Router Interface. When the congestion clears, traffic stops using the parallel SVC and is redirected to the primary SVC. The Parallel SVC then idles out and deactivates.

A parallel SVC can be configured to go over the same network port as the primary SVC or over another network port. This can be either a leased or dial line. With a dial line, you must configure the dial port and the Switched Services Table.

This feature works between Vanguard routers or between any RFC877-compliant router and a Vanguard router (except for dial port operation, which works only between Vanguard routers).

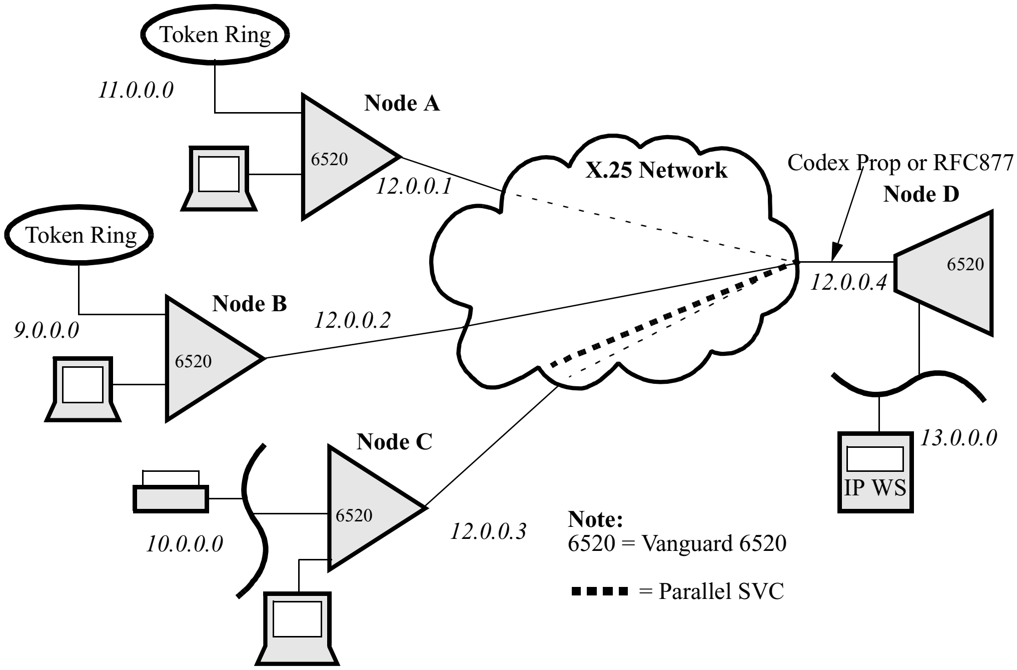


Figure 1-9. Bandwidth on Demand Connection

Typical BoD Configuration

Figures 1-10 and 1-11 depict configuration of the BoD application example described below. Figure 1-10 shows configuration of Nodes A and D (shaded gray). Figure 1-11 shows configuration of Nodes B and C (shaded gray).

This is a typical example of using BoD parallel SVCs.

Here, when the primary On Demand Link between Node C and Node D is congested, Node D brings up a parallel SVC (BOLD dashed) to Node C, connected to the same Router Interface. When the congestion clears, traffic stops using the parallel SVC, which then idles out and deactivates.

A parallel SVC can be configured to go over the same network port as the main SVC, or over another network port. This can be either a leased or dial line.

This feature works between Vanguard routers or between any RFC877-compliant router and a Vanguard router (except for Dial port operation, which works only between Vanguard routers).

Node A - IP Interface Table

Entry 1	Interface Number:	5
	IP Address:	12.0.0.1
	IP Address Mask:	255.0.0.0
	IP Address Mask:	
	IP Address Mask:	
	IP Rip Split Horizon:	Enabled

Node A - Mnemonic Table

Entry 1	Mnemonic Name:	Node D
	Call Parameters:	40094

Node A - Route Selection Table

Entry 1	Address:	400*
	#1 Destination:	X25-1
Entry 2	Address:	10094
	#1 Destination:	LCON

Node A - LAN Connection Table

Entry 1

LAN Forwarder Type:	Rout
LAN Connection Type:	Group
Router Interface Number:	5
Encapsulation Type:	Codex
Next Hop IP Address:	12.0.0.4
Next Hop IPX Node Number:	0
Autocall Mnemonic:	Node D
Autocall Timeout:	5
Max. No. of Autocall Attempts:	0
Remote Connection ID:	1
Parallel SVCS:	0
On Demand	Enabled
Idle Timeout	90
Broadcast:	Enabled
LCON Queue Limit:	16000
Billing Records:	Off
Traffic Priority:	High

Node D- Mnemonic Table

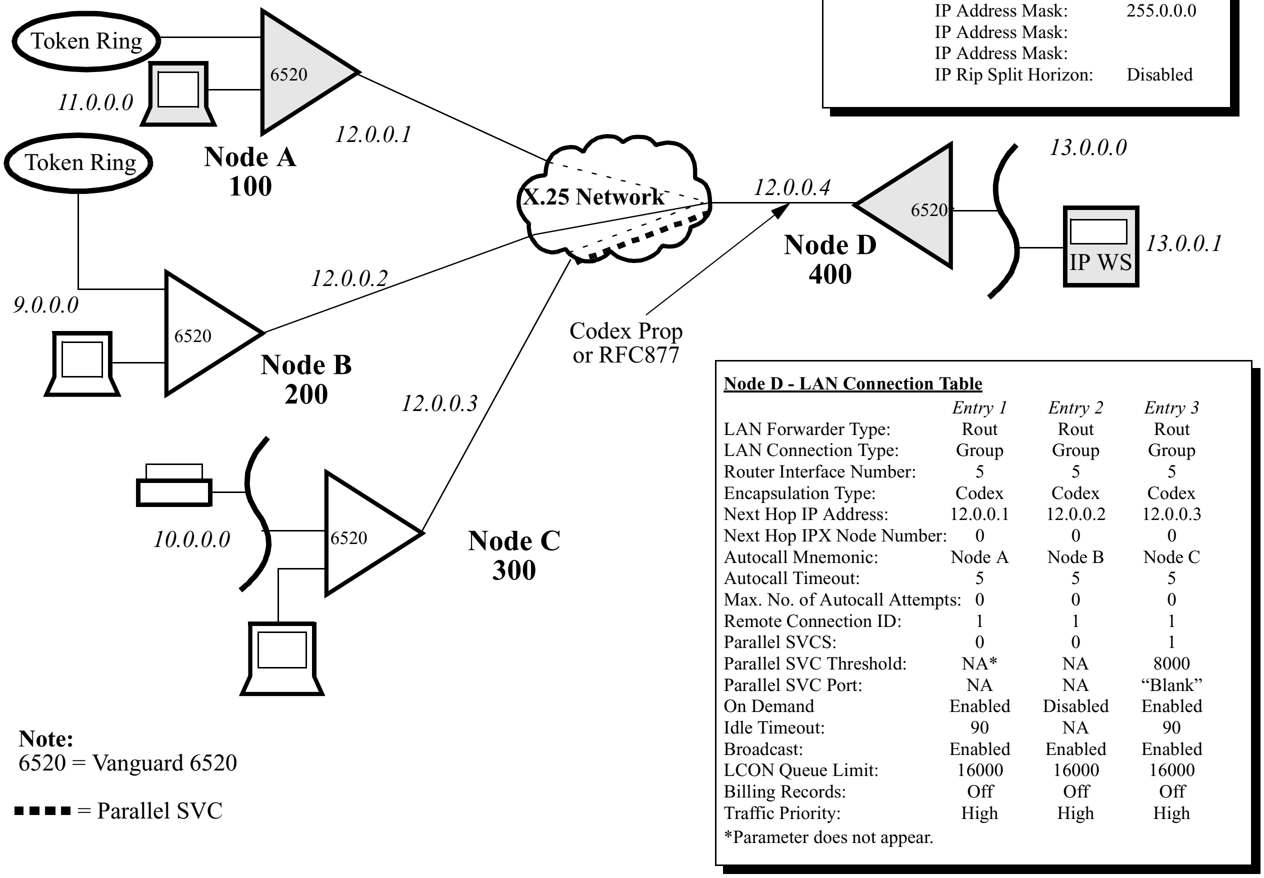
Entry 1	Mnemonic Name:	Node A
	Call Parameters:	10094
Entry 2	Mnemonic Name:	Node B
	Call Parameters:	20094
Entry 3	Mnemonic Name:	Node C
	Call Parameters:	30094

Node D- Route Selection Table

Entry 1	Address:	100*
	#1 Destination:	X25-1
Entry 2	Address:	200*
	#1 Destination:	X25-1
Entry 3	Address:	300*
	#1 Destination:	X25-1
Entry 4	Address:	40094
	#1 Destination:	LCON

Node D - IP Interface Table

Entry 1	Interface Number:	5
	IP Address:	12.0.0.4
	IP Address Mask:	255.0.0.0
	IP Address Mask:	
	IP Address Mask:	
	IP Rip Split Horizon:	Disabled



Note:
6520 = Vanguard 6520

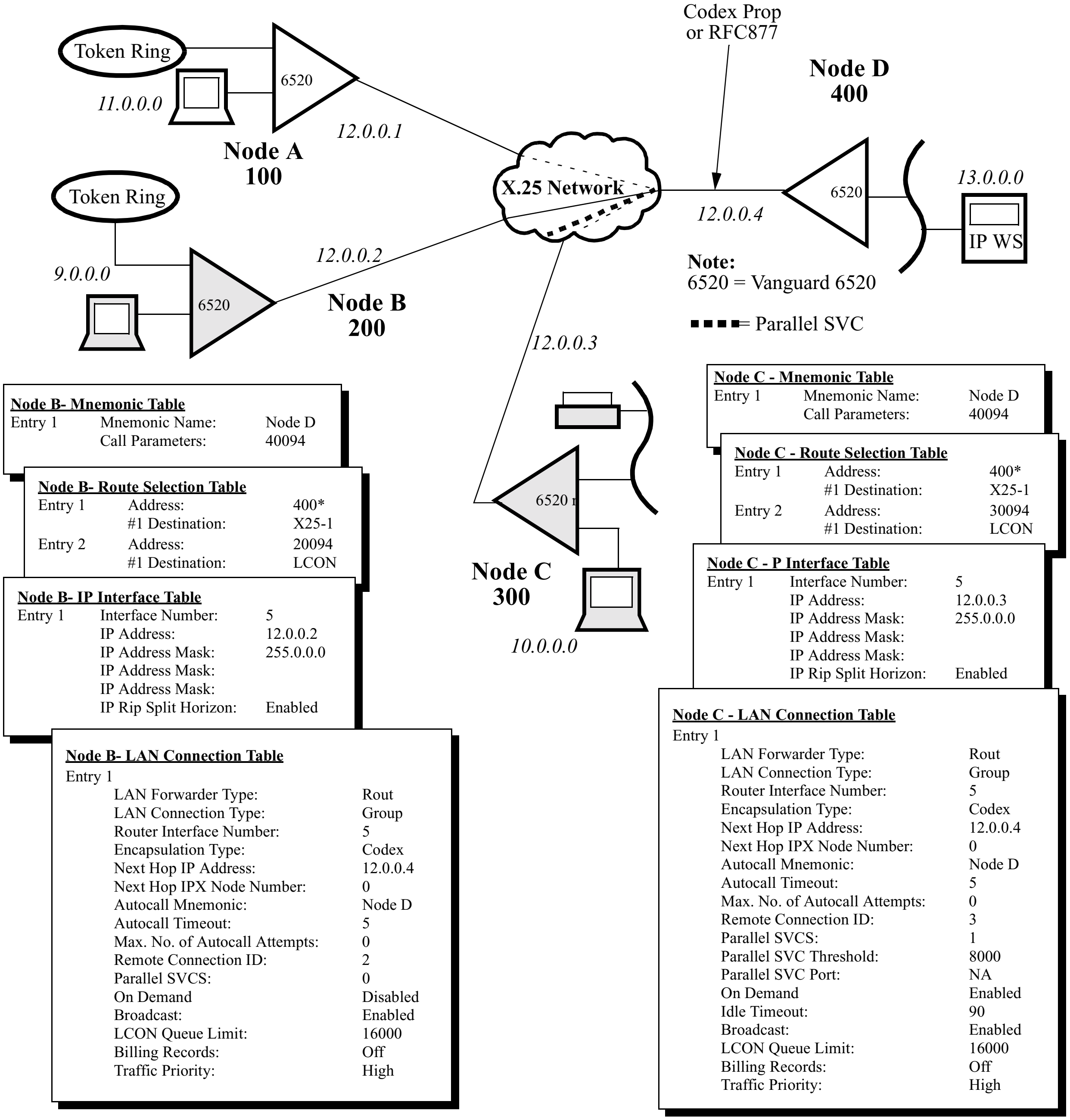
■■■■ = Parallel SVC

Node D - LAN Connection Table

	Entry 1	*Entry 2*	*Entry 3*
LAN Forwarder Type:	Rout	Rout	Rout
LAN Connection Type:	Group	Group	Group
Router Interface Number:	5	5	5
Encapsulation Type:	Codex	Codex	Codex
Next Hop IP Address:	12.0.0.1	12.0.0.2	12.0.0.3
Next Hop IPX Node Number:	0	0	0
Autocall Mnemonic:	Node A	Node B	Node C
Autocall Timeout:	5	5	5
Max. No. of Autocall Attempts:	0	0	0
Remote Connection ID:	1	1	1
Parallel SVCS:	0	0	1
Parallel SVC Threshold:	NA*	NA	8000
Parallel SVC Port:	NA	NA	“Blank”
On Demand	Enabled	Disabled	Enabled
Idle Timeout:	90	NA	90
Broadcast:	Enabled	Enabled	Enabled
LCON Queue Limit:	16000	16000	16000
Billing Records:	Off	Off	Off
Traffic Priority:	High	High	High

*Parameter does not appear.

Figure 1-10. Parallel SVC Configuration Example (Nodes A and D)



Node B- Mnemonic Table

Entry 1	Mnemonic Name:	Node D
	Call Parameters:	40094

Node B- Route Selection Table

Entry 1	Address:	400*
	#1 Destination:	X25-1
Entry 2	Address:	20094
	#1 Destination:	LCON

Node B- IP Interface Table

Entry 1	Interface Number:	5
	IP Address:	12.0.0.2
	IP Address Mask:	255.0.0.0
	IP Address Mask:	
	IP Address Mask:	
	IP Rip Split Horizon:	Enabled

Node B- LAN Connection Table

Entry 1

LAN Forwarder Type:	Rout
LAN Connection Type:	Group
Router Interface Number:	5
Encapsulation Type:	Codex
Next Hop IP Address:	12.0.0.4
Next Hop IPX Node Number:	0
Autocall Mnemonic:	Node D
Autocall Timeout:	5
Max. No. of Autocall Attempts:	0
Remote Connection ID:	2
Parallel SVCS:	0
On Demand	Disabled
Broadcast:	Enabled
LCON Queue Limit:	16000
Billing Records:	Off
Traffic Priority:	High

Node C - Mnemonic Table

Entry 1	Mnemonic Name:	Node D
	Call Parameters:	40094

Node C - Route Selection Table

Entry 1	Address:	400*
	#1 Destination:	X25-1
Entry 2	Address:	30094
	#1 Destination:	LCON

Node C - P Interface Table

Entry 1	Interface Number:	5
	IP Address:	12.0.0.3
	IP Address Mask:	255.0.0.0
	IP Address Mask:	
	IP Address Mask:	
	IP Rip Split Horizon:	Enabled

Node C - LAN Connection Table

Entry 1

LAN Forwarder Type:	Rout
LAN Connection Type:	Group
Router Interface Number:	5
Encapsulation Type:	Codex
Next Hop IP Address:	12.0.0.4
Next Hop IPX Node Number:	0
Autocall Mnemonic:	Node D
Autocall Timeout:	5
Max. No. of Autocall Attempts:	0
Remote Connection ID:	3
Parallel SVCS:	1
Parallel SVC Threshold:	8000
Parallel SVC Port:	NA
On Demand	Enabled
Idle Timeout:	90
Broadcast:	Enabled
LCON Queue Limit:	16000
Billing Records:	Off
Traffic Priority:	High

Figure 1-11. Parallel SVC Configuration Example (Nodes B and C)

Switched Services Link Backup

Introduction

The Switched Services Link Backup feature lets you configure ports as backup (or standby) ports in case monitored ports are unexpectedly terminated. The backup port only takes over once all the monitor ports are terminated. A backup port can be one of the following:

- X.25 port - Uses a dial modem to dial a remote port so that communications can continue with minimum disruption.
- ISDN B channel - Uses a high-bandwidth switched connection to a remote ISDN B channel so that communications can continue with a minimum of disruption.

Switched Services Link Backup monitors the following port types:

- X.25 port
- ISDN D channel
- Frame Relay Annex G station

■ **Note**

Do not confuse Link Backup with the parameter X.25 Option=BKUP. These are separate features, though they work together.

Modems With Blacklist Function

Modems that contain a Blacklist function may interfere with the Switched Service Link Backup redial feature. After five reconnection attempts within an hour, the telephone number is placed on the modem’s Blacklist and cannot be dialed for one hour. Because Vanguard products continue to redial every five minutes, the number is never removed from the Blacklist.

Link Backup Examples

Simple Network

Figure 1-12 describes a simple network where Nodes A and B normally communicate over X.25 Port 1. The system administrator has configured the Switched Services Table Record to monitor Port 1 in Node A. If Port 1 is terminated, Link Backup automatically activates Port 2 to call the dial modem connected to Node B. The X.25 calls on Port 1 are disrupted and cleared. New X.25 calls destined for Port 1 are directed to the backup port and communications between the two nodes can be reestablished.

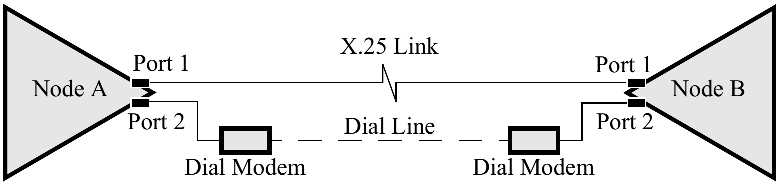


Figure 1-12. LBU Example: X.25 and Dial Modems

Figure 1-13 shows the same example for a node that is operating over a dedicated Frame Relay Annex G connection to the rest of the network. If the link fails, the node dials an alternative connection and directs a B channel towards a preconfigured destination over the ISDN interface.

■ **Note**

Link Backup does not check to ensure that the attributes at both ends of the connection are compatible. It does not incorporate procedures indicated by X.32, which may be required by some PDNs.

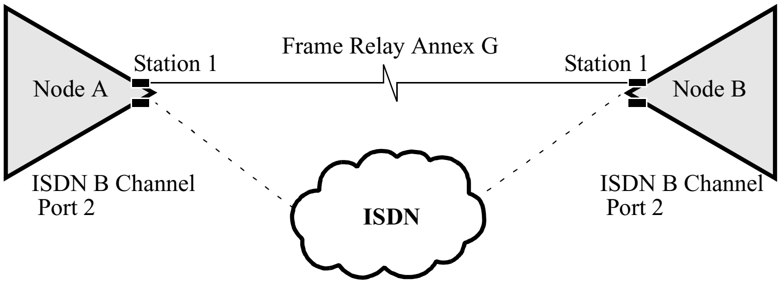


Figure 1-13. LBU Example: Frame Relay Annex G and ISDN B Channels

Link Backup in Point-to-Point Network

In a point-to-point network (see Figure 1-14) Link Backup is a straightforward process. It becomes increasingly complex in larger networks, when one Backup or Switched Services Port is used to back up multiple leased lines destined to different nodes.

Multiple Nodes

Figure 1-14 shows a network in which Node A has two monitored ports (Port 1 and Port 2) and one Backup or Switched Services Port (Port 3). Two Switched Service Table entries are configured so that Port 3 is activated if either of the monitored ports fails.

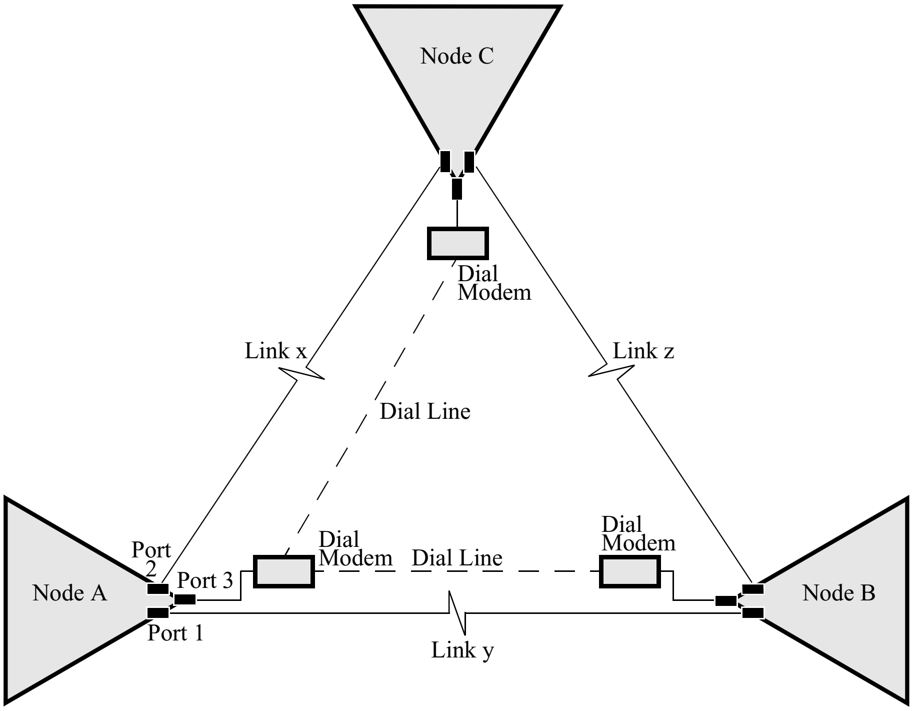


Figure 1-14. LBU Routing

LBU Routing Description

If Port 2 fails (link X), Port 3 dials the modem attached to Node C. If Port 1 fails (link Y), Port 3 dials the modem attached to Node B.

The two configured Switched Service Table entries work together to direct new X.25 calls even if both monitored ports fail at the same time. Consider a case where Link X (Port 2) has failed and the Backup or Switched Services port (Port 3) has been activated. Port 3 has effectively replaced Port 2 and data is now passing between Nodes A and C across the dial line.

If Link Y fails (Port 1) while the Backup or Switched Service port is still active for Port 2, communications between Nodes A and B are routed to the Backup or Switched Service Port (Port 3) link to Node C and then to Node B. This rerouting works because each node has a Route Selection Table for all other nodes in the network.

Caution

When either monitored link is restored, the Backup or Switched Service port *immediately* terminates its dial call and data may be lost. The Backup or Switched Service port then tries to establish a dial call for a link that is still down.

Routing Options

The process of rerouting in the delta network shown in Figure 1-15 has only one alternate route. Routing becomes more complicated if there are several possible paths between the two endpoints.

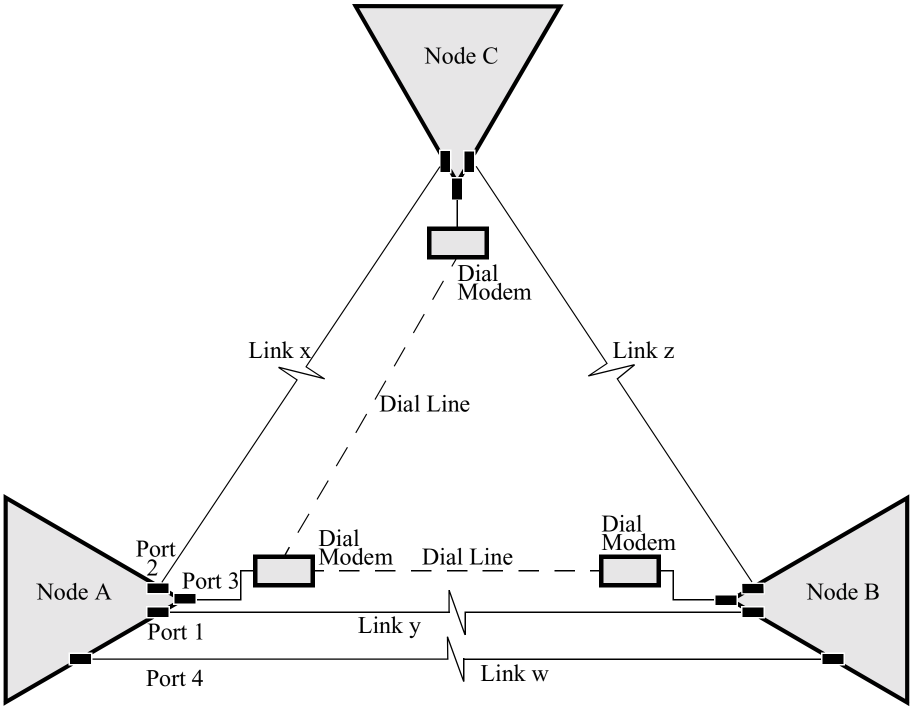


Figure 1-15. Routing Options with LBU

LBU Routing Options Description

Consider the example in Figure 1-15 where there are two links between Node A and Node B. Link Y is on Port 1 and Link W is on Port 4. If Link X fails, the Backup or Switched Service port is activated, connecting Nodes A and C. If Link Y (Port 1) fails (while Port 3 is still active), data between Nodes A and B can be routed in either of two ways:

- Over Port 3 (the Backup or Switched Service port) to Node C and then to Node B
- Over Port 4 and then directly to Node B

The choice of paths is determined by the interaction of link speed and the routing priority of Ports 3 and 4.

- If Port 3 has a high routing priority (lower number) than Port 4, communications may be routed over Port 3 (the roundabout path).
- If Port 4 has a higher routing priority (lower number) than Port 3, communications may be routed over Port 4 (the direct path).
- The higher the link speed the greater the possibility that the X.25 call is directed to the port.

Additional LBU/ Routing Considerations

In some network configurations, it is important to understand how misdirected routing paths can arise. Consider the linear network shown in Figure 1-16. The Backup or Switched Service port on Node A is configured to back up X.25 leased lines between Nodes A and B, and between Nodes A and C.

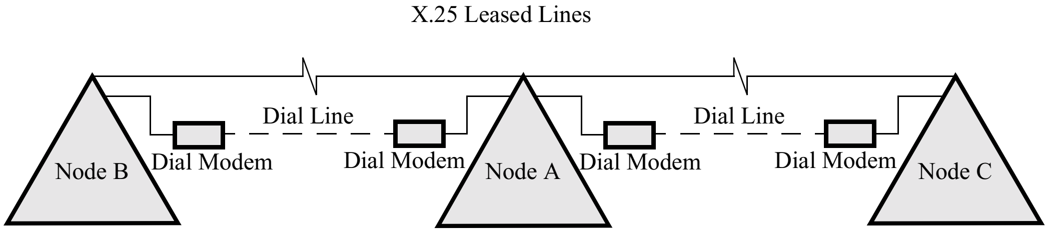


Figure 1-16. Simple Linear Network

If the X.25 link between Nodes A and B fails, the Backup or Switched Service port is activated and communications between the two nodes can resume. If the X.25 Link between Nodes A and C fails during this time, X.25 calls from Node A destined for Node C are directed to Node B instead. This situation cannot be prevented with the network shown in the Figure 1-16. Therefore, it is important to design your Switched Service Link Backup application to reduce the chances of this happening.

Load Sharing and Alternate Routing

Introduction

This section describes features for effective routing configuration using load sharing and alternate routing options. Do not confuse Load Sharing with Load Balancing, which is discussed on page 1-14.

Load Sharing

For load sharing, you can specify up to eight port destinations and priorities for each entry in the Route Selection Table. To implement load sharing, the network address, destination, and priority for the ports involved in load sharing must be in the same Route Selection Table entry and must have the same priority and link speed.

Choosing Port Priority for Load Sharing and Alternate Routing

When configuring 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, give this route a lower priority so that it is less likely to be used.

■ **Note**

The higher the priority number, the lower the priority. The top priority is 1. For example, a port with a priority number of 1 has a higher priority than a port with a priority of 2.

Zero is not valid. 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.

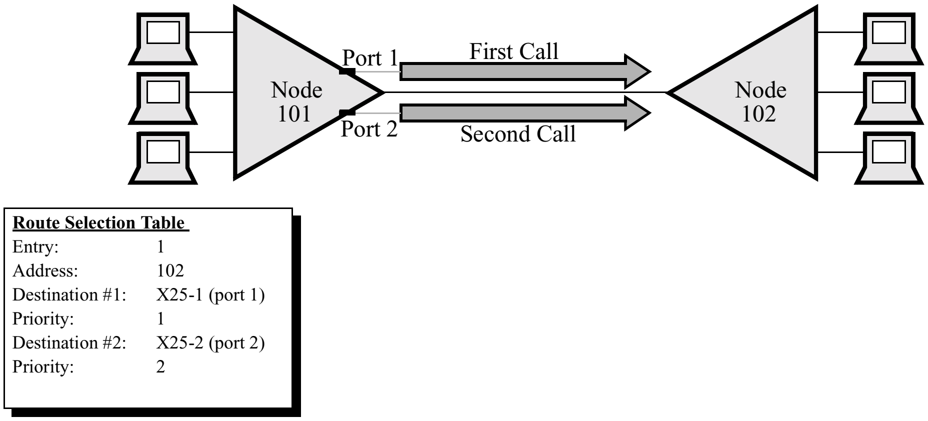
How Load Sharing and Alternate Routing Work

Introduction

Load Sharing lets you route calls destined for a particular node over two links instead of one to reduce congestion and maintain a reasonable throughput level. Alternate Routing allows you to direct traffic over alternate routes when the preferred link is unavailable.

Example of Load Sharing

Figure 1-17 shows an example of load sharing. Calls from terminals attached to Node 101 to terminals in Node 102 are routed over Ports 1 and 2 in Node 101 and the link speeds are the same.



Route Selection Table

Entry:	1
Address:	102
Destination #1:	X25-1 (port 1)
Priority:	1
Destination #2:	X25-2 (port 2)
Priority:	2

Figure 1-17. Load Sharing Example

How Load Sharing Works

The following table describes the load sharing example shown in Figure 1-17.

Step	Action	Result/Description
1	When the first call to Node 102 is initiated, Node 101 examines the network address comparing it against its own address.	Because there is no match, Node 101 then compares the Network Address against its Route Selection Table and finds a match for Node 102.
2	Node 101 then checks the Route Selection Table for the port over which calls are sent to Node 102 as well as the priority of the port.	Port 1 has a priority of 1.
3	The call goes out over Port 1.	
4	The second call goes through the same process, except it goes out over Port 2.	

Alternate Routing

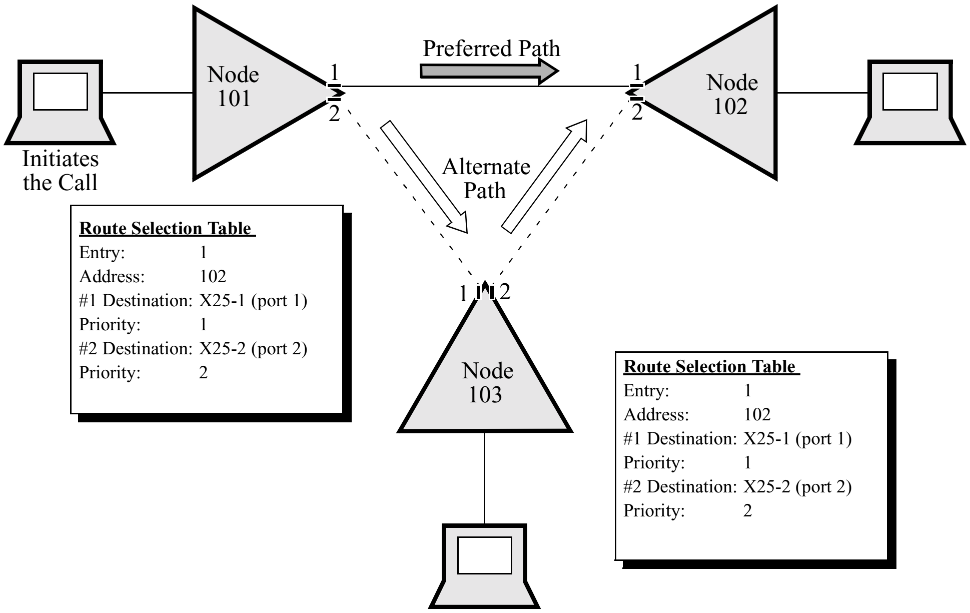
You can configure the Route Selection Table so that calls are routed over alternate links when the preferred link is unavailable.

Example of Alternate Routing

Figure 1-18 shows Node 101 configured for alternate routing. Node 101 has two paths to Node 102. Calls can be routed directly to Node 102. Alternatively, calls can be routed Node 102 via Node 103. This is configured in the Route Selection Table using multiple destinations in a single entry. The first destination entry is the preferred path. Subsequent destinations up to eight by default may be configured as alternate paths. You can use a CSK to increase the limit on destinations up to 16 per entry.

■ **Note**

There must be a corresponding Route Selection Table entry in Node 103 to provide a path to Node 102.



Route Selection Table

Entry:	1
Address:	102
#1 Destination:	X25-1 (port 1)
Priority:	1
#2 Destination:	X25-2 (port 2)
Priority:	2

Route Selection Table

Entry:	1
Address:	102
#1 Destination:	X25-1 (port 1)
Priority:	1
#2 Destination:	X25-2 (port 2)
Priority:	2

Figure 1-18. Alternate Routing Example

Data Connection Protection

Introduction

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

■ **Note**

You must enable DCP on the port that originates the call and the port that receives it. Set the Protection level parameter in the Port Record to Full_DCP to enable DCP. Do not use the control terminal to disconnect a call that is protected by DCP. Instead, disable the port.

CSK Required

Although you see the DCP parameters as part of the record, they are active only after you have purchased DCP and enabled the CSK. Because DCP is a option, you must purchase it from your VanguardMS representative and enable it with the CSK.

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

Data Protection

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

■ **Note**

DCP does not support calls to the Broadcast module.

Connection Protection

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

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

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

Data Connection Example

Figure 1-19 shows a data connection example. Nodes B and C have DCP configured for the ports attached to the terminal and mainframe.

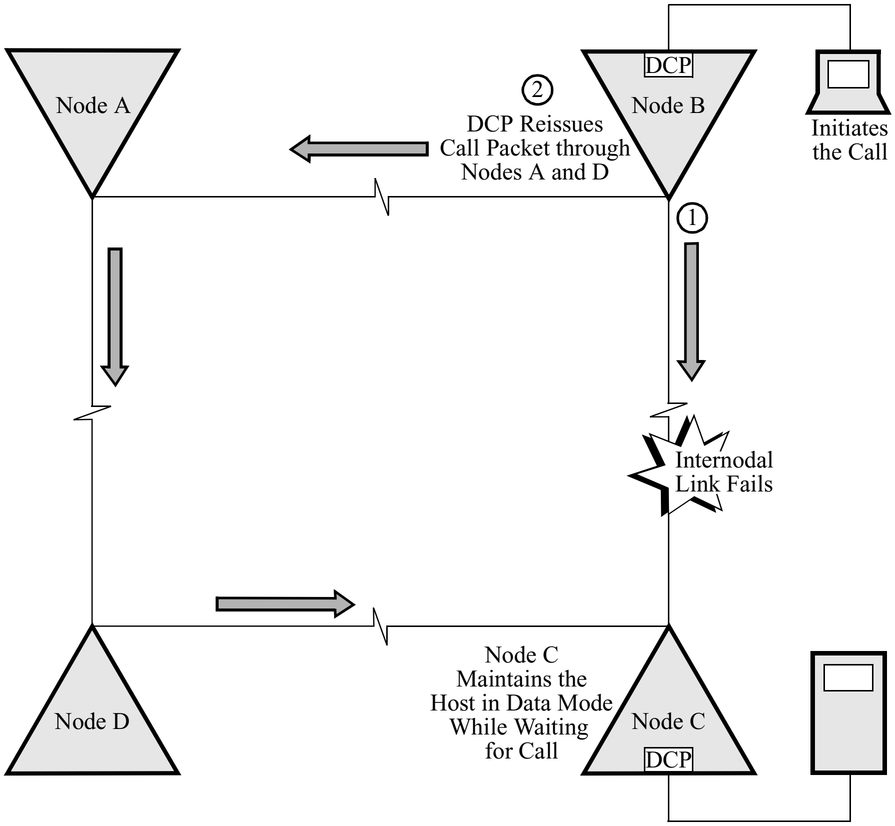

Node A
DCP
Node B
2
DCP Reissues Call Packet through Nodes A and D
Initiates the Call
1
Internodal Link Fails
Node C Maintains the Host in Data Mode While Waiting for Call
Node D
Node C
DCP

Figure 1-19. Data Connection Example

Data Protection Process

This table describes how data protection works.

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

DCP Parameters

Configure the following parameters to allow DCP to function in your network:

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

Traffic Priority

Introduction

Traffic priority applies to both Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs). You can assign traffic priority within an SVC and between SVCs.

Traffic Priority Between SVCs

Traffic priority at layer 3 of the X.25 network stack operates on virtual circuits (VC). Once you assign a priority class, the network port protocol stack uses the priority class to determine the order in which user ports transmit data packets for X.25 and Frame Relay Annex G traffic.

Traffic Priority Within an SVC

Besides prioritizing traffic between SVCs, you can assign priority to the various forwarders such as Source Route, Transparent Bridge, IPX, or IP. The WAN Adapter uses these forwarders to determine the order that frames are sent from the WAN Adapter to the network port within a VC.

Traffic priority occurs between the LAN Forwarder and the WAN Adapter only when the WAN Adapter has queued packets after being flow controlled from the network port.

When the WAN Adapter gets released from being flow controlled, it sends the higher priority traffic first. You configure this priority based on forwarder type and not for each Bridge Link or Router Interface.

Example of LAN Traffic Priority

Figure 1-20 shows the LAN Traffic Priority process.

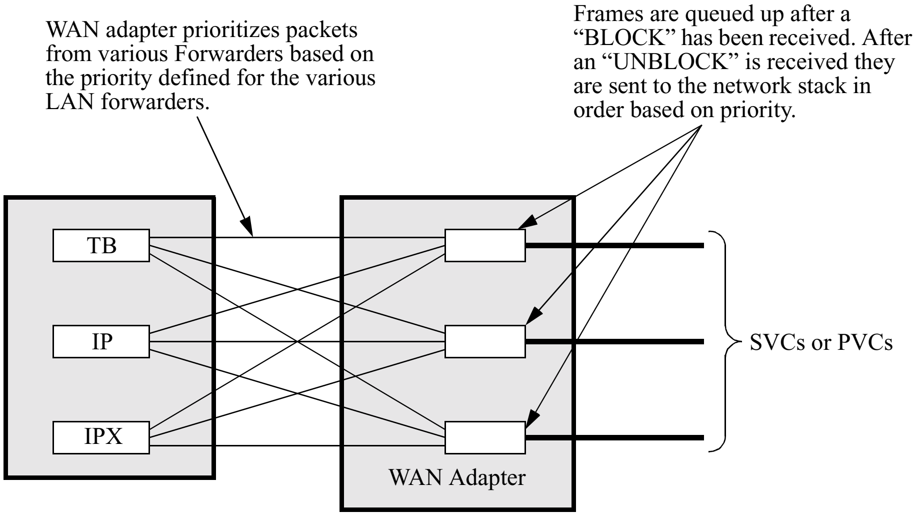

WAN adapter prioritizes packets from various Forwarders based on the priority defined for the various LAN forwarders.
Frames are queued up after a "BLOCK" has been received. After an "UNBLOCK" is received they are sent to the network stack in order based on priority.
TB
IP
IPX
WAN Adapter
SVCs or PVCs

Figure 1-20. LAN Traffic Priority

Traffic Priority Classes

The four priority classes for data passing are:

- Expedite
- High
- Medium
- Low

The expedite priority packets have the highest priority and use all of the link bandwidth that they need. Any remaining bandwidth is shared by the high, medium, and low priority packets.

■**Note**

All call control, call setup, and call clear default to the Expedite class. Do not assign protocol traffic to the Expedite class.

How Traffic Is Prioritized

The following table describes how traffic is prioritized:

<table>
<tr><th>Step</th><th colspan="2">Action</th><th>Result/Description</th></tr>
<tr><td>1</td><td colspan="2">LAN traffic is prioritized in an SVC within the WAN Adapter.</td><td>Priorities are set for bridged and routed (IP or IPX) traffic.</td></tr>
<tr><td>2</td><td colspan="2">The data frames from each of the SVCs passed to X.25, layer 3, are segmented into smaller frames to fit into the maximum packet size for the network link.</td><td></td></tr>
<tr><td>3</td><td colspan="2">The frames are placed on four priority queues depending on the assigned priority of the SVC.</td><td>Performing prioritization after the segmentation allows for interleaving of higher priority traffic and a large lower priority frame.</td></tr>
<tr><td rowspan="3">4</td><td colspan="2">When the X.25 layer 3 is ready to transmit another frame, it checks the expedite queue first.</td><td></td></tr>
<tr><th>If</th><th>Then</th><td></td></tr>
<tr><td>There are no frames ready for transmission</td><td>The X.25 layer 3 checks the other priority queues.</td><td>As long as there is data waiting on all three priority queues, X.25 layer 3 sends one medium priority packet for every number of high priority packets that you specify in the Traffic Priority Step parameter. See the “Priority Assignments By Port Type” section on page 1-33.
For every number of medium priority packets sent (specified in the Traffic Priority Step parameter), the X.25 layer 3 sends one low priority packet.</td></tr>
</table>

Configuration Information

Priority effects both the source and destination of the call if both nodes have been configured. Depending on the port type, you can configure the priority of a virtual circuit (VC) in one of two records:

- Station record - used for SDLC, Bisync, FRA-DCE, and LAN connections
- Node record - used for all other port types

Priority Assignments By Port Type

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

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

How Traffic Priority Functions

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

- Traffic Priority
- Traffic Priority Step

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

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

Transmitted Packet Sequences

The following table shows the relationship of the transmitted packet sequences when there is no expedite traffic and various conditions exist. In this example, the Traffic Priority Step is configured as 3. Although spaces are shown in the TX Packet Sequences column of the table, there is no actual time delay between frames.

If There Is No Expedite Traffic and There Are....	***The TX Packet Sequence With a Traffic Priority Step = 3 Is***
Sufficient high, medium and low priority packets to fill the queue.	HHH M HHH M HHH M L HHH M HHH M HHH M L
High and low priority packets to fill the queue, but no medium priority packet.	HHH HHH HHH L HHH HHH HHH L
Only two highs and enough medium and low priority packets to fill the queue.	HH M M M L M M M L

Packet Transmission Example

Figure 1-21 shows transmission of packets.

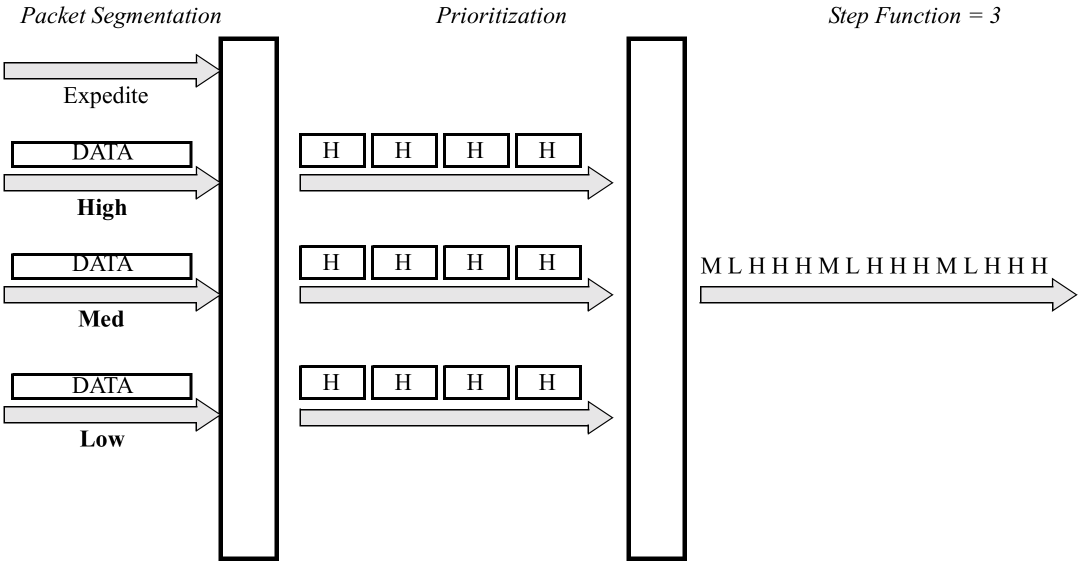


Figure 1-21. Packet Transmission

Recommendation

High, medium, and low priority packets are suitable for general data transfer. Because the Expedite packet can use up all the bandwidth of the link, only call control packets should be assigned Expedite priority.

With only high, medium, and low priority calls in a node, you can fine tune the networking prioritizing algorithm by changing the Traffic Priority Step parameter to ensure that even low priority packets are given some network bandwidth under heavy network loading conditions.

Traffic Priority Examples

Traffic Priority on X25 Links

Figure 1-22 shows the Traffic Priority process on X.25 links. When the network port on the Vanguard Products uses X.25 service, the data passing priorities determine which data is sent to the X.25 network. A round-robin algorithm within each priority level gets the next packet. The high, medium, and low priority packets are sent only when there are no expedite priority packets waiting to be sent.

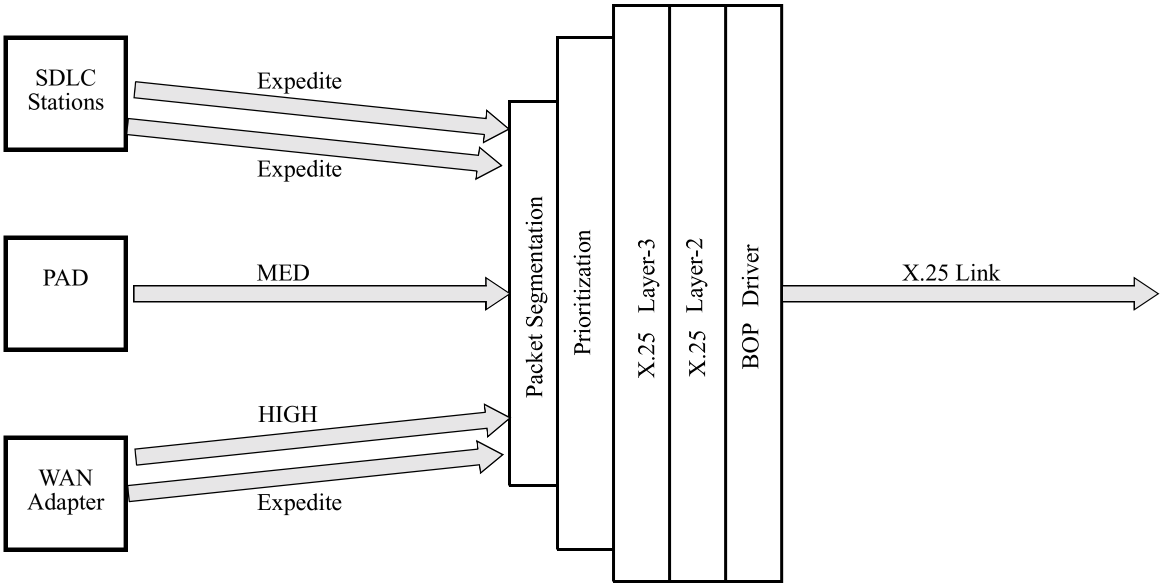


Figure 1-22. Traffic Priority on X.25 Links

Traffic Priority on Frame Relay Links

When the network port on the Vanguard products uses Frame Relay service as shown in Figure 1-23, traffic priority is performed within each Annex-G station only. This could cause lower priority traffic on one FRI station to be transmitted before higher priority traffic on other FRI stations. FRI-Bypass stations do not support traffic priority.

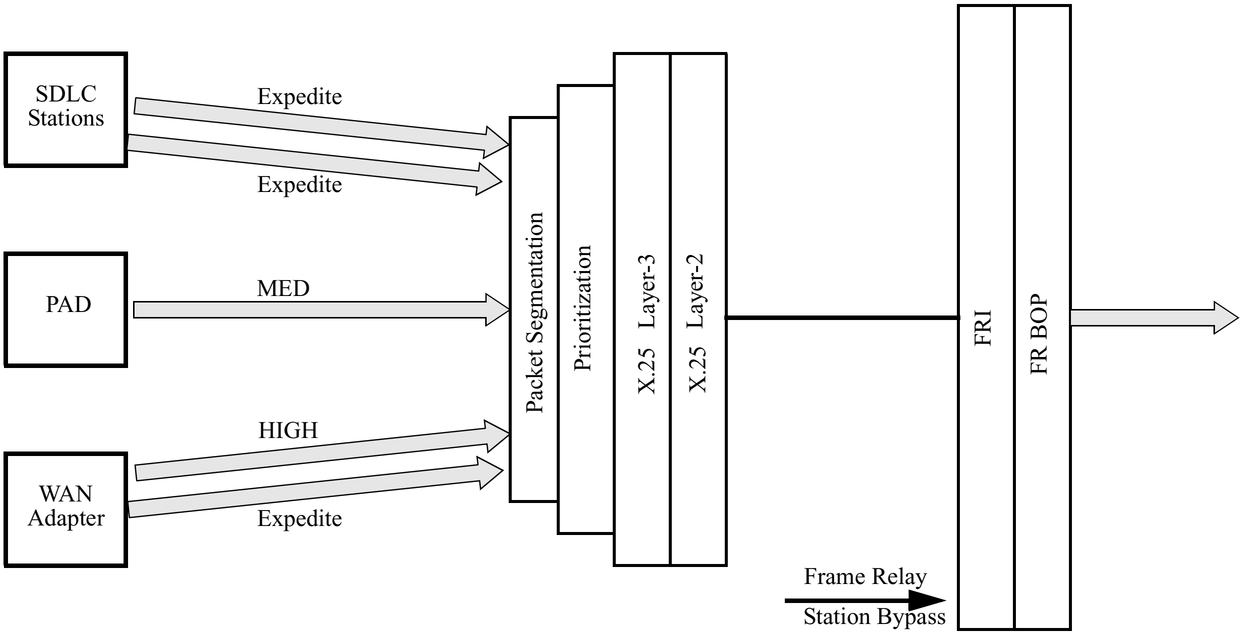


Figure 1-23. Traffic Priority on Frame Relay Links

Traffic Priority on Frame Relay

The following table describes how traffic priority works on Frame Relay links. MX.25 and XDLC ports operate the same as FRI ports.

<table>
<tr><th>Step</th><th colspan="2">Action</th><th>Description/Result</th></tr>
<tr><td>1</td><td colspan="2">Data frames queue up in Layers 2 and 3 of the Annex-G stacks in the same manner as Layers 2 and 3 of an X.25 port.</td><td></td></tr>
<tr><td rowspan="3">2</td><td colspan="2">The data frames are passed to FRI from either Annex-G or Bypass stations,</td><td>FRI passes the data frames to the BOP driver in the order they are received regardless of the priority of the data.</td></tr>
<tr><th>If</th><th>Then</th><td></td></tr>
<tr><td>One or more DLCIs are in a congested state</td><td>The FRI passes the frames to the BOP driver based on the Congestion Control Mode defined in the FRI port record.</td><td></td></tr>
<tr><td>3</td><td colspan="2">The data frames queue up for transmission in the BOP driver in the order that they were received from FRI.</td><td>The number of data frames that can be queued up in the BOP driver depends on the number of Bypass and Annex-G stations.
Because both FRA and the WAN Adapter support 4K frames, the size of the frames queued up in the BOP drivers could be up to 4K bytes long, which increases the time required to transmit these frames.</td></tr>
</table>

About the Bypass Station

Each bypass station (either connected to an FRA station or a WAN Adapter port using PVC) can have up to 16 data frames *outstanding*.

In the case of a bypass station, outstanding means waiting for transmission in either FRI or BOP driver queues. This means that it is possible, but unlikely, that the number of data frames queued in the BOP driver could equal 16 times the number of Bypass stations plus two times the number of Annex-G stations. It is more likely that there could be only one to three data frames from a number of Bypass stations.

Time of Week Dial Filtering

Introduction

Time of Week (ToW) Dial Filtering refers to disabling an ISDN port's incoming and outgoing dialing for a specified time. You configure a set of intervals to define the day, time, and duration during which dialing applications cannot access the port. The maximum configurable duration is one week.

How Time of Week Dial Filtering Works

The Time of Week Table is a set of records where each record contains an entry name identifying the record, and a set of time intervals that determine how and when a dial port functions. When you configure this table and a Switched Services dial port, using the same entry name in each, the time duration specified by the intervals determines when the port can dial in or dial out and when it cannot.

Advantages

Time of Week Dial Filtering, which restricts dial-out and dial-in access for ISDN ports at certain time periods, can be useful, for example, when considering costs during peak usage periods or after hours.

Features

ToW offers the following features:

- Configurable control over dial port usage for both incoming and outgoing calls.
- Up to 10 sets of configurable, non-overlapping time period intervals per port within a week, allowing you to enable or disable dialing at different times and for different reasons to create a port "profile" and specify how dialing is controlled.
- Centralized placement within the Switched Services architecture allowing easy access by dialing applications that can benefit from Time of Week functionality.

Support

Time of Week Dial Filtering supports the following:

Vanguard Routers

- Dial-out control for the following Switched Services port types:
  - Monitored ports: X.25, Frame Relay Station (Annex G), ISDN D Channel
  - Backup ports: X.25, ISDN B Channel (Switched Channel)
- Dial-in control for ISDN channels only. X.25 and FRI ports are not supported.
- ToW Dial Filtering works with Policy Based Routing. See the IP Routing Manual (Part Number T0100-03) for more information on Policy Based Routing and ToW.

Vanguard 100PC/200/300/305/310/320

- Dial-out control for the following Switched Services port types:
  - Monitored ports: X.25, Frame Relay Station (Annex G), ISDN D Channel
  - Backup ports: X.25, ISDN B Channel (Switched Channel)
- Dial-in control is unavailable for all port types, including ISDN.

Vanguard 6400 Series

- Dial-out control for the following Switched Services port types:
  - Monitored ports: X.25, Frame Relay Station (Annex G), ISDN D Channel
  - Backup ports: X.25, ISDN B Channel (Switched Channel)
- Dial-in control is unavailable for all port types, including ISDN.

Examine, List, Delete, and Copy Menus

- The Time of Week Table functions in a similar manner to other menus supported by the Vanguard Products CTP.

Chapter 2
Tables and Records Used to Manage Bandwidth

Introduction

This chapter describes the tables, records, parameters, and procedures you use to configure Vanguard bandwidth management features. Many of these features share common menus and are, therefore, grouped together.

Configure Network Services Menu

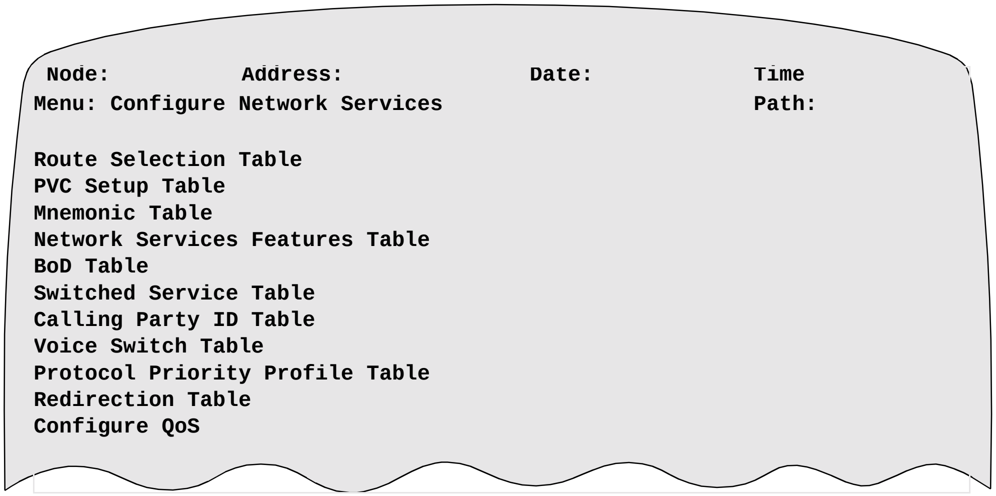
Introduction

The Configure Network Services menu provides access to various tables you use to determine how traffic is transferred. These include tables such as:

- Route Selection Table - Used to direct outbound calls to a specific node or port.
- Bandwidth on Demand (BoD) and Switched Services Tables: Used to configure dialing operations such as:
  - Dial on Demand (DoD)
  - Bandwidth on Demand
  - Load Balancing
  - Link Backup
- Protocol Priority Profile Table: Used to assign priority classes to traffic and the percentage of bandwidth available to those classes. For information on Protocol Priority, refer to the *Protocol Priority Manual* (Part Number T0100-09).
- Configure QoS (Quality of Service): Used to provide end-to-end service with respect to service availability, throughput, delay, jitter, and packet loss. For more information on QoS, refer to the *Quality of Service Manual* (Part Number T0100-10).

What You See in This Menu

Figure 2-1 shows the Configure Network Services menu:



```
 Node:          Address:              Date:            Time
Menu: Configure Network Services                       Path:

Route Selection Table
PVC Setup Table
Mnemonic Table
Network Services Features Table
BoD Table
Switched Service Table
Calling Party ID Table
Voice Switch Table
Protocol Priority Profile Table
Redirection Table
Configure QoS
```

Figure 2-1. Configure Network Services Menu

Records

Records that effect Bandwidth Management that are available from the Configure Network Services menu include:

Record	***Description***
Route Selection Table	Used to select links over which calls are routed to a specific node or port in the network.
BoD Table	Used to configure Bandwidth on Demand primary and secondary (parallel SVC) links.
Switched Services Table	Supports dialing options such as Dial on Demand, Bandwidth on Demand, and Link Backup.
Calling Party ID Table	Provides configurable security parameters for Switched Services Table entries.
Protocol Priority Profile Table	Allows prioritization of traffic classes and percentage of bandwidth for various protocols.

Network Services Control Menu

Also part of the Network Services menu group is the Network Services Control Menu, which has parameters that globally enable or disable Bandwidth on Demand across all ports for the node. Refer to page 2-39.

Switched Services Table (Dialing Operations)

Introduction

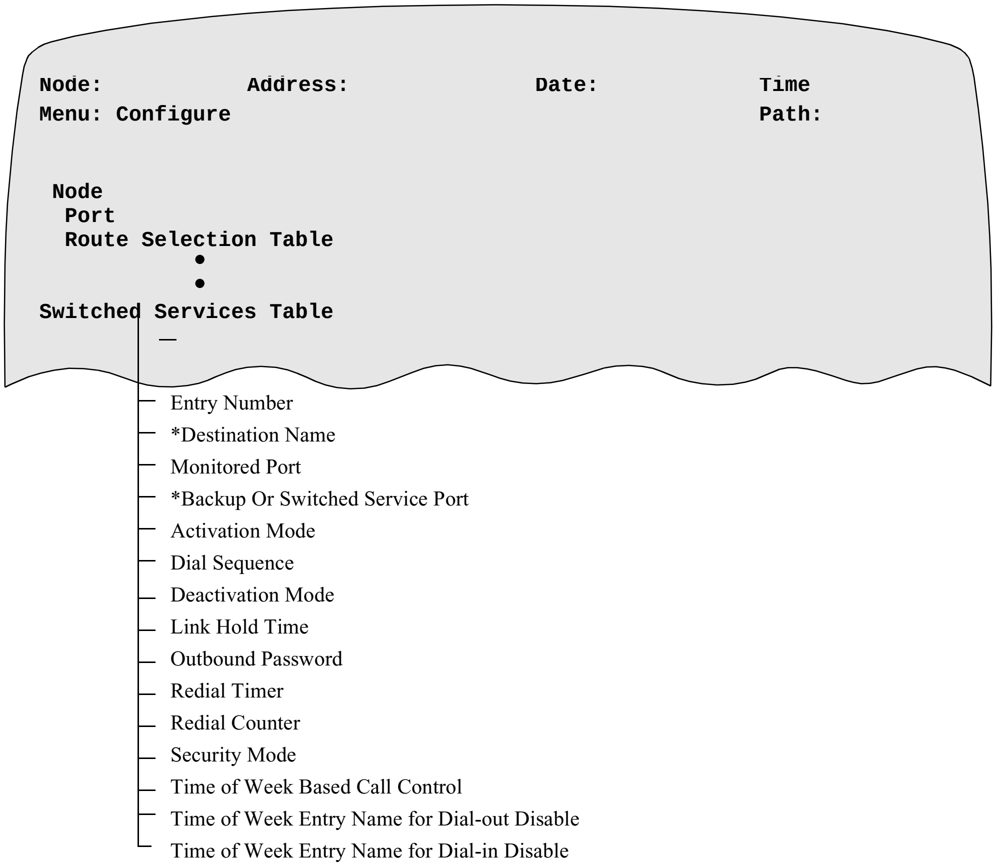
This section describes the Switched Services Table.

The Switched Services Table supports dialing operations such as:

- Dial on Demand, including the sharing of a dial port with multiple destinations
- Bandwidth on Demand, for congestion backup
- Link Backup, for backup of a monitored port in case of failure
- Time of Week Dial Filtering

What You See in This Record

Figure 2-2 shows the Switched Services Table Record and its configuration parameters. These include parameters for Link Backup, dialing, and security operations. The parameters are described on page 2-10.



```
Node:           Address:                Date:            Time
Menu: Configure                                          Path:


 Node
  Port
  Route Selection Table
            •
            •
Switched Services Table
         _
```

Figure 2-2. Switched Services Table

Guidelines

This table describes some guidelines for configuring switched services.

Step	Description
1	Configure the Port Records for the monitored ports: • Idle Timer: A value other than zero for an X.25 port • X.25 Option: BKUP • Connection Type: DIMOv, or SW56K (or DIMO, which is not recommended) ■ **Note** You can configure up to four ports as monitored ports. The backup takes over only when all four of these monitored ports are Down.
2	Configure the Switched Services Table: • Backup Or Switched Services Port: X25-*n* (for X.25 ports) BRI-*ny* (for ISDN ports) where *n* is the port number and *y* is the channel number • All other necessary parameters (see Figure 2-2).
3	Configure the Route Selection and Mnemonic Table Destination parameters to the same value if you intend to use mnemonics.

Recommended Settings

When configuring a port as backup to a monitored port or as a Switched port, you must configure the following in the backup port's X.25 Port Record. This is true whether you are configuring the port for Dial on Demand or Bandwidth on Demand purposes.

- X.25 Option: BKUP
- Connection Type: DIMOv or SW56K

  The DIMOv connection type supports V.25 *bis* type modems, which can accept packets containing a destination phone number. This allows up to 200 entries to be set in the Switched Services Table and forwarded to the modem.

The SW56 Kbps connection type is similar to DIMOv except that it works with Switched 56 Kbps circuits.

You can also specify the DIMO connection type, used to set DTR dialing on modems. However, DTR dialing requires phone numbers to be configured in the modem, where only a limited number of entries are allowed.

Accessing the Switched Services Table

Follow these steps to access the Switched Services Table record:

Main -> Configure -> Configure Network Services -> Switched Services Table.

Using the Switched Services Table

Introduction

This section describes how you use the Switched Services Table Record, including information on dialing operations, support, and security features.

Support

Switched Services supports the following:

- Monitored port types
  - X.25
  - Frame Relay Station (Annex G)
  - ISDN D channel
- Backup port types
  - X.25
  - ISDN B Channel (Switched Channel)
  - Serial Protocol over TCP (SoTCP)

Entry Compression

As of release 5.1, new entries in the Switched Services table are compressed. Entries in the Switch Services that you made while the node was running a software image 5.0 (or earlier) remain uncompressed.

If you want to compress the entire Switched Services (old entries and new), access the record through the CTP menu and save it.

■ **Note**

You can only view compressed Switched Services entries and records with software release 5.1 and later.

Sharing a Dial (DoD) Port with Multiple Destinations

For IP data, you can use a Switched Services Port as a primary dial port that is activated any time there is data arriving to establish an outbound call. This is not possible with other serial protocols. If Switched Services is desired, configure the Monitor Port parameter of the Switched Services configuration as blank.

Switched Services allows different phone numbers to be configured in multiple Switched Services entries for the same dial port. This means that once a Backup Or Switched Services Port is inactive, another phone number in a different Switched Services entry (also configured to use this port) can dial over it. This allows you to share the dial port for dialing different locations.

Using the Switched Services Port for BoD Connections

You can use a Switched Services port as congestion backup to a LAN Connection's monitored port. To do this, you configure a Parallel SVC(s) and Parallel SVC Threshold in the LAN Connection's Monitored port to point to the Backup Or Switched Port in the Switched Services Table. When the congestion threshold is met on the monitored port, a Parallel SVC(s) is activated through the dial port specified in the Switched Services Table. Once congestion is alleviated, packets are redirected to the primary (monitor) port.

Using SoTCP as a Backup

To use SoTCP as a backup link, you must have an SoTCP session configured on the node. It can be an SoTCP session that you are using for other traffic or an SoTCP session configured solely as a backup.

SoTCP, unlike other links used as a backup, is not activated or deactivated by Switched Services. SoTCP brings up the TCP connection up and down based on X.25 calls. So when Switched Services forwards a call to an SoTCP backup session, it does not know if the SoTCP session is configured. If the node does not have a configured SoTCP session, the call fails.

These are the configuration rules for SoTCP as a backup port:

- Set the Activation Mode parameter to NONE or NONE_ALL.
- Set the Deactivation Mode parameter to IMM_CALL_CLR and NONE.
- Set the Link Hold Time parameter to 0.
- Use the Spacebar to blank the Dial Sequence #1-4 field.

For information on configuring SoTCP, see the *SoTCP Manual* (Part Number T0100-06).

■ **Note**

Switched Services Statistics always shows SoTCP status as IDLE because SoTCP, not Switched Services, controls activation and deactivation. View the SoTCP status from SoTCP statistics.

Switched Services Security

Switched Services provides Calling Party ID and Password security features for ISDN ports. Switched Services security features do not work for X.25 ports. The security feature:

- Provides the CTP interface for configuring security.
- Provides passwords for outgoing switched calls.
- Validates incoming calls.

Calling Party ID Table

The Calling Party ID Table is a list of phone numbers that are accepted by the node. You can configure up to 200 entries in this table.

Each phone number can be 30 characters in length. Numerics, dashes, and periods are valid for the Calling Party ID Table. Refer to page 2-16 for details.

Passwords

You can configure a single node password in the node record to validate incoming calls. You can also configure a password for outgoing calls via the Outbound Password parameter on the Configure Switched Services Table menu.

How Switched Services Security Works for Incoming ISDN Calls

When an incoming switched call arrives at an ISDN port, the port calls the Switched Services Table with either or both of the following:

- Inbound password
- Calling party ID

Switched Services checks the security mode you have configured to determine what to check. The call is accepted if:

- No security is enabled.
- A password is configured in the node record, which matches the incoming password.
- The Calling party ID Table, if enabled, matches the incoming Calling party ID

Any test that is not passed generates an alarm.

■ **Note**

These events are not mutually exclusive. If both security options are enabled, both checks must be passed. You can activate a Switched Services/Backup port via the CTP.

Deactivating a Switched Services Link

There are several ways to deactivate a Switched Services link:

- Link Failure (physically disconnected).
- A port boot/disable from the CTP.
- Link Hold Timer/X25 Idle Timer expires (X25 port only).
- When a monitored port comes up.

Link Hold Time

For ISDN port/channels, the Link Hold Time deactivates the link if there are no X.25 SVC calls.

For X.25 ports, the Link Hold Time overwrites the X.25 idle time. For example, if Link Hold Time is configured as one minute while the X.25 idle time is configured for ten seconds, the link deactivates after one minute provided there are no X.25 SVC calls.

Redundant Backup

With the Switched Services, you can configure the monitor ports so they are prioritized and the backup port to activate when one or all monitor ports fail.

Port Prioritization

The Redundant Backup CSK controls port prioritization only. When you use this CSK, the first port in the list of monitored ports is treated as the primary monitored port and the remaining ports are treated as secondary. When the primary port is down, the secondary ports pass its traffic. When the primary port reactivates, the node clears the secondary ports and routes traffic to the primary port.

To enable port prioritization, follow these steps:

Step	*Action*
1	Select **Configure** from the CTP Main menu.
2	Select **Software Key Table** from the Configure menu.
3	Press ENTER to access the Key Value field and enter the following CSK number: **TVK3Y4F6L3FYDQNSG8B2**
4	Perform a Node boot to implement your changes.

Backup Activation

You can configure a Switched Services Table so the allocated backup port activates when the monitor ports fail. You can configure backup in two ways:

- If you want the backup port to activate when one of the monitor ports fails, configure the Activation Mode parameter with the option FAIL.
- If you want the backup port to activate only when all of the monitor ports fail, configure the Activation Mode parameter with the option FAIL_ALL. If any one of the monitor ports becomes active, the backup link is de-activated.

Multi-Dial Sequence

You can enter up to four dial sequences for each backup port. The default values of the Dial Sequences should be blanked out, if not required.

When the backup port is dialing out, it selects the first configured dial sequence for dial-out. If this number is unreachable, it selects the second configured dial sequence. In this way, the back up port selects each configured dial sequence until it exhausts the list. After exhausting all possible dial sequences, it goes back to the first dial sequence.

The Retry Limit specifies the number of retry cycles that the backup port performs before clearing the application call. When the backup port activates, the retry cycle terminates.

Switched Services Table Parameters

Introduction

This section describes the Switched Services Table parameters including the Link Backup parameters.

■ **Note**

Any parameter with an asterisk (*) requires a Node boot; changes to other parameters require a Table and Node Record boot.

Parameters

From the Switched Services Table, you can configure the following parameters (with the exception of Entry Number):

Entry Number

Range:	1 to 200
Default:	1
Description:	Specifies the Entry number used to reference this table record. ■ **Note** On the Vanguard device, the number of maximum number Switched Services Entries can be set to 1024 with the Max Switched Services Entries parameter in the Node Record.

*Destination Name

Range:	0 to 32 alphanumeric characters. Use the space character to blank the field.
Default:	(blank)
Description:	Enter a unique name that identifies this entry. The name is mapped to a destination name configured in a ROUT entry record. It can be used by a LAN connection parallel SVC port, which maps this name to bring up a dial on demand link.

Monitored Port #1-4

Range:	0 to 32 alphanumeric characters. Use the space bar to blank the field.
Default:	(blank)
Description:	Specifies the network protocol port to be monitored for link failure. Supported port types are as follows: • X.25 • FRI • Annex G Station • BRI Permanent Channel

*Backup Or Switched Service Port

Range:	0 to 32 alphanumeric characters
Default:	Space blanks the field.
Description:	This port acts as the backup when there is a port failure on the port specified in the Monitored Port parameter or when the congestion threshold is met for a Parallel Dial port. The format must be X25 -*n*, where *n* is the X.25 port number. The priority of this port in the Route Selection Table should not be set to 0. X25, BRI Switched Channels, FRI, and SoTCP are supported port types. ■Note An SoTCP session must be configured to use the SoTCP backup option. See the SoTCP Manual (T0100-06) for more information on configuring an SoTCP session.

*Activation Mode

Range:	FAIL, CALL, EITHER, BOTH, FAIL_ALL, NONE, NONE_ALL
Default:	CALL
Description:	Specifies how the backup port is activated: • FAIL: Activate backup port upon link failure. • CALL: Activate backup port upon call request. • EITHER: Activate backup port upon link failure or call request. • BOTH: Activate backup port upon link failure and call request. • FAIL_ALL: Activate backup when all the monitored ports/stations are inactive. • NONE: Forwards the call to a backup port if the monitor port or ports are down. If the backup port is up, the call goes through; if the backup port is down, the call fails. • NONE_ALL: Forwards the call to a backup port if all the monitor ports are down. If the backup port is up, the call goes through; if the backup port is down, the call fails. ■Note The SoTCP backup option requires the NONE or NONE_ALL setting to function.

Dial Sequence #1-4

Range:	0 to 30 numerical characters and/or special characters. Use the space character to blank the field.
Default:	#1
Description:	You can either have the modem dial a preprogrammed telephone number or you can enter the telephone number yourself. • To have the modem dial one of its preprogrammed telephone numbers, enter #*n* where *n* is the preprogrammed telephone number stored in the modem. • To enter your own telephone number, use any combination of the following characters: – 0 to 9 (Decimal) – : (Wait tone) – < (Pause) – = (Separator 3) – > (Separator 4) ■ **Note** For the SoTCP backup option, use the spacebar to blank the field.

Deactivation Mode

Range:	NONE, BUSYOUT, IMM, IMM_CALL_CLR
Default:	BUSYOUT
Description:	Specifies how the backup port is deactivated: • NONE: Backup port can be activated only by operator intervention. • BUSYOUT: Backup port is deactivated after the calls on the port are deactivated for a predetermined amount of time. For X.25 port, this substitutes the value assigned to the parameter Link Hold Tone with the value assigned to the parameter Idle Disconnect Time in the X.25 port record. When deactivation mode = Busy Out and Link Hold Time - 0 (zero), the overall effect is the same as setting this entry to NONE. • IMM: The backup link is terminated immediately when the monitored port is restored regardless of how many calls are present. • IMM_CALL_CLR: Forwards all the calls meant for the monitor ports that are down to the backup link and saves them. When one of the monitor ports comes up, all these calls are cleared, but the backup link is not brought down. ■ **Note** For the SoTCP backup option, Deactivation Mode must be set to IMM_CALL_CLR or NONE. Other backup options can use the IMM_CALL_CLR setting.

Link Hold Time

Range:	0 to 3200 seconds
Default:	0
Description:	Detects idle conditions on the line, where idle means no calls active. This replaces the setting of the parameter Idle Disconnect Timer (in the X.25 Port Record), and specifies how long (in seconds) the backup link remains active after the original link is backed up. A longer period gives the original link time to stabilize before it accepts calls. This timer works for protocols other than X.25. Operation for non-X.25 ports is the same as for X.25 ports. ■ **Note** The SoTCP backup option requires a 0 setting.

Outbound Password

Range:	0 to 9 alphanumeric characters
Default:	The Space character blanks the field.
Description:	Password used by the remote station to determine if dial access is authorized.

Redial Timer

Range:	5 to 3600
Default:	300 (See Below)
Description:	Defines the time (in seconds) between dialing attempts when activating a Switched Services call. ■ **Note** Redial time must be set to at least four minutes (240 seconds) for an X.25 port. On a Vanguard 6560 if the redial timer in the switched service is changed (from its default of 300 seconds) to a value that is less then it takes frame relay to establish its control protocol, then switched services places another call before the first one completes. This creates a call collision and both calls are cleared. To prevent collision, increase the redial time in the switched services record so that it is greater than the time required for the frame relay port to declare itself up. Any value greater than 60 seconds should be sufficient.

Redial Counter

Range:	0 to 255
Default:	5
Description:	Specifies the number of times that Switched Services attempts to redial once the redial timer has expired. A value of zero allows unlimited attempts.

Security Mode

Range:	Password, Calling party ID, Both, None
Default:	None
Description:	Determines the port's security option(s), which Switched Services checks when receiving a call.

Switched Services Time of Week Dial Filtering Parameters

Configure parameters in this section to enable Time of Week functionality for a Switched Services dial port. Switched Services controls the dialing timeouts configured on the Time of Week Table, available from the Configure menu. From the Switched Services Table, you can configure the following Time of Week parameters:

■ **Note**

Other Time of Week parameters are discussed beginning on page 2-18.

Time of Week Based Call Control

Range:	ENABLED/DISABLED
Default:	ENABLED
Description:	Specifies time intervals during a week when dial-ins and dial-outs for a port must be disabled. ■ **Note** Set to ENABLED for SoTCP backup.

Time of Week Entry Name for Dial-out Disable

Range:	0 to 20 alphanumeric characters matching entry name configured in Configure Time of Week menu.
Default:	DEFAULT
Description:	Points to a Time of Week profile table to disable dial-out capability on this port during the time interval specified by the ToW parameters, provided the Time of Week Entry Name parameter matches the name specified here. This parameter appears only when Time of Week-based Call Control is enabled. The entry name configured for the Switched Services dial port must be the same as the ToW entry name.

Time of Week Entry Name for Dial-in Disable

Range:	0 to 20 alphanumeric characters matching entry name configured in Configure Time of Week menu.
Default:	DEFAULT
Description:	Points to a Time of Week profile table to disable dial-in capability on this port during the time interval specified by the ToW parameters provided the Time of Week Entry Name parameter matches the name specified here. This parameter appears only when Time of Week-based Call Control is enabled. The entry name configured for the Switched Services dial port must be the same as the ToW entry name.

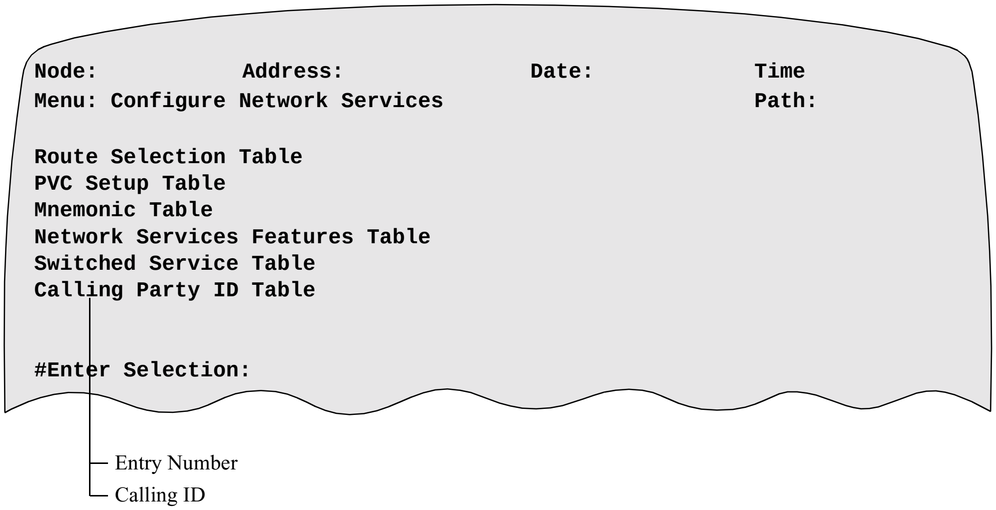
Switched Services Security (Calling Party ID Table)

Introduction

This table provides parameters you use to configure the Calling Party ID Table, which provides incoming call validation for Switched Services.

What You See In This Record

Figure 2-3 shows how the Calling Party ID Table and its configuration parameters fit into the Vanguard products menu hierarchy. Use these parameters to configure the Calling Party ID Table:



```
Node:            Address:              Date:            Time
Menu: Configure Network Services                        Path:

Route Selection Table
PVC Setup Table
Mnemonic Table
Network Services Features Table
Switched Service Table
Calling Party ID Table


#Enter Selection:
```

Figure 2-3. Calling Party ID Table Record

Configuration Considerations

There are no specific configuration considerations associated with the Calling Party ID Table.

Accessing the Calling Party ID Table

Follow these steps to access the Calling Party ID Table:

Main -> Configure -> Configure Network Services -> Calling Party ID Table

Parameters

From the Calling Party ID Table Record, you can configure these parameters:

Entry Number:

Range:	1 to 512
Default:	255
Description:	Identifies the entry number used to reference this record. The range is determined by the Node Record parameter Maximum Calling Identifier Table Size. See the *Vanguard Basic Configuration Manual* (Part Number T0113) for more information.

Calling ID:

Range:	0 to 30 numeric or special characters, including period (.) or dash (-). Use the space bar to blank the field.
Default:	A Space character blanks the field.
Description:	Each Calling Party ID is a numeric value that can contains periods or dashes. Only calls matching these IDs are allowed when Calling ID security is enabled for Switched Services.

Time of Week Table Dial Filtering Configuration

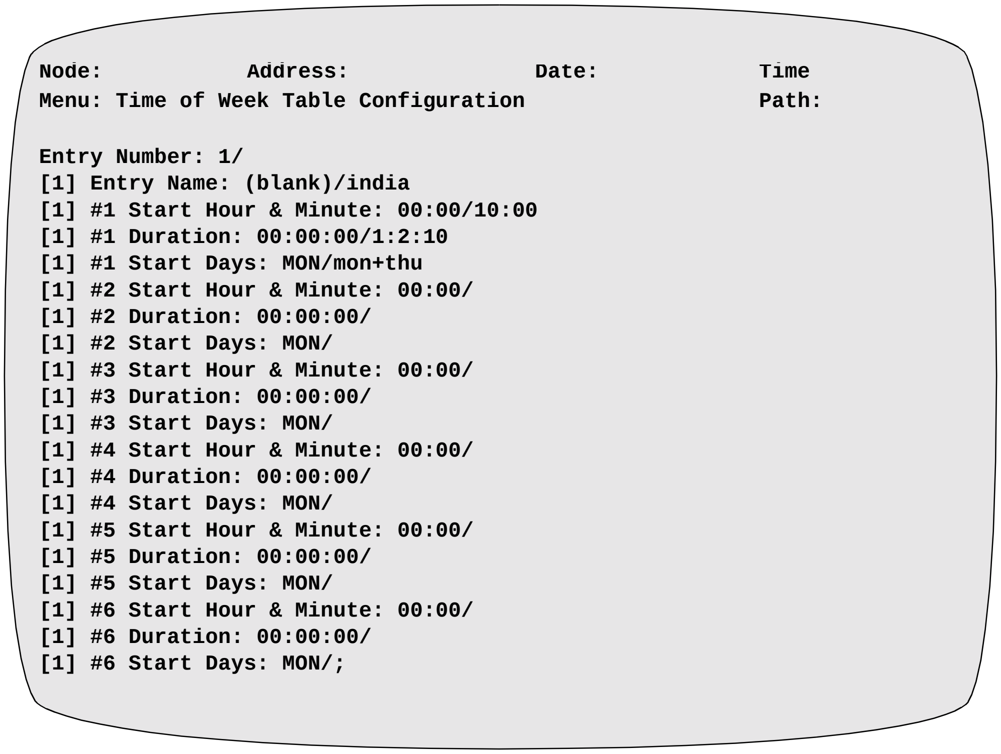
Introduction

This section describes the parameters you use to configure Time of Week Dial Filtering. The Time of Week Table is used to configure start times, duration, and days for Dial-in or Dial-out disabling of a Switched Services dial port.

Also refer to page 2-4 for Time of Week parameters you enable through the Switched Services Table.

What You See in This Table

Figure 2-4 shows the Time of Week Table, available from the Configure menu.



```
Node:           Address:               Date:            Time
Menu: Time of Week Table Configuration                  Path:

Entry Number: 1/
[1] Entry Name: (blank)/india
[1] #1 Start Hour & Minute: 00:00/10:00
[1] #1 Duration: 00:00:00/1:2:10
[1] #1 Start Days: MON/mon+thu
[1] #2 Start Hour & Minute: 00:00/
[1] #2 Duration: 00:00:00/
[1] #2 Start Days: MON/
[1] #3 Start Hour & Minute: 00:00/
[1] #3 Duration: 00:00:00/
[1] #3 Start Days: MON/
[1] #4 Start Hour & Minute: 00:00/
[1] #4 Duration: 00:00:00/
[1] #4 Start Days: MON/
[1] #5 Start Hour & Minute: 00:00/
[1] #5 Duration: 00:00:00/
[1] #5 Start Days: MON/
[1] #6 Start Hour & Minute: 00:00/
[1] #6 Duration: 00:00:00/
[1] #6 Start Days: MON/;
```

Figure 2-4. Sample Configure Time of Week Table

General Steps to Configure Time of Week Dial Filtering

This table lists the general steps you perform to configure ToW. Refer to the sections “Accessing the Time of Week Table” on page 2-18 and “Accessing the Switched Services Table” on page 2-5 for specific configuration steps.

Step	*Action*
1	Access the Time of Week Table Record from the Main Configure menu.
2	Configure an entry name that is meaningful to your Time of Week dialing application, for example, **afterhours**.
3	Configure other Time of Week parameters.
4	Access the Switched Services Table record.
5	Enable the Time of Week Call Control parameter and configure a dial-in or dial-out entry name that matches the one you configured under the Configure Time of Week menu.
6	Boot the table and node to implement your changes.

Guidelines

These guidelines apply to configuring the ToW parameters using the Time of Week and Switched Services Tables:

Interval Considerations

- The three parameters: Start Hour & Minute, Duration, and Start Days, together specify one interval.
- You can configure a total of ten intervals for any one entry.
- The intervals configured for a single entry must not overlap.
- An interval with a duration of zero (00:00:00) is treated as having no interval.

Present Time Considerations

- If the present time falls within one of the configured disable time intervals, no dial-outs are made, although the link can still be activated. If the link is already active (because of a call) and the present time falls within one of the disable time intervals, the link remains active. If the link is deactivated because of a call clear (switched port or link backup), the link cannot be activated again until the present time no longer falls within the disable period.
- ToW depends on accurate system date and time. Any changes to system date and time that occur without rebooting the ToW and Switched Services Tables can result in the following situations:
  - If an interval falls within the present time, and the system time is changed to a later time, the interval may be skipped.
  - If an interval falls within the present time, and the system time is changed to an earlier time, the same interval may be entered again.

Switched Services Considerations

- When configuring Switched Services for Vanguard ISDN ToW dialing applications, make sure no dial-out number is configured in the ISDN Channel configuration. If a dial-out number is configured in the Vanguard ISDN Channel configuration, it overrides the dial-out made by Switched Services. Since ToW-based dial control is part of the Switched Services functionality, the feature works only when Switched Services controls the dialing. This limitation does not apply to Vanguard ISDN.
- Time of Week Call Control can be enabled or disabled at runtime.

Accessing the Time of Week Table

Perform these steps to access the Time of Week Table:

Main -> Configure -> ToW Table

Time of Week Dial Filtering Parameters

Introduction

This section describes the Time of Week Dial Filtering parameters that you configure using the Configure Time of Week menu. Parameters in these prompts list the default value followed by a slash character. To accept the default, press ENTER; otherwise, enter a valid value following the slash, and then press ENTER.

■Note

Changes to parameters in this table require a Table and Node Boot to take effect. You can also choose the Time of Week table from the Boot Menu to boot the Time of Week table independently of the node if you do not want the boot to effect other Vanguard product modules.

Parameters

From the Time of Week Table, you can configure these ToW parameters:

Entry Number

Range:	1 to 10
Default:	1
Description:	Identifies by number the particular ToW Table entry being configured by the other parameters in the record.

Entry Name

Range:	0 to 20 alphanumeric characters
Default:	DEFAULT
Description:	Identifies by name the particular ToW Table entry being configured by the other parameters in the record. This entry name should match the entry name configured under Switched Services.

Start Hour & Minute:

Range:	hh = 00 to 23, mm = 00 to 59
Default:	00:00
Description:	Specifies the start time of the interval in the format hh:mm, where hh is the start hour and mm is the start minute. All intervals configured in an entry must not overlap. Intervals configured in different entries can overlap.

Duration:

Range:	dd = 00 to 06, hh = 00 to 23, mm = 00 to 59.
Default:	00:00:00
Description:	Specifies the duration of the interval starting from the configured start time, in the format dd:hh:mm where dd is the end day, hh is the end hour, and mm is the end minute. To check that the end time of the interval is as desired, boot the table and check the Time of Week intervals under the statistics menu.

Start Days

Range:	DDD = one of the following: MON, TUE, WED, THU, FRI, SAT, SUN
Default:	MON
Description:	Specifies the days to which the interval applies in the format DDD or DDD+DDD+DDD, where the following are format definitions: • DDD - Specifies the day. • DDD+DDD+DDD - Specifies that the interval starts on each of these days. The + operator implies “and.” You can specify a maximum of 7 days.

LAN Connections

Introduction

This section describes LAN Connections, the LAN Connection Table you use to configure LAN Connections, and LANView of the WAN, which allows you to group LAN Connections. Use the LAN Connection Table to configure:

- On Demand SVCs
- Dial on Demand SVCs
- Parallel SVCs (Bandwidth on Demand)
- Traffic Priority
- Protocol Priority

Theory of Operation

A key concept in the VanguardMS WAN routing model is that the router connects to virtual circuits. A virtual circuit is an X.25 Switched Virtual Circuit (SVC) or Permanent Virtual Circuit (PVC) or a Frame Relay DLCI. The virtual circuit used to carry traffic between LANs is called a LAN connection or LCON. See the *Vanguard Router Basics Manual* (Part Number T0100-01) for more information on LCONs and the WAN routing model.

Most other bridge and router manufacturers configure WAN links based on physical circuits only. In the VanguardMS model, configuration of a router WAN link has two steps:

Step	***Action***
1	Map a router interface to an LCON.
2	Map the LCON to a particular virtual circuit.

The same X.25 addressing model used to establish virtual circuits for serial traffic is used to establish the LCON virtual circuits for LAN interconnection. The WAN adapter module in each VanguardMS node is X.25 subaddress 94. For example, a node 100 establishes an LCON virtual circuit to node 200 by establishing an X.25 SVC to address 20094. These SVCs are established whenever the calling node reboots.

■ **Note**

SVCs are described beginning on “Switched Virtual Circuits (SVCs)” section on page 1-4.

LANView of the WAN (Adding Dial Connections to a Node)

Introduction

The LANView feature provides flexible configuration of all virtual circuits over the WAN port for either single or multiple IP interface addresses.

LANView can map several SVCs/PVCs to a single Router Interface. This is useful for adding new Vanguard nodes at branch sites, or when adding Dial on Demand or Bandwidth on Demand connections to a node. Configuring a Wide Area Network as a single IP network avoids costly workstation and PC reconfigurations.

LANView allows a group of SVC connections, known as a *LAN Connection Group*, to be mapped to a single IP Router Interface, and thus a single IP network level address. This lets the WAN be treated as a logical LAN, where all nodes on the logical LAN use the same IP network level address.

The LANView of WAN also applies to Router IPX addresses. All WAN SVCs in a LAN Connection Group are considered to be on the same IPX Network Number.

Router Interface

The connection point of any IP forwarder to a network is called a *Router Interface*. A Router Interface has an IP Host address associated with it. This interface address must have its network portion equal to the network number to which it connects.

The LANView feature can map several SVCs/PVCs to a single Router Interface. This is useful for adding new Vanguard device nodes at branch sites, or when adding Dial on Demand or Bandwidth on Demand connections to a node. Configuring a Wide Area Network as a single IP network avoids costly workstation and PC reconfigurations.

LAN Connection Group

A LANView of the WAN allows a group of SVC connections, known as a *LAN Connection Group*, to be mapped to a single IP Router Interface, and thus a single IP network level address. This lets the WAN be treated as a logical LAN, where all nodes on the logical LAN use the same IP network level address.

The LANView of WAN also applies to Router IPX addresses. All WAN SVCs in a LAN Connection Group are considered to be on the same IPX Network Number.

Advantages

The advantage of LANView is that the LANView feature simplifies adding Dial on Demand and Bandwidth on Demand connections to a node.

Limitations

These limitations apply to the LANView feature:

- Bridging traffic *is not* allowed over On Demand SVCs that are part of a LANView. However, Bridging traffic *is* allowed over permanent SVCs that are part of LANView.

LANView Configuration Matrix

The LAN Forwarder Type that you select determines the parameters that appear on the screen. The following table shows a matrix of the allowable combinations. An "X" means that for the LAN Forwarder Type you configured, there is no prompt for the listed parameter.

Parameter Displayed	*For ROUT LAN Forwarder Type*	*For BRID LAN Forwarder Type*	*For BROUT LAN Forwarder Type*
*Router Interface Number	5 to Maximum Configurable	X	5 to Maximum Configurable
Parallel SVCs	0 to 1 Appears if Autocall Mnemonic configured and Encapsulation Type is *not* RFC1294 No prompt appears if LAN Connection Type is GROUP and Next Hop IP Address is 0.0.0.0.	X	0 to 1 Appears if Autocall Mnemonic configured and Encapsulation Type is *not* RFC1294 No prompt appears if LAN Connection Type is GROUP and Next Hop IP Address is 0.0.0.0.
Parallel SVC Threshold	1 to 65534 Appears if Parallel SVCs configured to non-zero value or the Encapsulation Type is RFC 877	X	1 to 65534 Appears if Parallel SVCs configured to non-zero value or the Encapsulation Type is RFC 877
Parallel SVC Port	0 to 32 alphanumeric Appears if Parallel SVCs configured to non-zero value	X	0 to 32 alphanumeric Appears if Parallel SVCs configured to non-zero value
On Demand	ENABLED, DISABLED Appears if Autocall Mnemonic configured and Encapsulation Type is CODEX	X	X
Idle Timeout	0 to 65534 seconds Appears if Encapsulation Type is RFC877, or On Demand is Enabled, or Parallel SVCs are configured	X	X

LANView Example

Typical Application

Figure 2-5 is a common application for LANView over X.25. At the HQ site is a router (Node D) that needs to connect to three other branch nodes (Nodes A to C). The solid line denotes a permanent SVC. The dotted lines denote On Demand SVCs.

In Figure 2-5, Node D has a LANView of the WAN. The WAN is really a logical LAN with an IP network level address of 12.0.0.0. Node D has one IP Router Interface with address 12.0.0.4, which can reach any of the branches (Nodes A to C) via three SVCs tied to the same Router Interface (for example, Interface #5). This example shows that a LANView can be a mix of Permanent and On Demand SVCs.

Without LANView functionality, this same network would require Node D to have three IP Router Interfaces, each with a different IP network level address. With LANView, the same three connections use only one IP network level address.

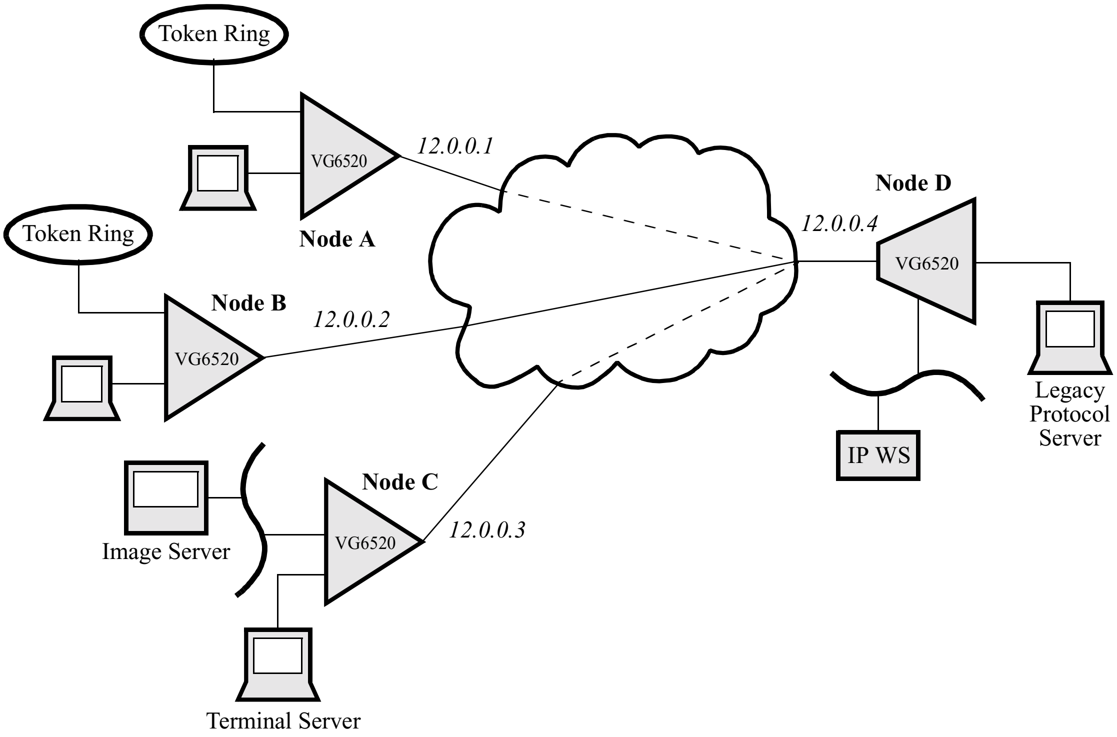


Figure 2-5. LANView for IP Over X.25

LAN Connection Table (Dialing and Priority Features)

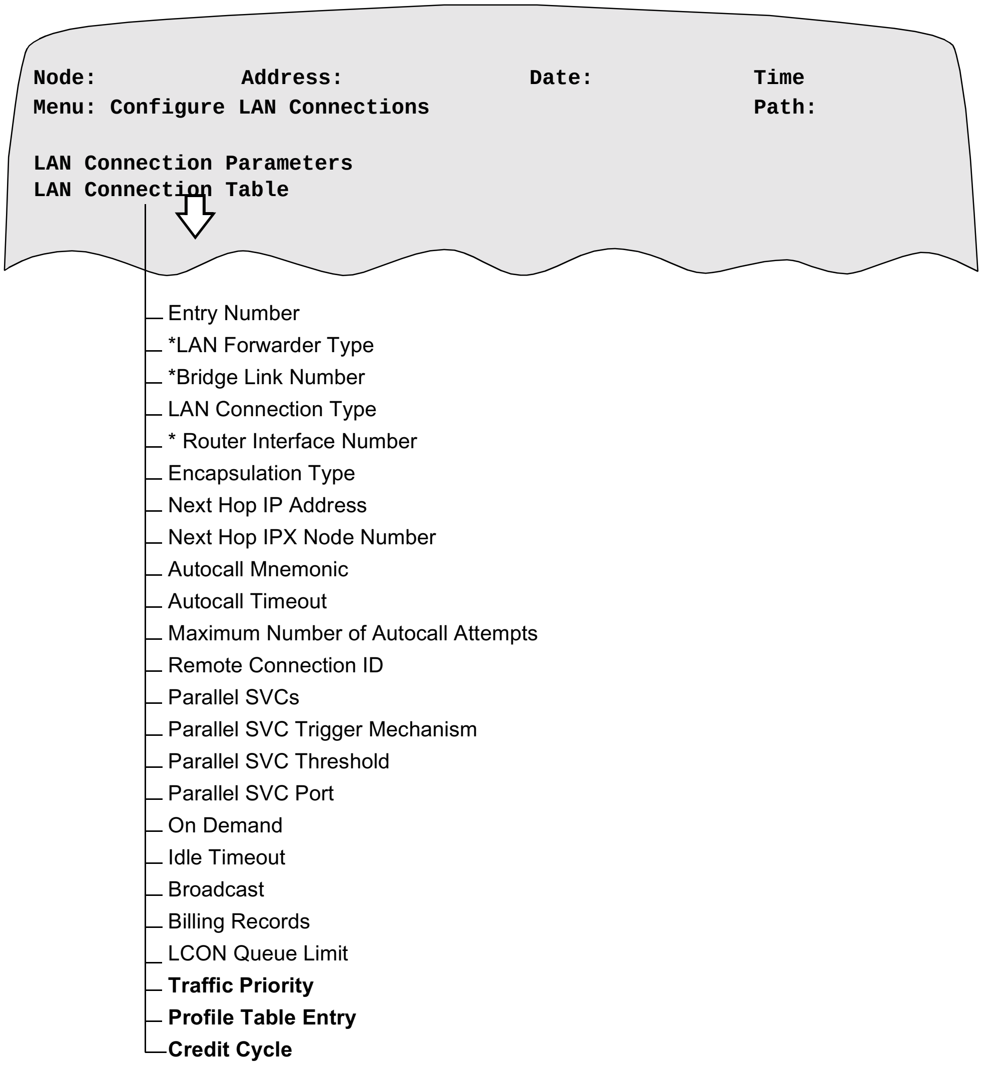
Introduction

The LAN Connection Table is used to configure single and Group LAN Connections that cross over the WAN. These include Dial, Dial on Demand, and Bandwidth on Demand connections, as well as parameters you use to configure priority. You can define up to 254 LAN Connection Table entries.

What You See in This Record

Figure 2-6 displays the LAN Connection Table Record.

.



```
Node:            Address:              Date:            Time
Menu: Configure LAN Connections                         Path:

LAN Connection Parameters
LAN Connection Table
```

Entry Number
*LAN Forwarder Type
*Bridge Link Number
LAN Connection Type
* Router Interface Number
Encapsulation Type
Next Hop IP Address
Next Hop IPX Node Number
Autocall Mnemonic
Autocall Timeout
Maximum Number of Autocall Attempts
Remote Connection ID
Parallel SVCs
Parallel SVC Trigger Mechanism
Parallel SVC Threshold
Parallel SVC Port
On Demand
Idle Timeout
Broadcast
Billing Records
LCON Queue Limit
Traffic Priority
Profile Table Entry
Credit Cycle

Figure 2-6. LAN Connection Table

Configuration Guidelines

Use these guidelines when you configure the LAN Connection Table Record:

- The Bridge Link Number must reference a configured Bridge Link.
- If an Autocall Mnemonic is specified, then the entry must exist in the Mnemonic Table.
- If Billing Records are ON, then a Billing Printer Mnemonic must be specified in the Mnemonic Table.
- If a LAN Connection is to receive calls, there must be an LCON entry in the Routing Table.

Accessing the LAN Connection Table

Follow these steps to access the LAN Connection Table record:

Main -> Configure -> Configure LAN Connections -> LAN Connection Table

LAN Connection Table Parameters

Parameters

Configure the following parameters from the LAN Connection Table Record parameters for configuring Bandwidth Management (BWM) functions. See the *Vanguard Router Basics Manual* (Part Number T0100-01) for more information on LCONs.

■ **Note**

Not all parameters shown in Figure 2-6 are described in these parameter tables.

■ **Note**

Any parameter with an asterisk (*) requires a Node boot. Changes to other parameters require a Table and Node Record boot.

Entry Number

Range:	1 to *n*, where *n* = 32 to 254
Default:	1
Description:	Specifies the entry number used to reference this table record. The allowable range of values reflect the maximum number of LAN connections set in the LAN Connection Parameters menu.

*Router Interface Number

Range:	5 to *n*, where *n* = 36 to 254
Default:	5
Description:	Specifies a Router Interface using this LAN Connection record. This connection makes it possible to pass LAN data through the WAN network to a remote router. The allowable range of values reflects the maximum number of IP or IPX interfaces set in the IP or IPX Parameters Menu. ■ **Note** This parameter appears if the LAN Forwarder Type is configured as ROUT or BROUT.

Parallel SVCs

Range:	0 to 1
Default:	0
Description:	Specifies the maximum number of parallel connections that can be established to the remote destination. Parallel SVCs are established when congestion thresholds are reached on active connections. This parameter appears only if: • LAN Forwarder Type is configured as ROUT/BROUT. • An Autocall Mnemonic name has been specified. • Encapsulation Type is either RFC 877 or CODEX.

Parallel SVC Trigger Mechanism:

Range:	THRESHOLD, PORT_CONGEST
Default:	THRESHOLD
Description:	Specifies which criterion is used to activate or deactivate parallel SVCs. • THRESHOLD - The length of the queue at the LAN-WAN interface determines when to bring up a second link. • PORT_CONGESTION - The port utilization is compared to the configured thresholds to determine when to activate or deactivate a second link. ■ **Note** If you use the PORT_CONGEST value, you must configure the Network Services BoD Table parameters.

Parallel SVC Threshold

Range:	0 to 65534
Default:	8000
Description:	Specifies the number of outstanding data bytes that triggers the use of a Parallel SVC. If this number of data bytes was transmitted without acknowledgment, the receipt of additional data for transmission triggers Parallel SVC use. If a Parallel SVC does not exist, one is established (if the Parallel SVCs parameter is configured to a non-zero value). ■ **Note** Note that this parameter must be configured with a value less than the LCON Queue Limit parameter. ■ **Note** This parameter appears only if the Parallel SVC field is configured to a non-zero value, or if the Encapsulation Type is RFC 877, and parallel SVC Trigger Mechanism is set to THRESHOLD.

Parallel SVC Port

Range:	0 to 32 alphanumeric characters. Use the space character to blank the field.
Default:	blank
Description:	Specifies the port over which the Parallel SVC is established. Allowable values can take one of two forms. The first is a port identifier string. For example, to send the Parallel SVC over port 8: • Type the string **X25-8**. The other form is a Switched Services Table destination name. For example, if the port that the Parallel SVCs come up over is a dial on demand port: **a)** Type the string, **New York**. **b)** In the corresponding entry in the Switched Services Table, map “New York” to any port string, for example, X25-8. ■ **Note** If you the Parallel SVC Port parameter blank, the Parallel SVC is established over the same port as the Primary SVC. This parameter appears only if the Parallel SVC field is configured to a non-zero value.

On Demand

Range:	ENABLED/DISABLED if Encapsulation Type = CODEX
Default:	DISABLED if Encapsulation Type = CODEX. On when Encapsulation Type = RFC 877.
Description:	Specifies whether a circuit is established at system startup or upon receiving data to pass. On Demand SVCs can support IP, IPX, and Asynchronous traffic over X.25 by becoming active when there is data to send and deactivating when all data is sent. This parameter appears only with: • LAN Forwarder Type = ROUT and when the Autocall mnemonic is selected.

*Idle Timeout

Range:	0 to 65535 seconds
Default:	90 seconds
Description:	Specifies the amount of time in seconds the SVC remains connected without passing data before the SVC is deactivated. Any positive value deactivates the On Demand SVC as stated earlier in this document. A zero Idle Timer entry allows the SVC to come up as On Demand, but when there is no more data to send, the link remains active and functions as a Permanent SVC. This parameter appears only with: • LAN Forwarder Type configured as ROUT and, • RFC 877, or CODEX configured with On Demand ENABLED and, when the Autocall mnemonic entered.

You use the following parameters to configure Protocol Priority at the LCON.

Traffic Priority

Range	LOW, MED, HIGH, EXP, LOW-AND-PROTOCOL, MED-AND-PROTOCOL, HIGH-AND-PROTOCOL, EXP-AND-PROTOCOL
Default	HIGH
Description	Specifies the Traffic Priority of this LAN Connection and also enables Protocol Priority depending on the option configured. Available options are: • LOW - Low Priority • MED - Medium Priority • HIGH - High Priority • EXP - Expedite Priority • LOW-AND-PROTOCOL - Low Priority with Protocol priority enabled • MED-AND-PROTOCOL - Medium Priority with Protocol priority enabled • HIGH-AND-PROTOCOL - High Priority with Protocol priority enabled • EXP-AND-PROTOCOL - Expedite Priority with Protocol priority enabled ■ **Note** Changes to this parameter require a Table boot to take effect.

Profile Table Entry

Range	1 to 100
Default	1
Description	Specifies the Protocol Priority profile entry in Network Services.

Credit Cycle

Range	1 to 200
Default	4
Description	Specifies the granularity of traffic forwarding in KBytes. This is the block of byte transfer within which each class has its share depending on its assigned percentage and is used for the bandwidth allocation for each traffic class as configured in the Protocol Priority Profile Table. (For example, If port speed or CIR equals 64000 Kbits, credit cycle equals: 64,000/8 2

Configuring DoD Using the LAN Connection Table

Steps to Configure Dial on Demand

Perform the steps in the table below. Other factors follow the table.

Step	Action
1	Access the LAN Connection Table in the Configure menu.
2	Configure the LAN Connection as On Demand.
3	Configure the autocall mnemonic defined by the LCON to point to a dial port. To do this: a) Access the Mnemonic Table under Switched Services and map the autocall mnemonic to a Destination Node string. b) Access the ROUT table and map the Destination Node string to a Switched Service string. c) Access the Switched Services Table (previously LBU table) and map the Switched Service string to a Dial port. d) Also in the Switched Services Table, configure Link Hold Time, which brings down the physical dial link once the line is idle.

DoD Configuration Considerations

A DoD LAN Connection can be part of a LANView or a point-to-point view.

■ **Note**

DoD ports can be part of the same LANView as other X.25/Frame Relay ports in the same Vanguard device.

You can configure a dial port to serve as:

- Backup port for some links (Use “BKUP”).
- DoD port for some LAN Connections.
- Parallel SVC port for some LAN Connections.

Usage is on a first-come, first-served basis. If backup functionality is operational first, DoD and Parallel SVC support through this port is busied out and unavailable.

You can configure a single Dial port to call up to 64 destinations. Each destination phone number is mapped using LAN Connections (one autocall mnemonic associated with each LAN Connection).

Configuring for Minimal Overhead Traffic

Configure DoD links only when the Router Interface corresponding to this LAN Connection is configured for Static Route IP. This ensures that the link is not brought up for periodic RIP broadcasts.

If the Router Interface passes IPX traffic, you should also configure IPX Static Routes or combine Delta updates with a desirable delay between RIP/SAP updates.

Configuring BoD/IP Load Balancing Using LAN Connection Table

Introduction

This section describes how to configure Bandwidth on Demand and IP Load Balancing using either congestion detection method.

Configuring BoD Based on Queue Threshold

This configuration is consistent with all other Vanguard Products configurations. Perform these steps to configure Bandwidth on Demand based on queue threshold:

Step	*Action*
1	Access the LAN Connection Table menu.
2	Configure the parallel SVC parameter.
3	Configure the parallel SVC Threshold parameter to a suitable congestion level. Once configured, you are prompted for a port entry.
4	Enter a different port to: • Activate a dial link (modem or ISDN). • Direct SVCs over another existing port. ■ **Note** If you leave the left blank, the parallel SVC goes over the same port as the primary SVC.

Queue Threshold Configuration Considerations

Configuration considerations for Bandwidth on Demand based on queue length include the following:

- The number of parallel SVCs initiated to the same next hop destination is configurable up to three.
- Either end of the link can activate the parallel SVC. The number of parallel SVCs that are accepted depends on the encapsulation type. RFC877 encapsulation supports any number of incoming parallel SVCs. CODEX encapsulation accepts only the number of parallel SVCs configured locally.

  Incoming parallel SVCs are used to transmit packets even if parallel SVC support is not configured in the LAN Connection record.
- For dial ports, you must configure the Switched Service Link Hold Time for the physical connection to be terminated.

Configuring BoD Based on Port Utilization

This configuration is consistent with all other Vanguard Product configurations. Perform these steps to configure Bandwidth on Demand based on port utilization:

Step	Action
1	Enable BoD functionality for all ports globally using the Port/Station/ Channel Control menu.
2	Configure the Network Services BoD Table parameters for the primary SVC port. Save the values and exit.
3	Configure the Network Services BoD Table parameters for the secondary SVC port. Save the values and exit.
4	Configure the LAN Connection Table parallel SVC parameters. The parameters that appear depend on the BoD parallel SVC Trigger Mechanism you choose. You must use the following values to configure congestion based on port utilization: • Parallel SVC: **1** • Parallel SVC Trigger Mechanism: **PORT_CONGEST** • Parallel SVC Port: **Any valid port other than the primary** Configure other parameters as appropriate.
5	Boot the node.

Port Utilization Configuration Considerations

Configuration considerations for Bandwidth on Demand based on port utilization (Load Balancing) include the following:

- Idle Time for the parallel SVC must be as large or larger than the Up Hysteresis time on the primary link.
- If BoD is not configured for the primary and secondary ports, load balancing does not work.
- If you specify THRESHOLD for the parallel SVC Trigger Mechanism, Network Services BoD Table configuration is unnecessary and load balancing does not work.

Checking the Load Balancing Configuration

Perform these steps to check that the load balancing configuration is done correctly. If load balancing does not work as described below, check your configuration as follows:

Step	***Action***
1	Send data through the primary SVC so that the link utilization goes beyond the high threshold and stays that way for the period of time configured in the Up Hysteresis parameter.
2	Observe that the parallel SVC activates. Check the BoD statistics field, to see that the primary port is congested. This indicates that load balancing is occurring between the two links.
3	Reduce the traffic over the primary link so that it drops below the low threshold.
4	The BoD statistics show that the primary port is no longer congested. Notice that the parallel SVC remains up, but idle, for however long you have configured in the idle timeout parameter. This is to prevent rapid oscillations.

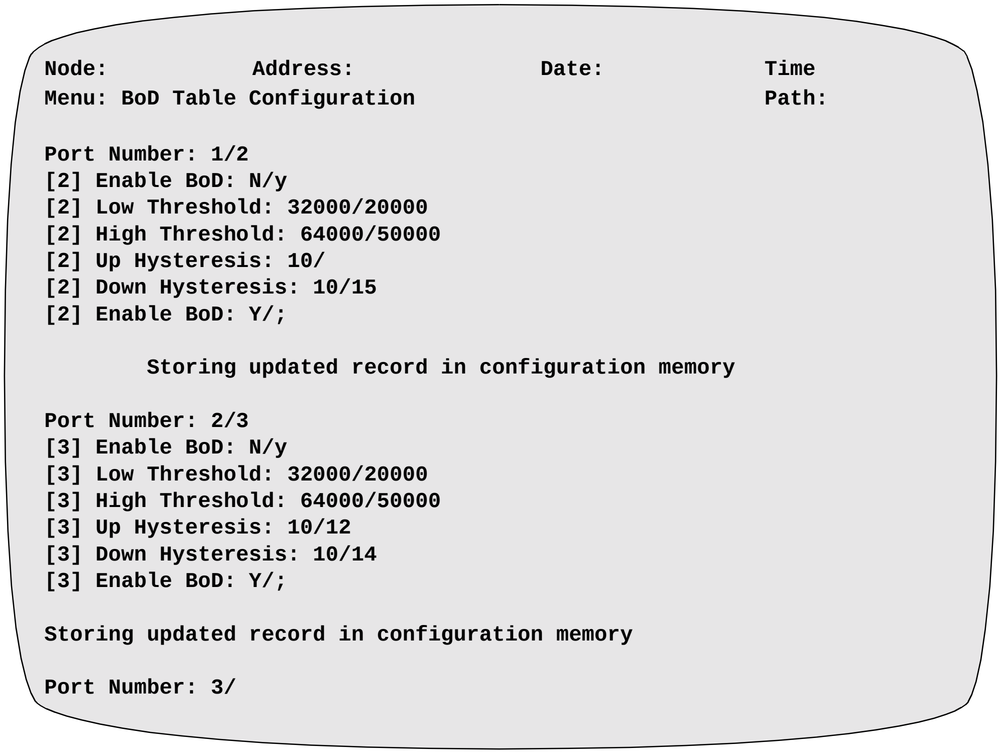
Bandwidth on Demand Table Record

Introduction

This section describes the Bandwidth on Demand Table Record that you access from the Configure Network Services menu. This record provides parameters for configuring the primary and secondary ports (that is, the main link and primary SVC).

What You See in This Record

Figure 2-7 shows the Bandwidth on Demand Table Record and the parameters you use to configure link utilization thresholds and link speed switches.



```
Node:           Address:               Date:            Time
Menu: BoD Table Configuration                           Path:

Port Number: 1/2
[2] Enable BoD: N/y
[2] Low Threshold: 32000/20000
[2] High Threshold: 64000/50000
[2] Up Hysteresis: 10/
[2] Down Hysteresis: 10/15
[2] Enable BoD: Y/;

        Storing updated record in configuration memory

Port Number: 2/3
[3] Enable BoD: N/y
[3] Low Threshold: 32000/20000
[3] High Threshold: 64000/50000
[3] Up Hysteresis: 10/12
[3] Down Hysteresis: 10/14
[3] Enable BoD: Y/;

Storing updated record in configuration memory

Port Number: 3/
```

Figure 2-7. Sample Bandwidth on Demand Table Record

Bandwidth on Demand Table Record Parameters

Parameters

From the Bandwidth on Demand Table, you can configure these parameters:

Port Number

Range:	Platform specific. Refer to the operator’s manual for your unit.
Default:	1
Description:	Specifies the number of the X.25/FRI primary or secondary port you are configuring.

Enable BoD:

Range:	Y, N
Default:	N
Description:	Enables BoD for the port if **Y** is entered and disables BoD if **N** is entered.

Low Threshold:

Range:	0 to 384000
Default:	32000
Description:	When the link goes below this value, the BoD module initiates a switch to a low link speed.

High Threshold:

Range:	0 to 384000
Default:	64000
Description:	When the link utilization goes above this value, the BoD module initiates a switch to a higher link speed.

Up Hysteresis:

Range:	10 to 1200
Default:	10
Description:	This is the hysteresis measured in seconds. The link utilization must cross and stay above the High Threshold value for at least this amount of time for the BoD module to initiate a switch to a lower bandwidth.

Down Hysteresis:

Range:	10 to 1200
Default:	10
Description:	This is the hysteresis measured in seconds. The link utilization must cross and stay above the Low Threshold value for at least this amount of time for the BoD module to initiate a switch to a lower bandwidth.

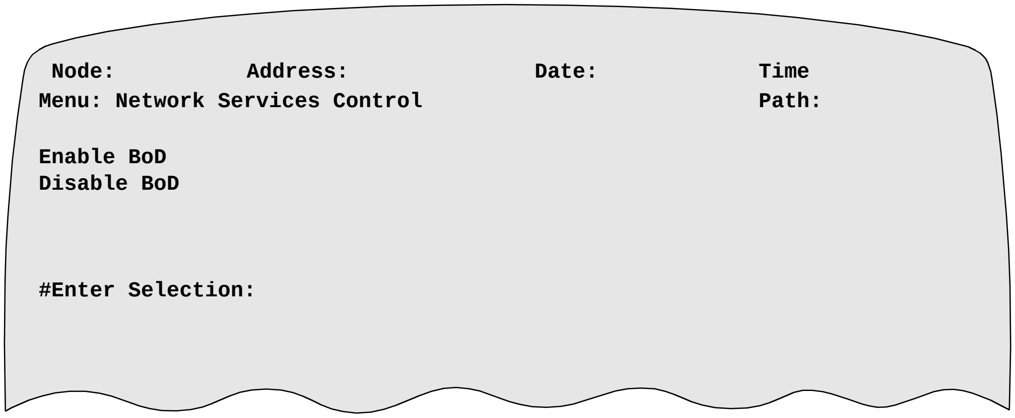
Network Services Control Menu and BoD

Introduction

The Enable BoD parameter in the Network Services Control menu globally enables Bandwidth on Demand across all ports for the node. This parameter appears on the menu as shown in Figure 2-8. The Network Services Control menu is available from the Port/Station/Channel Control menu in the Main menu.

What You See on This Menu

Figure 2-8 shows the Enable BoD and Disable BoD parameters.



```
 Node:          Address:                Date:            Time
Menu: Network Services Control                           Path:

Enable BoD
Disable BoD



#Enter Selection:
```

Figure 2-8. Network Services Control Menu

Enable BoD/ Disable BoD Parameters

The Enable BoD parameter and Disable BoD parameter essentially function as one parameter. Enable BoD enables Bandwidth on Demand on all ports on the node. Disable BoD disables Bandwidth on Demand on all ports on the node.

Enable BoD and Disable BoD

Range:	BoD enabled or BoD disabled
Default:	BoD disabled
Description:	Globally enables or disables Bandwidth on Demand functionality for all ports on the node.

Setting the Enable and Disable BoD Parameters

To set the Enable BoD parameter:

Step	***Action***	***Result/Description***
1	From the Main menu, select the **Port/Station/Channel** menu.	The Port/Station/Channel menu appears.
2	From the Port/Station/Channel menu, select the **Network Services Control** menu.	The Network Services Control menu appears.

Step	***Action** (continued)*	***Result/Description***
3	Type the number of the Enable BoD selection at the **Enter Selection:** prompt, then press ENTER.	The selection number disappears. The Network Services Control menu remains. BoD is enabled globally on all ports. ■ **Note** If BoD is already enabled, when you type the selection number and press ENTER, an error message appears: **ERROR -- BoD is already ENABLED.**

Setting the Disable BoD Parameter

To set the Disable BoD parameter:

Step	***Action***	***Result/Description***
1	From the Main menu, select the **Port/Station/Channel** menu.	The Port/Station/Channel menu appears.
2	From the Port/Station/Channel menu, select the **Network Services Control** menu.	The Network Services Control menu appears.
3	Type the number of the Disable BoD selection at the **Enter Selection:** prompt, then press ENTER.	A message appears: **Caution--This would cease to BoD operation for all ports.** **Proceed (y/n):**
4	Type **y**, then press ENTER.	The selection number disappears. The Network Services Control menu remains. BoD is disabled globally for all ports on the node.

Limitations

The following limitations apply to the Bandwidth on Demand feature:

Sequencing

- Applications that do not run with a transport layer such as TCP can experience problems with out of order packets. Sequencing is assumed to be the responsibility of the transport layers of the external devices.
- IPX traffic sent over a LAN Connection configured as ROUT can cause problems with packets arriving out of sequence. Hence, the packets are transmitted over the primary SVC only.

Frame Relay

- Parallel SVCs for IP are not supported over Frame Relay networks since Frame Relay uses PVCs.

Route Selection Table Record

Introduction

You select the links over which calls are routed in the Route Selection Table. You can configure the Route Selection Table record to do the following:

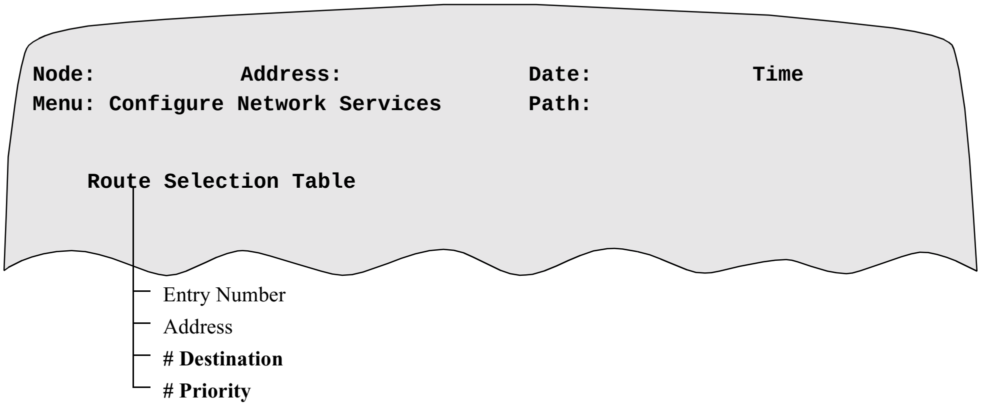
- Route calls to a specified node or port in the network.
- Implement load sharing.
- Implement alternate routing.
- Choose port priority to handle call routing.

■**Note**

Routing features are described beginning on page 1-25.

What You See in This Record

Figure 2-9 illustrates the Route Selection Table:



```
Node:            Address:              Date:            Time
Menu: Configure Network Services       Path:


    Route Selection Table
```

Figure 2-9. Route Selection Table Record

Configuration Guidelines

When you configure the Route Selection Table Record, use these guidelines:

- No blank Address values
- No duplicate Address values
- No duplicate Destination values
- Destination and Priority entries repeat for all ports (each entry can contain eight Destination/Priority pairs, unless you use a CSK to increase limit to 16 destinations).
- Configure a separate Route Selection Table entry for all possible call destinations, including calls that originate at terminals connected to the node, and calls that are received by a node and sent to another node. Local PAD ports and local modules are the exception.

Accessing the Route Selection Table Record

Follow these steps to access the Route Selection Table:

Main -> Configure -> Configure Network Services -> Route Selection Table

Route Selection Table Record Parameters

Introduction

This section describes the Route Selection Table Record parameters that apply to Bandwidth Management functionality.

■ **Note**

Changes to parameters in this table require a Table and Node Boot to take effect.

Parameters

From the Route Selection Table Record, you can configure the following parameters (with the exception of Entry Number):

Entry Number

Range:	1 to 128
Default:	1
Description:	Identifies the particular Route Selection Table entry being configured by the other parameters in the record.

Address

Range:	0 to 15 digits
Default:	(blank); using the default causes this parameter to be ignored.
Description:	Specifies the Network Address for calls routed beyond this node. • Enter an asterisk (*) as a wildcard to match anything. • A Route Selection Table entry is not needed for calls destined for the local node. Use the space bar to blank the parameter value.

#1 Destination

Range:	0 to 32 alphanumeric characters. Use the space bar to blank the parameter value.
Default:	(blank); using the default causes this parameter to be ignored
Description:	Specifies the network address to which calls are routed. By default you can configure up to eight destinations per entry. You can use a CSK to increase the limit to 16 destinations per entry. Addresses for different port types can be entered in the following formats where: • *x* is the port number, • *y* is the station number, and • *z* is the channel number. Protocol address types include: • X25-*x* – For example, to route calls to X.25 port 1, type X25-1. • SDLC-*x*S*y* – For example, to route calls to SDLC port 2, station 4, type SDLC-2S4. • FRI-*x*S*y* • MX25-*x*S*y* • BSC3780-*x* • BSC3270-*x* • NCRBSC-*x*

Priority

Range:	0 to 15
Default:	1
Description:	Specifies the priority for call forwarding to ports within this Route Selection Table. A combination of priority and load conditions determines call forwarding. • 0 is backup port • 1 is highest priority • 15 is the lowest priority A priority can be assigned for each port and appears on the screen as #1 Priority, #2 Priority, and so on. These correspond to the Destination parameter values (#1 Destination, #2 Destination, and so on). Note the following guidelines: • The backup port is selected only when all other ports with other priorities are unavailable or down, as opposed to busy. • Do not set the priority to 0 (zero) if this port is to be configured as a Link backup port (in the Switched Services Table Record). • After you type a priority value (or press ENTER), the next Destination appears and then the next Priority. This sequence repeats until you have entered all the Destination and Priority values or until you type a semi-colon (;) to implement the values or press ESC to abort the process.

Node Record

What You See in This Record

The Node Record contains parameter values that define the node characteristics. It specifies many key node values, including node name, address, thresholds, and timers. You can use the Node Record to configure bandwidth management parameters such as:

- CPU, Buffer, and Port utilization thresholds
- Traffic Priority
- Data Connection Protection

Listed below are the Node Record parameters that effect Bandwidth Management. For more information on configuring a node and Node Record parameters, see Appendix A, *Vanguard Basic Configuration Manual* (Part Number T0113).

- Buffer Utilization Threshold
- CPU Utilization Threshold
- DCP Facility (DCP Only)
- Traffic Priority
- Traffic Priority Step
- Node switched services security password
- DC enable facility
- DC negotiate facility
- Max Switch Service Entries

Accessing the Node Record

Follow these steps to access the Node Record:

Main -> Configure -> Node

Node Record Parameters

Introduction

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

■ **Note**

Changes to parameters in this table require a Table and Node Boot to take effect.

Parameters

From the Node Record, you can configure the following BWM parameters:

Port Utilization Threshold (%)

Range:	10 to 99
Default:	75
Description:	A percentage of the port's capacity specifying how much data traffic can be handled relative to port speed before triggering a medium-severity alarm.

Buffer Utilization Threshold (%)

Range:	10 to 99
Default:	75
Description:	Specifies the percentage of the buffer that can be used before triggering a medium-severity alarm.

CPU Utilization Threshold (%)

Range:	10 to 99
Default:	75
Description:	Specifies the percentage of the CPU that can be used before triggering a medium-severity alarm.

DCP Facility (Data Connection Protection)

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

*Traffic Priority

Range:	LOW, MED, HIGH, EXP
Default:	MED
Description:	Default traffic priority used on this node: • LOW: One Low Priority packet is sent for every Traffic Priority Step number of Medium priority packets. • MED: One Medium priority packet is sent for every Traffic Priority Step number of High priority packets. • HIGH: High is the first level of priority packets sent, if no expedite priority packets are sent. • EXP: Expedite priority packets have the highest priority and use all of the link bandwidth that they need. Any remaining bandwidth is shared by the high, medium, and low priority packets.

*Traffic Priority Step

Range:	1 to 65000
Default:	8
Description:	Specifies the number of packets that a higher priority queue sends (as long as it has packets queued) before one packet in the next- lower priority queue is sent. This global parameter applies to all networking links in the node.

Node Switched Services Security Password

Range:	0 to 9 alphanumeric characters
Default:	(blank)
Description:	This password is used by switched services security for verification when determining if a call should be allowed to come up. ■**Note** Use the space character to blank the field.

DC enable facility

Range:	10 to 61
Default:	61
Description:	Specifies the Class A facility used to carry the Data Compression and enables configuration information at call setup time in Call Request and Call Accept packets through the network.

DC negotiate

Range:	62
Default:	10 to 62
Description:	This defines the Class A facility used to carry the Data Compression-negotiate configuration information at call setup time in Call Request and Call Accept packets through the network.

Max Switch Service Entries

Range:	1 to 1024
Default:	200
Description:	Specifies the maximum permitted number of Switch Service entries. The value of this parameter determines the maximum entry number for new table entries. It may be necessary to increase this size parameter value before adding new table entries.

PAD Port Record

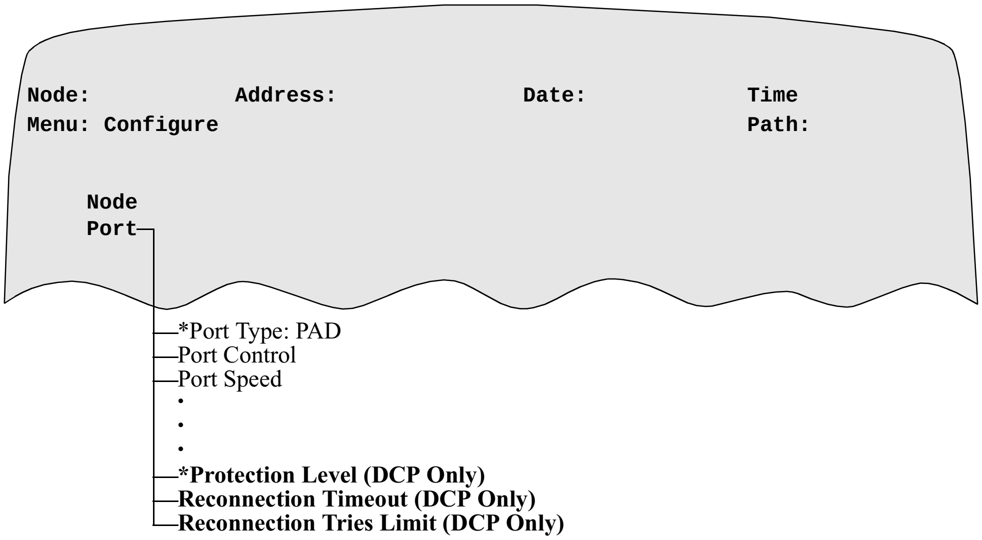
Introduction

A Packet Assembler/Disassembler (PAD) port type lets you transmit asynchronous data. Selecting a port type of PAD causes the remainder of the Port Record to contain only those parameters needed for configuring a PAD port.

Use this record to configure parameters for Data Connection Protection (DCP):

What You See in This Record

Figure 2-10 shows the PAD port configuration parameters that apply to Bandwidth Management in bold. Not all PAD configuration parameters are included.



```
Node:            Address:               Date:            Time
Menu: Configure                                          Path:

     Node
     Port
```

- *Port Type: PAD
- Port Control
- Port Speed
- .
- .
- .
- ***Protection Level (DCP Only)**
- **Reconnection Timeout (DCP Only)**
- **Reconnection Tries Limit (DCP Only)**

Figure 2-10. PAD Port Record

Accessing the Record

Follow these steps to access the PAD Port Record:

Step	***Action***	***Result***
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **Port** from the Configure menu and type the Port Number in the Port Record.	
3	Type **PAD**, the port type.	The first parameter for PAD Port Type appears, as shown in Figure 2-10.
4	Enter each parameter value and save the record. Press ESC to return to the Configure menu.	

PAD Port Record Parameters

Introduction

This section describes the PAD port parameters that apply to Bandwidth Management functionality. Any parameter with an asterisk (*) requires a Node boot.

■ **Note**

Changes to this record require a Port Boot to take effect, unless otherwise noted.

Parameters

From the PAD port record, you can configure the following parameters

*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. Valid only when the Data Connection Protection Option has been purchased for this node. ■ **Note** Changes to this parameter require a Node Boot to take effect.

Reconnection Timeout

Range:	1 to 128
Default:	2
Description:	Specifies how many seconds the Data Connection Protection feature waits between reconnection attempts: • The call originator determines the value. • If symmetric operation is required, the Reconnection Timeout and the Reconnection Tries limit should be equal. • Valid only when the Data Connection Protection Option has been purchased for this node.

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. • The call originator determines the value. • If 0 is entered, there is no attempt to reconnect. If symmetric operation is required, the Reconnection Timeout and the Reconnection Tries limit should be equal. • Valid only when the Data Connection Protection Option has been purchased for this node.

X.25 Port Record

Introduction

A Port Type of X.25 allows the port to be connected to another, usually high-speed, device such as another Vanguard Products device or a network.

Selecting a port type of X.25 causes the remainder of the Port Record to contain only those parameters needed for configuring an X.25 port. Default parameter values for the parameters are generally correct for most applications.

You can use the X.25 Port Record record to configure bandwidth management parameters for:

- Data Connection Protection
- Link address Negotiation

Features

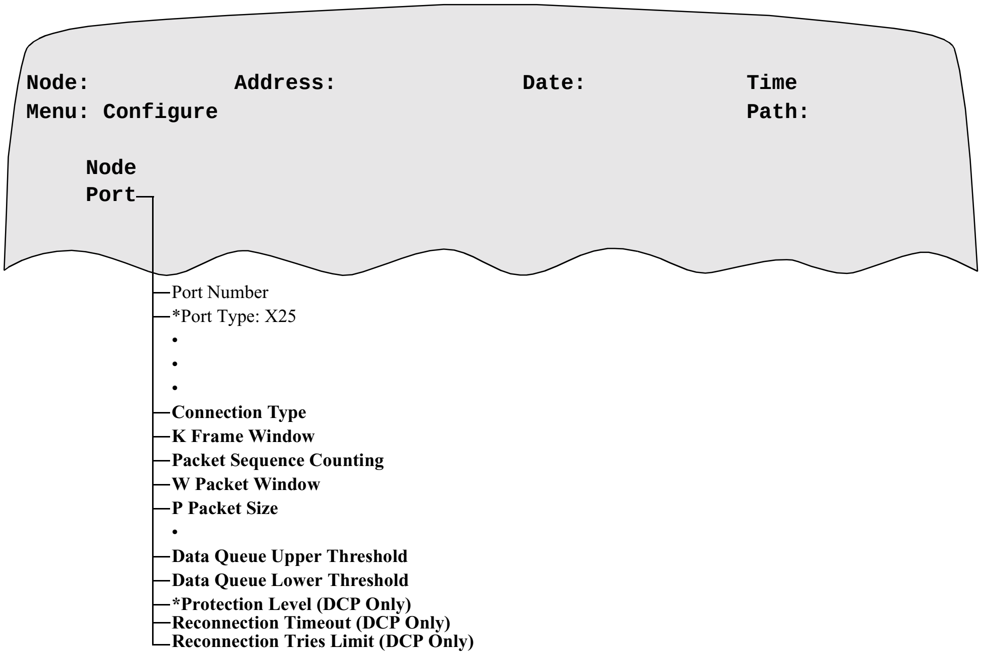
The Dial on Demand Bandwidth Management feature can be implemented when you configure a port as X.25.

What You See in This Record

Figure 2-11 primarily shows the X.25 port configuration parameters that are discussed in the remainder of this chapter. Parameters that apply to Bandwidth Management functionality appear in bold.

■Note

Not all X.25 port configuration parameters appear in Figure 2-12.



```
Node:           Address:              Date:            Time
Menu: Configure                                        Path:

    Node
    Port
         —Port Number
         —*Port Type: X25
           •
           •
           •
         —Connection Type
         —K Frame Window
         —Packet Sequence Counting
         —W Packet Window
         —P Packet Size
           •
         —Data Queue Upper Threshold
         —Data Queue Lower Threshold
         —*Protection Level (DCP Only)
         —Reconnection Timeout (DCP Only)
         —Reconnection Tries Limit (DCP Only)
```

Figure 2-11. X.25 Port Record

Configuring X.25 Port Record Parameters for Bandwidth Management

Introduction

This section describes the X.25 Port Record parameters that must be considered when you configure the X.25 Port Record for Bandwidth management..

■ **Note**
Changes to parameters in this record require a Port Boot to take effect. Any parameter with an asterisk (*) requires a Node boot.

Parameters

From the X.25 Port Record, you can configure these parameters:

*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 Valid only when the Data Connection Protection Option has been purchased for this node. ■ **Note** A Node boot is required for the change to take effect.

Reconnection Timeout

Range:	1 to 128
Default:	2
Description:	Specifies how many seconds the Data Connection Protection feature waits between reconnection attempts. 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 0 is entered, there is no attempt to reconnect. This parameter is valid only when the Data Connection Protection Option has been purchased for this node.

Link Address Negotiation Configuration Using the X.25 Port

Introduction

Link Address Negotiation for Dial on Demand (DoD) is part of X.25 support for Vanguard. It allows your Vanguard with DoD nodes to negotiate DCE or DTE link addressing at both ends of a link. For more information on this feature, see the *X.25 Configuration Basics Manual* (Part Number T0107).

How to Configure the Negotiate Link Address Feature

You can use this feature during X.25 port configuration.

Follow these steps to configure Link Address Negotiation:

Step	***Action***	***Result***
1	Select **Configure** from the CTP Main menu.	The Port Configuration record appears.
1	Select **Port** from the Configure menu.	The port configuration parameters appear.
2	Set the Port Number you want to use and define the Port Type as **X.25**.	The next parameter appears.
3	Use the ENTER key to move to the Link Address parameter, set it to **Negotiate.**	This sets the port configuration for the node to negotiate the link address each time a link is being established.
4	Perform a Port boot to implement your changes.	

How X.25 Port and FRI Station Parameters Effect Traffic Flow

Introduction

To fully understand traffic priority performance, it is important to understand how other X.25 port and FRI Station parameters can effect the traffic flow. The following configurable parameters effect traffic priority:

- K Frame Window
- W Packet Window
- P Packet Size
- Data Queue Upper Threshold
- Data Queue Lower Threshold
- X.25 option INL

K Frame Window

The K Frame Window specifies the number of unacknowledged frames that can be outstanding at Layer 2. When there is a high link delay, setting this parameter to a high number improves throughput but could cause more lower priority frames to be queued in front of a high priority frame in the X.25 Layer 2.

For example, if the window size is set to 7 and an acknowledgment is received for the previous seven frames, Layer 3 sends seven more frames to Layer 2. If there are only low priority frames, Layer 3 sends seven low priority frames to level 2 to fill the window. Now if a higher priority frame is received by Layer 3, it is not transmitted until all of the seven lower priority frames are transmitted.

Recommendation:

If the lower priority traffic has a large frame size, you may want to set the K frame window to a low value, but be careful of the end-to-end delay.

W Packet Window

The W Packet Window specifies the number of outstanding packets on a VC. Reaching the window limit on a VC halts the flow of data frames for that VC and allows lower priority VC data frames to be transmitted.

Recommendation:

Increase the value of this parameter from the default value of 2 for the higher priority VC, if possible.

P Packet Size

The P Packet Size specifies the packet size. The larger this parameter, the longer it takes to transmit the lower priority packets that are in front on the higher priority packet. When this parameter is smaller, other parameters could have a greater effect on Traffic Priority.

Recommendation:

Having a small packet size for lower priority traffic decreases the delay that occurs when high priority traffic gets behind the lower priority traffic in the various queues.

Data Queue Upper/ Lower Thresholds

The Data Queue Upper parameter specifies the maximum number of data packets a VC can queue for transmission before X.25 layer 3 invokes flow control to the attached channel.

The Data Queue Lower parameter specifies the number of queued data packets ready for transmission that must be reached before the X.25 layer 3 releases flow control to the attached channel.

A larger Data Queue Upper Threshold parameter allows more lower priority packets to be received by X.25 layer 3 and queued up in X.253 and X.252. Once flow control is invoked, having a small Data Queue Lower Threshold could reduce the data queues for higher priority packets, even when the attached channel has packets to send. This can result in sending lower priority packets in front of higher priority packets.

Recommendation:

Increase both of these parameters from the default value. Increasing the threshold parameters reduces the possibility of the higher priority channel queues from drying up in the X.25 layer 3.

■ **Note**

For more information on configuring Vanguards to use X.25, see the *X.25 Configuration Basics Manual* (Part Number T0107).

Chapter 3
Bandwidth Management Statistics

Overview

Introduction

This chapter describes the statistics provided for Bandwidth Management features.

Switched Services Table Statistics

Function

The Switched Services Table Statistics screen provides detailed information about Switched Services and Link Backup operation.

Guideline for Use

The information appearing on the Switched Services screen depends on how you use Switched Services and the LBU CSK. You can only obtain LBU statistics if Link Backup has been purchased and enabled for the node.

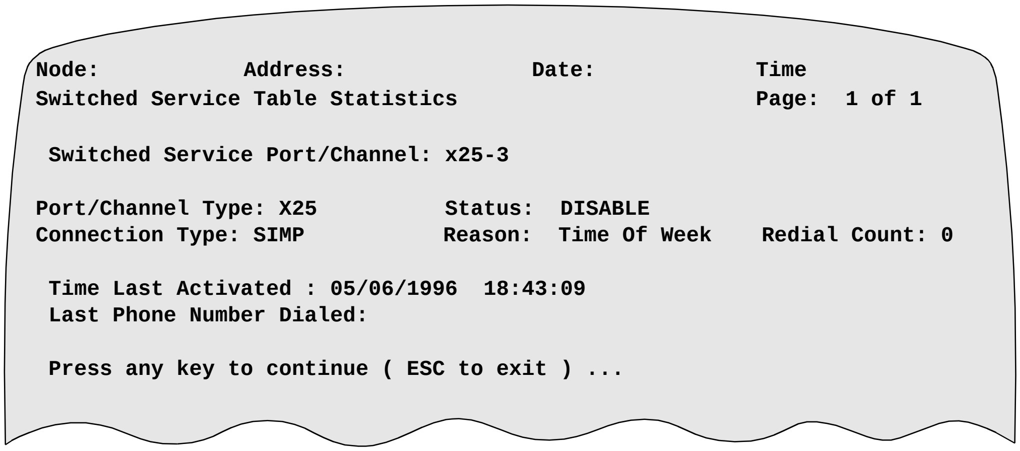
Accessing Switched Services Table Statistics

Use the following procedure to access Switched Services Table statistics:

Main -> Status/Statistics -> Networks Services Stats -> Switched Services Table Stats

What You See in This Screen

Figure 3-1 shows an example of the Switched Services Statistics screen.



```
Node:            Address:              Date:            Time
Switched Service Table Statistics                       Page:  1 of 1

 Switched Service Port/Channel: x25-3

Port/Channel Type: X25          Status:  DISABLE
Connection Type: SIMP           Reason:  Time Of Week    Redial Count: 0

 Time Last Activated : 05/06/1996  18:43:09
 Last Phone Number Dialed:

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

Figure 3-1. Example of Switched Services Statistics Screen

Screen Terms

The Switched Services Statistics screen contains this information:

Term	*Indicates*
Port Channel	Number of the Switched Service/Backup port
Port Channel Type	Type of port or channel (X.25, SDLC, FR, and so on)
Connection Type	EIA connection type set in the port record
Status	Dialing status of the Switched Service/Backup Port: • *Up*: Indicates that the link is active. • *Idle*: Indicates that the link is not active. • *Activating*: Indicates the link is configured and dialing. • *Disable*: Implies that the switched/backup port is both Dial-in and Dial-out disabled. • *Dial-in Disable/Dial-out Disable*: Implies that the switched/backup port is either Dial-in disabled or Dial-out disabled.
Reason	Reason for port activation: • *Failure*: A link failure occurred on a monitored port. • *Call*: A call was made from the Switched Service/ Backup port. • *Remote*: A call was made to the Switched Service/ Backup port. • *CTP*: Switched Service/Backup port was activated from the control terminal. • *None*: Switched Service/Backup port is deactivated or about to be deactivated. • *Time of Week*: A configured ToW interval is in effect.
Redial Count	Number of Redial attempts made after the Redial Timer has expired.
Calls Accepted	Number of calls passing configured security checks.
Calls Rejected	Number of calls rejected because of security violations.
Time Last Activated	The last time the Switched Service/Backup port was activated.
Last Phone Number Dialed	The last phone number the Switched Service/Backup port dialed.
Monitored Port(s) Summary	Port summary including: • Ports being monitored by the Switched Service/ Backup port for link failure or congestion. • State of each monitored port (up, down, congested). • Phone number that the Switched Service/Backup port dials when a monitored port has a link failure or congestion.

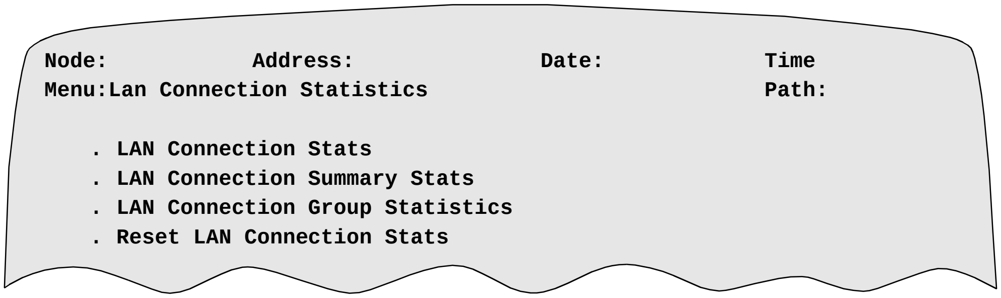
LAN Connection Statistics

Function

The LAN Connection Statistics menus provides options for viewing various LAN Connection statistics.

What You See in This Screen

Figure 3-2 shows the LAN Connection Statistics menu. Select the appropriate number to view a particular screen.



```
Node:            Address:              Date:            Time
Menu:Lan Connection Statistics                          Path:

   . LAN Connection Stats
   . LAN Connection Summary Stats
   . LAN Connection Group Statistics
   . Reset LAN Connection Stats
```

Figure 3-2. LAN Connection Statistics Menu

Selections

The LAN Connection Statistics menu provides these LAN statistics options:

Menu Option	*Displays*
LAN Connection Stats	Detailed transmit and receive statistics for primary and Parallel SVCs.
LAN Connection Summary Stats	An overall picture of the LANView indicating which connections are currently active.
LAN Connection Group Statistics	A single line of address information for each next hop destination in a LAN Connection Group.

LAN Connection Group Statistics

Function

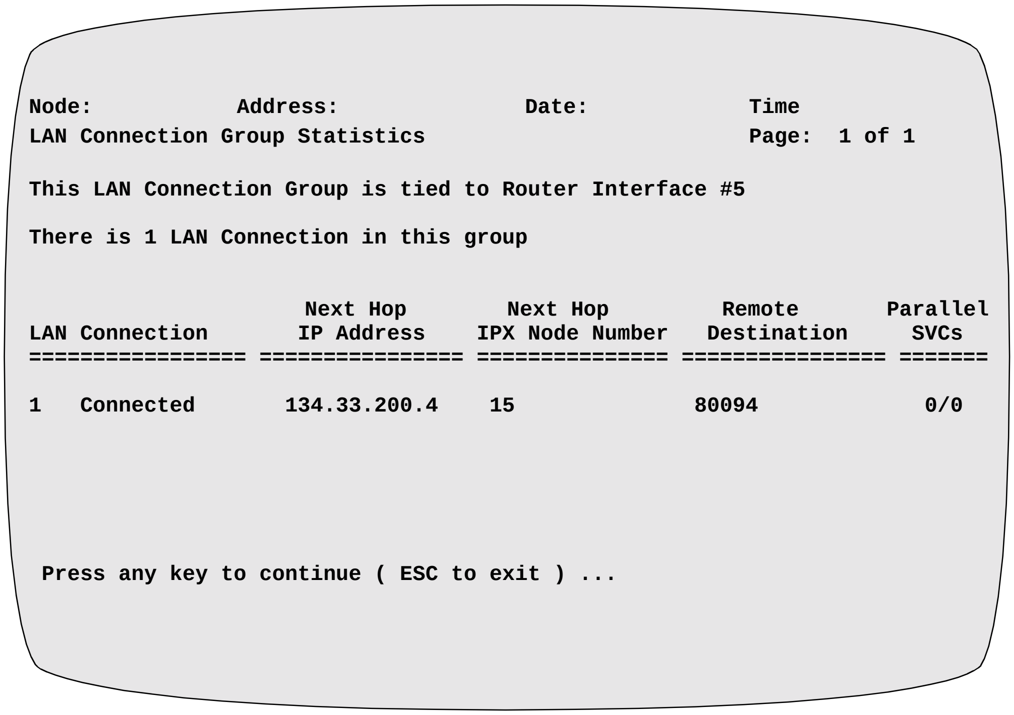
When you select LAN Connection Group Statistics, the Vanguard device prompts for:

- A Router Interface number corresponding to the LAN Connection Group
- Which Group to display, if multiple Groups exist on this Router Interface. This is based on IP/IPX Network Addresses configured for the interface.

Once you provide this information, a statistics screen appears displaying a single line for each next hop destination in the LAN Connection Group.

What You See In This Screen

Figure 3-3 shows an example LAN Connection Group Statistics screen.



```
Node:            Address:              Date:            Time
LAN Connection Group Statistics                         Page:  1 of 1

This LAN Connection Group is tied to Router Interface #5

There is 1 LAN Connection in this group


                     Next Hop        Next Hop         Remote       Parallel
LAN Connection      IP Address    IPX Node Number   Destination     SVCs
================ ================ =============== ================ =======

1   Connected       134.33.200.4    15             80094             0/0



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

Figure 3-3. **LAN Connection Group Statistics Screen Example**

Screen Terms

The LAN Connection Group Statistics screen contains this information:

Term	***Indicates***
Parallel SVCs	Number of Parallel SVCs currently configured/ established.
Next Hop Address	An IP address or IPX node number, or both.
Remote Destination	An X.21 address or Frame Relay Port/Station/DLCI.
Parallel SVCs	Number of Parallel SVCs currently configured/set.

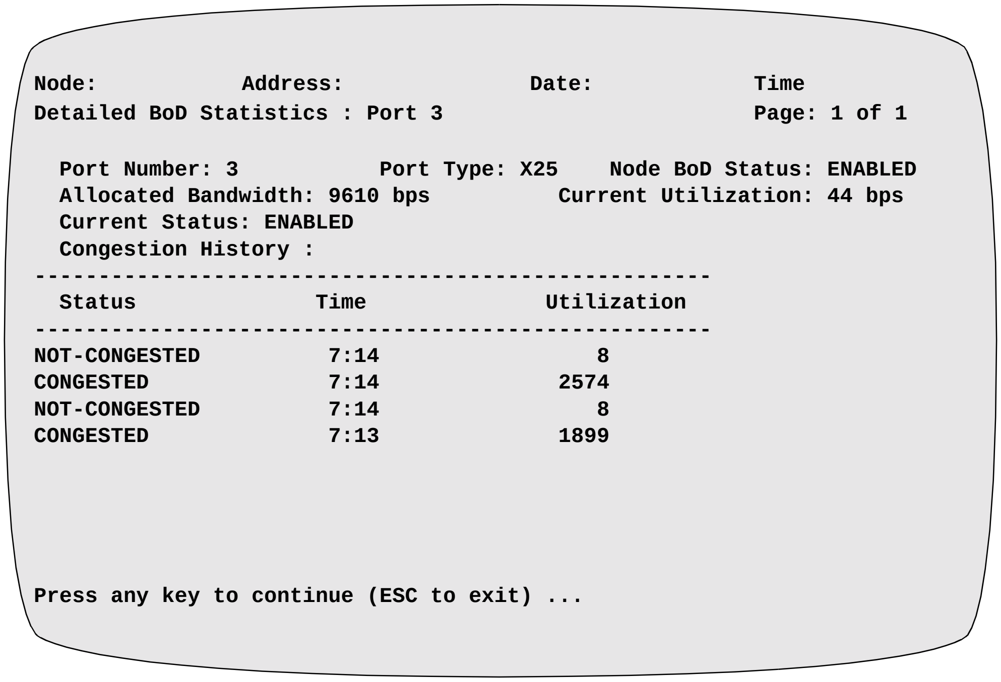
Bandwidth on Demand Statistics

Introduction

This section describes Bandwidth on Demand statistics.

What You See in This Screen

Figure 3-4 shows the Detailed BoD Statistics screen:



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

  Port Number: 3           Port Type: X25    Node BoD Status: ENABLED
  Allocated Bandwidth: 9610 bps          Current Utilization: 44 bps
  Current Status: ENABLED
  Congestion History :
-----------------------------------------------------
  Status              Time             Utilization
-----------------------------------------------------
NOT-CONGESTED          7:14                8
CONGESTED              7:14             2574
NOT-CONGESTED          7:14                8
CONGESTED              7:13             1899





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

Figure 3-4. Detailed BoD Statistics Screen

Screen Terms

The Detailed BoD Statistics screen contains the following information:

Term	Indicates
Port Number	Shows the number of the port displaying statistics.
Port Type	Shows the value of the Port type.
Allocated Bandwidth	Shows speed of the link. Because of calculations done by the hardware, this is not always a multiple of 100.
Current Utilization	Monitors utilization on the port. The IP Load Balancing feature looks at this parameter when deciding on which SVC to put the packet. This value is updated every three seconds.
Current Status	Shows the BoD configuration for this port. Values are: ENABLED or DISABLED.
Node BoD Status	Reflects the value of the BoD status as configured in the Port Station Channel Control/Network Services menu.
Congestion History	Lists the history of the last 10 congested/non-congested state changes. The current state is that specified in the first line of the list. For example, Port 3 is currently out of congestion. Utilization is measured when the state change occurs.

Index