Configuring Frame Relay Services

BayRS Version 12.00
Site Manager Software Version 6.00

Part No. 117376-A Rev. A
September 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Figures

Tables

About This Guide

If you are responsible for configuring frame relay, you need to read this guide.

If you want to	Go to
Start frame relay on a router and get it running with default settings for parameters	Chapter 1
Learn about the frame relay protocol and special aspects of the Bay Networks implementation of frame relay	Chapter 2
Change default settings for frame relay parameters	Chapter 3
Obtain information about Site Manager parameters (this is the same information you obtain using Site Manager online Help)	Appendix A
View default settings for all frame relay parameters	Appendix B

Before You Begin

Before using this guide with a new router, you must complete the following procedures:

- Install the router (see the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7–11.xx to Version 12.00*.

Conventions

bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
	Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is
	show at routes | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
B_c	committed burst rate
B_e	excess burst
BECN	backward explicit congestion notification
BofL	Breath of Life (message)
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
C/R	command/response bit
CIR	committed information rate
CRC	cyclic redundancy check
DCE	data communications equipment
DE	discard eligibility
DLCI	data link connection identifier
DLCMI	Data Link Control Management Interface
DTE	data terminal equipment
EA	extended address bit
FECN	forward explicit congestion notification
FTP	File Transfer Protocol
HSSI	High-Speed Serial Interface
IP	Internet Protocol
IPX	Internet Packet Exchange
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union–Telecommunications (formerly CCITT)
LAN	local area network
LMI	Local Management Interface
MAC	media access control
OSI	Open Systems Interconnection
PRI	Primary Rate Interface
PVC	permanent virtual circuit

QofS	quality of service
VC	virtual circuit
URL	uniform resource locator
WAN	wide area network
WCP	WAN Compression Protocol
XNS	Xerox Networking System

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone--U.S./Canada: 888-422-9773
- Phone--International: 510-490-4752
- FAX--U.S./Canada and International: 510-498-2609

The Bay Networks Press catalog is available on the World Wide Web at *support.baynetworks.com/Library/GenMisc*. Bay Networks publications are available on the World Wide Web at *support.baynetworks.com/Library/tpubs*.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Chapter 1
Starting Frame Relay

The quickest way to begin using frame relay on your network is to enable it with default values for all interface parameters and with a default service record. The sections that follow describe this procedure.

Preparing a Configuration File

To prepare a configuration file:

1. **Create and save a configuration file that has at least one WAN interface.**
2. **Retrieve the configuration file in local, remote, or dynamic mode.**
3. **Specify router hardware if this is a local-mode configuration file.**

Starting Frame Relay

To enable frame relay:

1. **Select a link- or net-module connector that requires a WAN circuit.**

2. **Specify frame relay as the WAN protocol by completing the tasks in the following table.**

Site Manager Procedure	
You do this	**System responds**
1. Choose a link or net module.	The Protocol window opens.
2. Choose Frame Relay and Click on **OK.**	The Select Protocols window opens.

You have enabled frame relay. You can now enable the protocols you want to run on this interface.

Protocol prioritization is enabled automatically when you select frame relay. For detailed information on protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.* See the appropriate configuration guides for information on enabling the protocols you want to run on this interface.

For further information, see *Configuring and Managing Routers with Site Manager*.

Deleting Frame Relay from a Platform

To delete frame relay from *all* circuits on which it is currently configured, complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. Choose Configuration Manager > Protocols > Frame Relay > Delete Frame Relay.	A window prompts: `Do you REALLY want to delete Frame Relay?`
2. Click on **OK**.	The Configuration Manager window opens. Frame relay is no longer operating on the platform.

Chapter 2
Frame Relay Overview

The following sections present an overview of frame relay.

Introduction

Frame relay is a high-speed, packet-switching WAN protocol that connects geographically dispersed LANs. Frame relay is usually offered by a public network provider; however, private organizations can acquire and manage their own frame relay networks as well.

Frame relay is a connection-oriented protocol, which means that it relies on existing end-to-end paths between devices connected across the network. It implements these connections using *permanent virtual circuits (PVCs)*.

A PVC is a logical path the network provides to connect two devices. This path between the source and destination point is a dedicated connection, so the PVC is always available to the connected devices. Since many PVCs can coexist, devices can share the bandwidth of the transmission line.

Figure 2-1 illustrates a frame relay network.

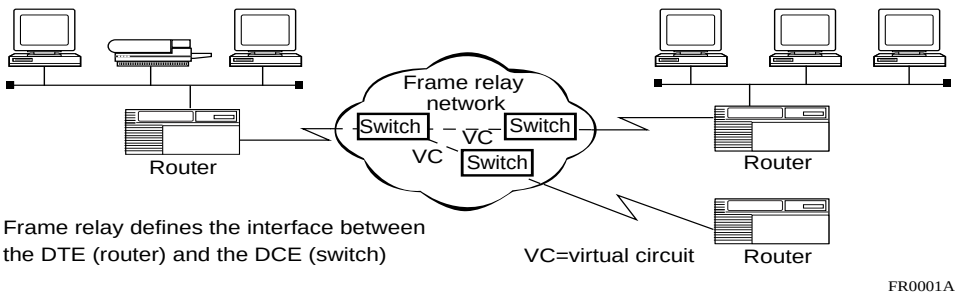

Figure 2-1. Frame Relay Network

Frame relay assumes that networks use transmission lines with low error rates, such as digital transmission media. Consequently, frame relay provides only basic error detection with no error recovery. This minimizes the processing required for each packet, allowing frame relay networks to operate at higher speeds with fewer network delays.

Because frame relay performs only basic error checking, end stations running upper-layer protocols such as Internet Protocol (IP) are responsible for resending packets that did not transmit correctly the first time.

Frame Relay Packets

Figure 2-2 illustrates the structure of a frame relay packet. The packet's header field includes the following:

- Data link connection identifier (DLCI)

  The DLCI is the permanent virtual circuit (PVC) identification number. The frame relay network uses the DLCI to direct basic data flow.

- Command/response bit (C/R)

  ITU-T (formerly CCITT) standards do not use this bit.

- Forward explicit congestion notification (FECN) and backward explicit congestion notification (BECN)

  The FECN and BECN indicate congestion on the network. See "Congestion Control," on page 2-14 for information about how the frame relay software uses these bits.

- Discard eligibility (DE)

  The DE bit allows the router to mark specific frames as low priority (discard eligible) before transmitting them to the frame relay network.

- Extended address bit (EA)

  The EA bit signals whether the next byte is part of the address. This bit indicates the last byte of the DLCI.

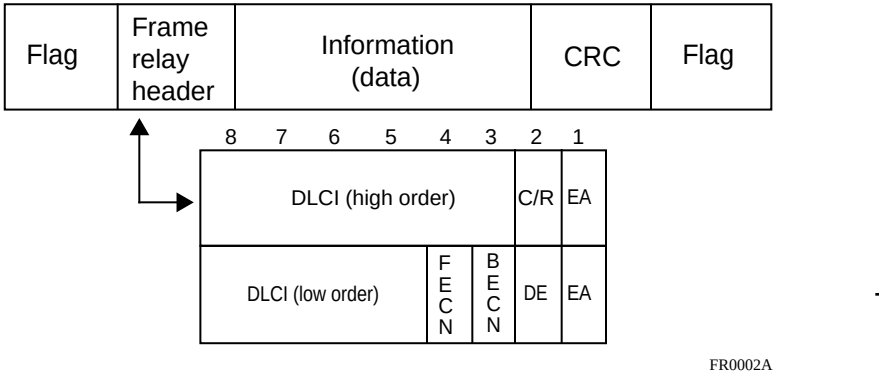

Figure 2-2. Frame Relay Header, 2-Byte Format

Figure 2-2 depicts the frame relay header as a 2-byte structure. Frame relay can also format the header using 3 or 4 bytes, as shown in Figure 2-3. Note, however, that you must configure the frame relay interface on the router to use the same header length as the switched network to which it is connected.

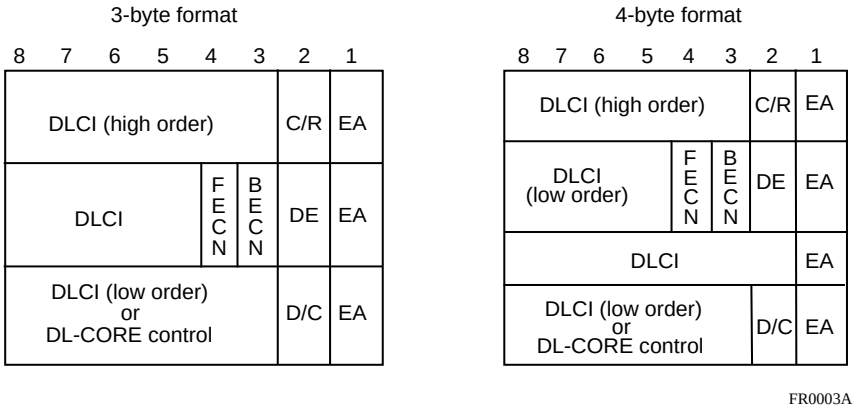

Figure 2-3. Frame Relay Header, 3- and 4-Byte Formats

Management Protocols

Frame relay is an access protocol that runs between a router or data terminal equipment (DTE) and a switch or data communications equipment (DCE). The router and the switch use the Data Link Control Management Interface (DLCMI) to exchange information about the interface and the status of each PVC (Figure 2-4).

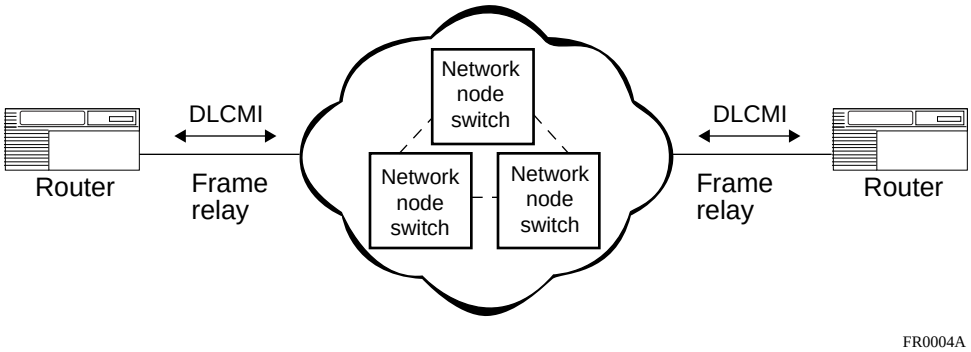

Figure 2-4. Conceptual Drawing of the DLCMI

DLCMI supports three standard data link management specifications: LMI, ANSI T1.617 Annex D, and CCITT (now ITU-T) Q.933 Annex A.

- The networking industry first developed the Local Management Interface (LMI) specification. The LMI approach is asymmetric; the router sends a status-inquiry message to the network, signaling that the router's connection to the network is functioning. The network replies with a status response.
- ANSI modified the LMI specification and incorporated it as Annex D to ANSI standard T1.617. The ANSI method is generally similar to the LMI approach.
- The CCITT (now ITU-T) modified the ANSI standard and adopted it as Annex A to Q.933. The CCITT Annex A specification is similar to Annex D, but it uses an international numbering scheme.

Be sure to configure the frame relay interface on the router to use the same management protocol as the switched network to which it is connected. See Chapter 3, "Customizing Frame Relay," for information about configuring frame relay.

Frame Processing

When a frame enters a frame relay network, the network performs three steps to process the data:

1. Verifies the cyclic redundancy check (CRC); if an error is found, it drops the frame.
2. Performs a table lookup for the DLCI; if the DLCI is invalid or unknown, it drops the frame.
3. If the frame is valid, forwards it to its destination.

Frame Relay Service Records

Bay Networks uses *service records* to define frame relay circuits. A service record is a data structure that allows flexible grouping and characterization of PVCs. A service record can contain a single PVC or multiple PVCs.

Service records:

- Support all protocols.
- Simplify network addressing because you define and associate only one protocol address with groups of frame relay PVCs.
- Allow multiple groups of PVCs per frame relay interface.
- Enable you to group multiple PVCs for each network protocol into separate service records, thereby reducing the number of buffers needed per circuit during broadcasts.
- Lower customer costs by creating multiple broadcast domains.
- Conserve resources because they require a small number of circuits.
- Are easy to configure.

Default Service Record

The router creates the first service record automatically when you select frame relay as your WAN protocol. This first service record is the *default service record*. Any PVCs not associated with another configured service record use the default service record.

Multiple Service Records

Interfaces can have multiple service records, and each service record can contain multiple PVCs.

Adding and Moving PVCs

You can add PVCs to a service record either individually, or in a range. You can also move PVCs on the same interface from one service record to another individually or as a group. See Chapter 3 for instructions.

Frame Relay Access Modes

Bay Networks describes frame relay in terms of three access modes: group, direct, and hybrid. The following sections define each of these modes within the context of service records.

Group Access Mode

Group mode describes a service record with multiple PVCs. It represents a true point-to-multipoint circuit. In group access mode, upper-layer protocols treat each frame relay network interface as a single access point to the switched network. The upper-layer protocols use a single network address to send all traffic destined for the switched network to the frame relay network interface. When you configure each router, you assign only one network address -- for example, an IP or IPX address -- to the frame relay interface, not to each PVC. The Data Link Control Management Interface (DLCMI) dynamically configures PVCs on the default service record; you do not need to explicitly configure them.

Service records in group mode:

- Allow multiple groups of PVCs per frame relay connection.
- Enable you to gather multiple PVCs for each network protocol into a separate group or service record, thereby reducing the number of buffers needed per circuit during broadcasts.
- Lower customer costs by creating multiple broadcast domains.

Direct Access Mode

Direct mode describes a service record with one PVC. In direct access mode, upper-layer protocols treat the frame relay network as a series of point-to-point connections. The upper-layer protocols view each PVC as an individual network interface.

Service records in direct access mode:

- Limit broadcasts to one PVC.
- Enable multiple layer 3 networks per interface.

Hybrid Access Mode

Hybrid access mode, as its name implies, combines characteristics of group and direct access modes. Frame relay hybrid mode enables you to use the same PVCs for both routing and bridging. It works only for non-fully meshed network configurations that use

- Both bridging and routing over a single frame relay interface
- Spanning tree bridging

In a *fully meshed* network PVCs exist between each pair of nodes in the network. In a *non-fully meshed* network, PVCs exist only between nodes that need to communicate. Figure 2-5 shows a non-fully meshed network that uses hybrid mode.

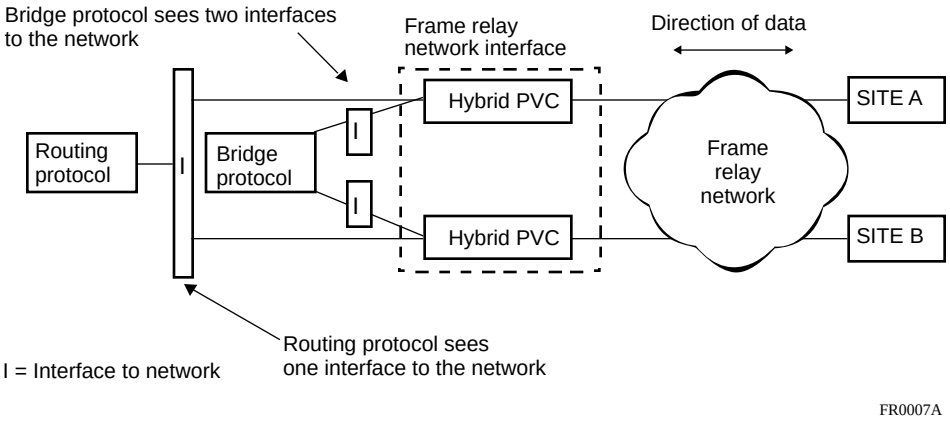

Figure 2-5. Hybrid Mode Configuration, Non-Fully Meshed Network

Using Hybrid Mode for Transparent Bridging

Figure 2-6 shows bridged traffic between site A and site B. The bridge (router 1) is running on the frame relay interface, and its configuration does not use hybrid mode.

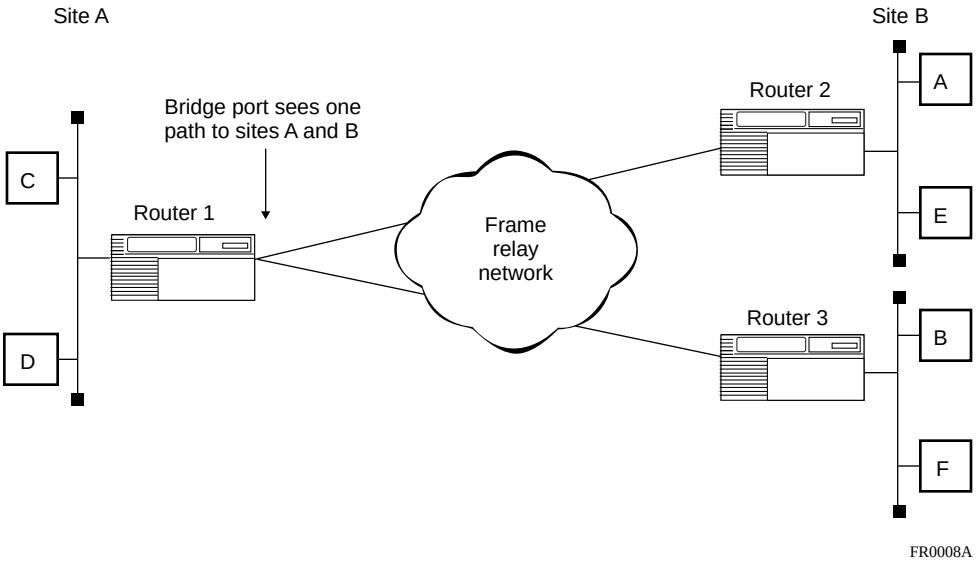

Figure 2-6. Example of a Bridged Network

In this example, the bridge receives data from Site A. If the bridge does not recognize the destination address, it tries to direct traffic through another bridge port. However, without hybrid access mode configured, the frame relay bridge port views the paths to Site A and Site B as the same path. Because the bridge does not send out data on the same port from which it just received data, the bridge does not direct the data to Site B. In this case, you should use hybrid access mode.

If you define the PVCs in hybrid mode (see Figure 2-5), each PVC acts as a separate bridge port. This enables the bridge running on the frame relay interface to view the traffic from site A as arriving on a different port than that of site B. When the bridge sends out data, it sends it out from all ports, including the port that has access to site B. Therefore, data from site A can reach site B.

You configure hybrid mode by enabling the hybrid mode PVC parameter. See Chapter 3, "Customizing Frame Relay," for instructions.

Source Routing

Source routing is the method by which a bridge sends data across two networks. The router supports source routing over frame relay networks, using RFC 1490 standard frame relay data encapsulation.

To configure source routing, see *Configuring Bridging Services*.

RFC 1490

RFC 1490 defines the encapsulation method for sending data across a frame relay network. Bay Networks routers implement RFC 1490 for all protocols that we support over frame relay networks.

Address Resolution

Address resolution maps a remote network address such as an IP address to a local DLCI number. For most protocols that you configure for a frame relay interface, the router performs address resolution automatically. However, IP, AppleTalk, and VINES use the Address Resolution Protocol (ARP). ARP dynamically generates an ARP table of addresses and DLCI numbers by sending messages back and forth to each network node to gather address information. This process increases broadcast traffic across the network.

To reduce broadcast traffic for all protocols, you can configure static routes and adjacent hosts at the protocol level. This eliminates the need for the router to perform address resolution. To reduce traffic associated specifically with VINES address resolution, you can configure Inverse ARP. Inverse ARP is the default for IP over frame relay. Refer to the appropriate protocol manual for more information about static routes, adjacent hosts, and Inverse ARP.

Table 2-1 lists how the router handles address resolution for each protocol and whether or not you can reduce broadcast traffic by modifying the address resolution configuration.

Table 2-1. How Protocols Handle Address Resolution

Protocol	How Router Performs Address Resolution	Configuration Requirements
Bridge (including source route)	Automatic	None
IP	ARP or Inverse ARP	Configure ARP Configure Inverse ARP
DECnet IV	Automatic	None
VINES	ARP or Inverse ARP	None for ARP Inverse ARP is the default for frame relay.
Internet Packet Exchange (IPX)	Automatic	None
Xerox Networking System (XNS)	Automatic	None
AppleTalk	AppleTalk ARP	None

Traffic Control

Frame relay is unreliable. It does not include error recovery mechanisms, relying instead on the upper layer protocols to detect and retransmit lost frames.

Hub and spoke topologies often present a “big pipe/little pipe” situation. The central or hub site has a faster link to the frame relay service because it is a point of concentration for many remote sites: it has a “big pipe,” with, for example, a T1/E1 connection that can transmit data at rates of 1.54 Mb/s. The remote sites usually support a much lower line speed, 56 Kb/s to 64 Kb/s, or “little pipe.” Figure 2-7 illustrates this concept.

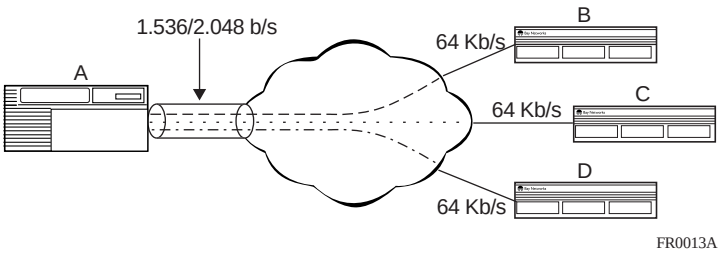

Figure 2-7. Big Pipe/Little Pipe Topology

The central site router sends traffic at its available bandwidth, in this example at T1 rates (1.536 Mb/s). Some switches recognize that the remote site is configured at a lower speed, and begin to drop frames above the capacity of the remote site router. At the remote site, the frame relay interface discards frames beyond its available buffer. The assumption is that the user application detects the lost frames and either retransmits them or uses a flow control mechanism in the protocol, such as windowing, to *throttle* (queue) the traffic. But not all applications have a robust mechanism to deal with lost or out-of-sequence frames.

You can use Bay Networks WAN Compression Protocol (WCP), protocol prioritization, congestion control, and traffic shaping either singly or in combination to help control the flow of traffic and avoid loss of data.

Data Compression

You can configure both hardware- and software-based data compression over WANs running frame relay.

Enabling compression improves bandwidth efficiency by eliminating redundant strings in data streams. This, in turn, improves network response times and reduces line costs. Enabling compression on a frame relay link also provides reliability. Both sides of a link using compression maintain a history of data that has already traveled across the network, and WCP (WAN Compression Protocol) detects and retransmits dropped packets.

To use data compression with frame relay, the Compression Control parameter must be set to Enable, the default value (see Chapter 3 or Appendix A for information about how to access this parameter). You must also select WCP from the protocols menu.

For a complete discussion of data compression, see *Configuring Data Compression Services*.

Protocol Prioritization

You can set priorities for the traffic sent across a synchronous line interface using a process called *protocol prioritization*. The ability to prioritize traffic is important for an application that is time-sensitive and that requires a fast response.

For example, a user at router A participating in a Telnet session with router B requires a more immediate response than does a user at router A performing a file transfer with router B.

When you select frame relay on a circuit, the router enables protocol prioritization automatically. It does so because the DLCMI packets must have a higher priority than any other packets you are sending across the network.

For more information about protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.*

Congestion Control

Network congestion can degrade network performance. Congestion occurs when a node receives more frames than it can process, or sends more frames than the transmission line can handle. The frame relay network informs the nodes of congestion, so that they can reduce the amount of traffic across the network.

In the frame relay packet header, there are two bits that the network sets to alert nodes of network congestion. These bits, as defined by the frame relay specification, are the FECN (forward explicit congestion notation) bit and the BECN (backward explicit congestion notation) bit.

If the network detects congestion, it alerts the router in the same direction as the received frame by changing the frame's FECN bit from 0 to 1. For nodes in the opposite direction of the received frame, it changes the frame's BECN bit from 0 to 1 (Figure 2-8).

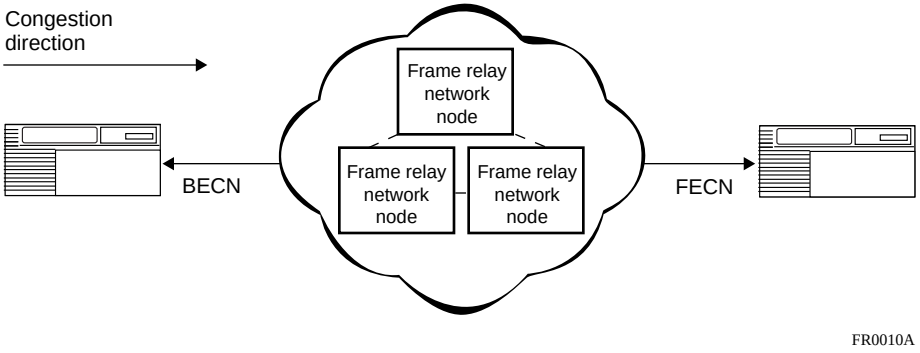

Figure 2-8. Detecting and Controlling Network Congestion

If you enable the congestion control feature, you can specify the number of FECN/BECN bits the router receives in a given time period before it stops transmitting frames. While frames are going across the network, the frame relay interface checks received packets for FECN and BECN bits set to 1. If the interface receives the specified number of bits during the designated time period, frame relay drops all traffic destined for the PVC where there is congestion. When the interface no longer receives these congestion notifications, the router resumes transmission.

For example, suppose you set the congestion timer to 0.5 seconds and the congestion count to 3. In this case, if an interface receives 3 FECNs or BECNs within 0.5 seconds, the node stops sending frames (although it continues to receive frames for this PVC). If the interface receives no FECNs or BECNs during the next 0.5 seconds, the router resumes transmission. See Chapter 3, "Customizing Frame Relay," for instructions on configuring the congestion parameters.

If you enable congestion control and also enable *traffic shaping*, you can queue or *throttle* congested traffic rather than drop it by choosing that value in the Congestion Method parameter (see Appendix A for the parameter description).

Traffic Shaping

Traffic shaping relieves bottlenecks in topologies with high-speed connections to the central site, and low-speed connections at remote sites as in Figure 2-7 on page 2-13. Committed information rate (CIR) enforcement and quality of service (QoS) are the major components of Bay Networks traffic shaping.

Committed Information Rate

The CIR is the rate at which the network supports data transfer under normal operations. Its name is descriptive: you have a contract with your carrier, who has *committed* to providing a given throughput, here called the *committed information rate*. The CIR is measured in bits per second. You configure this value that the carrier provides per virtual circuit (VC).

CIR of 0

You can contract with a carrier for a CIR of 0, which yields best-effort service at low cost. The carrier transmits data, but does not commit to providing a specified throughput. To configure a CIR of 0, set both the Throughput parameter (which is the CIR) and the Committed Burst (B_c) parameter to 0, and set the Excess Burst (B_e) parameter to a value greater than 0.

Maximum CIR

The maximum CIR should not be greater than the speed of the access line on the slower end of a VC. In a big pipe/little pipe topology (refer to Figure 2-7), likely CIRs at the remote sites would be 32 Kb/s, 56 Kb/s, or 64 Kb/s. If you configure CIRs for these VCs at the central site, you can use *CIR enforcement* to prevent the big pipe from sending traffic that exceeds the PVC CIRs.

CIR Enforcement

CIR enforcement means restricting the speed of outbound traffic to a rate no faster than the CIR. It is the major component of traffic shaping. You can configure CIR enforcement to operate over Synchronous, High-Speed Serial Interface (HSSI), T1, E1, and Integrated Services Digital Network (ISDN) lines, for frame relay backup, demand, bandwidth-on-demand, and leased lines at the VC level. CIR enforcement operates on whole frames only. It controls congestion either by bringing down the VC, or by queuing the traffic, which is also called throttling.

CIR and Committed Burst Rate and Excess Burst Rate

The committed burst rate (B_c) defines the number of bits that the router can transmit over a specified time interval (T_c) when congestion is occurring. The excess burst (B_e) defines the number of extra bits that the router attempts to send over the T_c when there is no congestion. Both the B_c and the B_e are values that you configure.

The sum of the B_c and the B_e is the maximum amount of traffic that can travel across the network per T_c when there is no congestion. If you set the B_e to a value greater than zero, the router can send traffic exceeding the CIR. To enforce the CIR, that is, to limit traffic that the router can send to the amount of the CIR, set the B_e to 0.

If you enable congestion control *and* set the congestion method to throttle, the VC sends only B_c bits of data over the time interval T_c when congestion occurs, even if you have configured the B_e to a value greater than 0. It queues the excess data until congestion abates. If you set the congestion method to throttle-then-shutdown, the VC first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion.

Quality of Service

QoS is the second major component of traffic shaping. It uses protocol prioritization with traffic shaping. You configure a prioritization filter on the default service record for the entire frame relay interface, and CIR enforcement per VC. QoS operates over Synchronous, HSSI, T1, E1, and ISDN lines, for backup, demand, and for leased lines. Although the HSSI driver does not support protocol prioritization, VCs on a HSSI interface do.

Using protocol prioritization with traffic shaping creates two levels of queues. For traffic shaping the queues are high/normal/low at the VC level. For protocol prioritization they are interrupt/shaping/high/normal/low at the driver level. Figure 2-9 illustrates this concept.

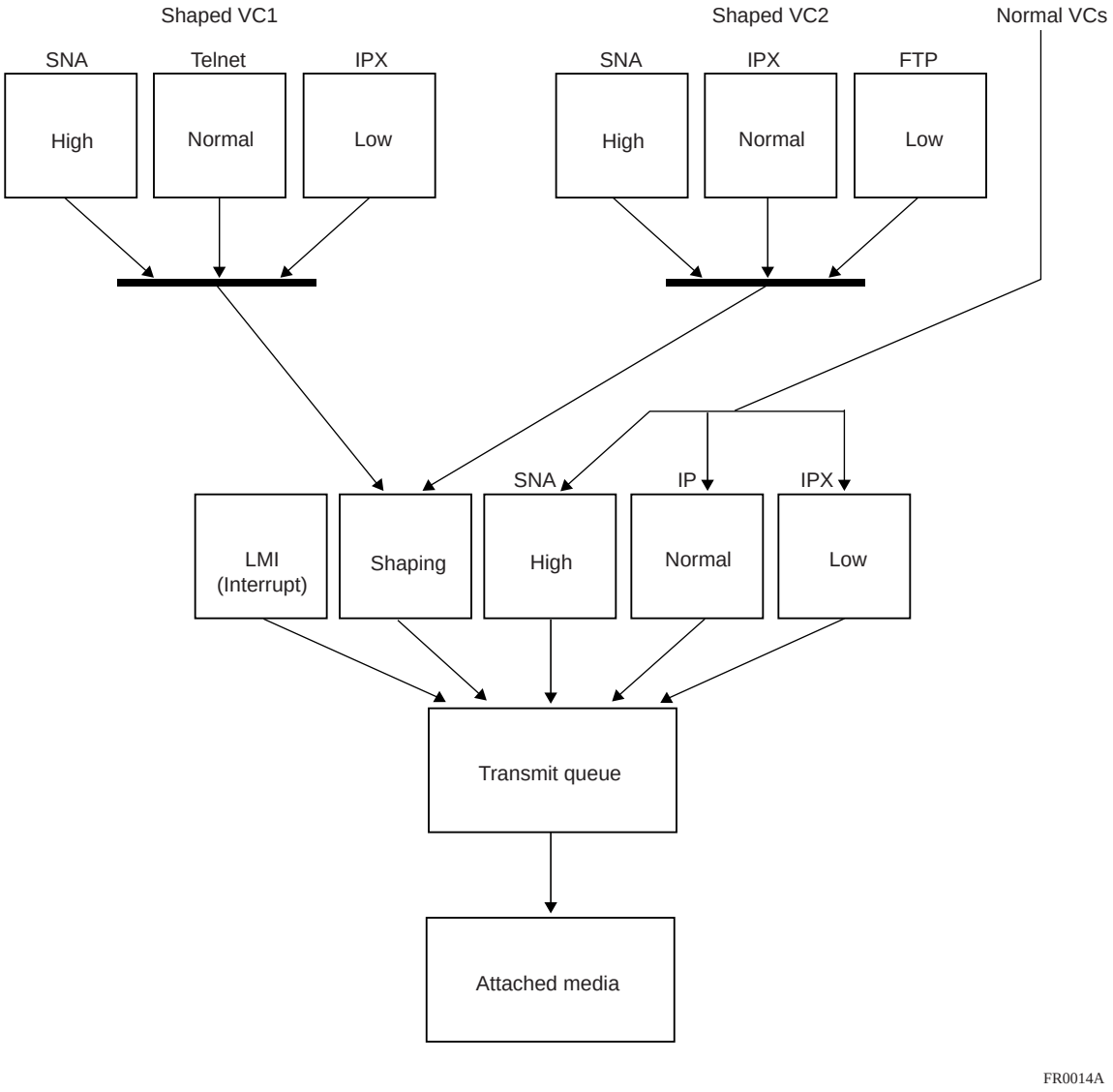

Figure 2-9. Traffic Shaping Queues

All traffic that goes to a traffic-shaped VC (VC1 or VC2) is queued as high, normal, or low priority at the VC level, and then it travels, by priority order, to a shaping queue within the driver. Normal VC traffic is queued as high, normal, or low priority at the driver level. At the driver level:

- Interrupt priority traffic, DLCMI/LMI requests (the LMI box in Figure 2-9), has the highest priority. You cannot change that.
- Shaped priority traffic (shaping box in Figure 2-9) has the second highest priority.
- Normal VC traffic (not shaped) has lower priority than shaped traffic. You can still prioritize normal VC traffic as high, normal, or low.

Queuing and prioritization only matter when the traffic rate exceeds the VC line rate or the CIR. If the total of all traffic is below the CIR, the router just transmits it.

You cannot prioritize between VCs on which you have enabled traffic shaping. The router schedules traffic among them in a round-robin manner.

For information about configuring filters for protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization*.

Traffic Shaping Considerations

Traffic shaping is best used at central offices to prevent the “big pipe” from sending too much data too quickly to remote sites with “little pipes.” Let this principle guide your decisions about how to use traffic shaping on your network.

CIR Configuration Guidelines

In general, the value you assign to the B_c should equal 1/4 of the CIR to avoid excessive queuing and dropped packets. If, however, you are sending frames that exceed the size of the B_c, data travels very slowly because the router must use multiple time periods to accommodate the packet size and avoid exceeding the CIR. If setting the B_c to 1/4 of the CIR yields a value lower than packet size, set the B_c to 1/3 or even 1/2 of the CIR.

For example, a typical TFTP frame is 548 bytes. If the CIR is 16,000 bits, the B_c configured according to the 1/4 guideline would be 4,000 bits, or 500 bytes, which is not big enough to accommodate a TFTP frame. If you set the B_c to 16,000/2, or 1/2 CIR, the result is 8,000 bits, or a packet size of 1,000 bytes, which works, but may result in excessive queuing because the T_c is 1/2 second. If you set the B_c to 16,000/3 or 1/3 of CIR, the result is a B_c of 5,333 bits or 666 bytes, much closer to the 548 TFTP frame size.

If you cannot predict the typical frame size, monitor frame relay shaping statistics for numbers of large frames and dropped frames. If either of these numbers is increasing constantly or dramatically, adjust the B_c to a higher value in small increments.

WCP and CIR Enforcement

Data compression maximizes throughput and increases reliability. Traffic shaping increases reliability, controls congestion, and prioritizes traffic. Compression and traffic shaping together maximize reliability, but at the expense of throughput.

Traffic shaping occurs at the VC level; compression, at the driver level. Shaping therefore occurs before compression, which compromises effective compression because only the precompressed traffic is shaped: the compressed traffic is not shaped. WCP compresses data at the rate it receives it, which with traffic shaping is the CIR. It is therefore unrealistic to expect a high compression throughput for data that originates from a site that also uses traffic shaping.

You can use traffic shaping at one or both ends of a link, but you must use compression at both ends of a link. It makes sense to use traffic shaping at a central site, where you have a T1 line that sends data to remote sites with 64 KB line rates, and the goal is to control the flow of traffic and avoid flooding the remote sites. But if the CIR is equal to the line rate, which could well be the case at the remote site with 64 KB line rates, there is no need to use traffic shaping.

You can use compression effectively in the case of the 64 KB site which does not use traffic shaping. You can also compensate for the throughput cost associated with using compression and traffic shaping at the central site by taking into account characteristics of compression and traffic shaping, and fine-tuning traffic shaping parameters.

- When you configure traffic shaping, take into account the compression ratio you want to achieve.

- If you set the B_e equal to the B_c, the router doubles the amount of traffic it attempts to send and, when you enable compression, compresses that amount of traffic, because WCP compresses data at the rate it receives it.
- If you also set the Congestion Method to throttle, the router will queue traffic if congestion occurs, and thus prevent exceeding the CIR.
- Congestion may occur if compression histories are not in sync, and WCP has to resend packets. If WCP retransmits many packets, it may exceed the CIR.

Oversubscribing the Interface

The CIRs that you configure are based on an average peak rate for the VCs on the network. If all VCs with traffic shaping try to send data simultaneously, they may exceed the capacity of the interface. If you oversubscribe the interface, traffic shaping will still enforce the CIR, but there may be additional latency for reserved flows. VCs without traffic shaping will send data after traffic shaped VCs.

Queue Limits and Data Clipping

Bay Networks routers maintain buffers for each traffic shaped VC. Each buffer can hold one frame that the router cannot send because of congestion. The router divides the number of buffers on the interface (default number of buffers is 200 per interface) by the number of traffic-shaped VCs, giving each VC the same number of buffers. If you have 10 traffic shaped VCs per interface, each VC has 20 buffers. If you enable protocol prioritization, the default number of buffers is 30 for high priority traffic, 200 for normal, and 30 for low.

You can use the Technician Interface to increase the total number of buffers for the interface, and you can also redistribute buffers among the VCs and among priority queues. The attributes that you customize at the interface level are

wfFrDlcmiShapingHiQueueLimit

wfFrDlcmiShapingNormalQueueLimit

wfFrDlcmiShapingLoQueueLimit

At the VC level the attributes are

wfFrCircuitShapedHiQueueLimit.

wfFrCircuitShapedNormalQueueLimit

wfFrCircuitShapedLoQueueLimit

For further information on using the Technician Interface, see *Using Technician Interface Software.*

FECN and BECN Notification Bits

The earlier section, "Congestion Control,"explained that a specified number of FECN and BECN bits received during a set time period indicate congestion. When congestion occurs on a traffic shaped VC, the router either drops traffic, throttles it, or throttles and then drops traffic, depending on the value of the Congestion Method parameter.

The FECN and BECN notifications are part of the header in a frame relay data packet. In a big pipe/little pipe topology (see Figure 2-10), the central site router typically sends much more data than it receives. Therefore, the remote site routers that receive a lot of traffic may be getting large numbers of FECNs, while the central site router is getting relatively few data packets, and therefore few BECNs, and is unaware than congestion is occurring. You may need to fine tune the Congestion Counter and Congestion Timer parameters (see Appendix A), from the default values of 20 FECN or BECN counts per one second to, for example, 10 counts per 5 seconds to account for the differences in traffic volume from and to the central site.

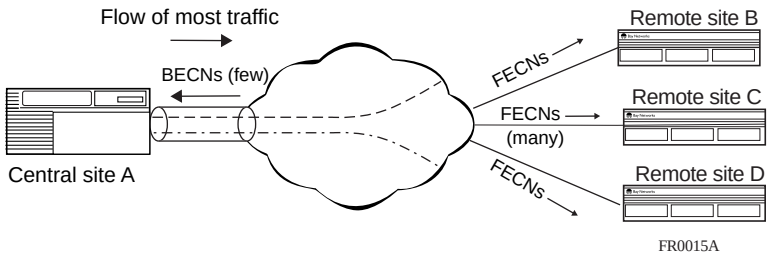

Figure 2-10. FECNs and BECNs in Big Pipe/Little Pipe Topology

Multiline

Frame relay provides a link redundancy feature called multiline. Multiline is a Bay Networks proprietary implementation that lets you group two or more physical lines that back each other up in case of a failure. This ensures that information arrives at its destination on the network. In addition, if both lines are up, the router uses both lines simultaneously. Two or more physical lines must be available for a multiline configuration. Figure 2-11 illustrates a multiline configuration.

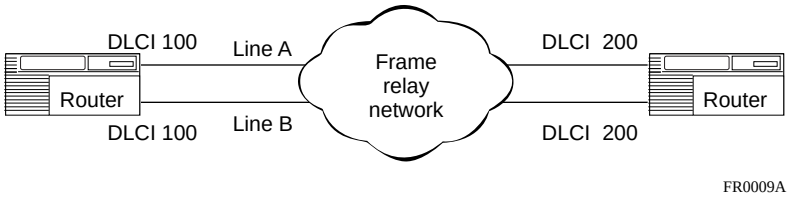

Figure 2-11. Multiline Network

In this example, when the router receives traffic destined for the network, it alternates or randomizes (depending on how you configure it) between line A and line B to transmit the data. The router uses both lines simultaneously to balance the traffic between each path. If one of these lines goes down, the router uses the remaining line.

You can multiline up to four service records together. Each service record must be on a different physical line on the router. We also recommend that each line be on a different slot to provide fault tolerance.

You must also match DLCIs in each service record of the multiline. Matching DLCIs ensures that a backup exists for each PVC.

The most important part of configuring multiline is setting the PVC DLCI number. This number identifies each PVC, thereby specifying a path for the router to direct data to the network. For each frame relay PVC that you configure, make certain that PVCs with the same destination have the same DLCI number.

Note: If you use multiline, packets traveling on the two paths may arrive at their destination out of sequence. Some protocols do not tolerate packets arriving out of sequence and, as a result, you may experience poor performance or failures.

See Chapter 3, "Customizing Frame Relay," for instructions about grouping service records for multiline.

Traffic Distribution Between Data Paths

To distribute traffic between multiline data paths, you can use one of two methods:

- Random distribution
- Address-based distribution

Random Distribution

Random distribution means that as the router sends out each packet, it alternates between the lines. This option determines which line the packet uses based on a randomly assigned number. For each outbound packet, the router generates a random number, and this number designates the line to use.

Random balancing evenly distributes traffic and lets the router use the two lines efficiently. Because packets travel on different paths, they arrive at the destination out of sequence, and the upper-layer protocols, for example, IP and Open Systems Interconnection (OSI), have to resequence the information. Some protocols cannot tolerate packets arriving out of sequence, so be sure this option is appropriate for your application.

Address-Based Distribution

Address-based distribution, as the name implies, determines the data path for outbound traffic from the source and destination address in each packet. Any given address pair always uses the same path.

The router determines whether to route or bridge the packet, and then uses the corresponding level of address. It uses routing-level addresses for routing traffic, and the MAC-level addresses for bridging traffic.

Address-based distribution ensures that all outbound traffic travels on the same path, and that packets arrive in sequence. For protocols that cannot receive packets out of sequence, use this method. Note, however, that this option does not always distribute traffic evenly across each line.

Protocol Prioritization and Multiline

You cannot use protocol prioritization with multiline. Protocol prioritization may change the order of frames arriving over a multiline interface, and frame relay multiline does not have the ability to correct the sequence.

Configuring Synchronous Lines for Frame Relay

If you enable frame relay on a circuit, Site Manager automatically sets the following synchronous line parameters (Table 2-2):

Table 2-2. Synchronous Line Parameters for Frame Relay

Parameter	Value
BofL	Disable
Promiscuous	Enable
Service	Transparent
WAN Protocol	Frame Relay

For more information on these parameters, refer to *Configuring WAN Line Services*.

For More Information About Frame Relay

For more information about frame relay, consult the following documents:

American National Standards Institute, T1.617-1991. *Integrated Services Digital Network (ISDN) – Digital Subscriber Signalling System No. 1 (DSS1) - Signalling Specification for Frame Relay Bearer Service*. Washington, D.C., June 1991.

-- T1.617 Annex D-1991. *Additional Procedures for Permanent Virtual Connections (PVCs) Using Unnumbered Information Frames*. Washington, D.C., June 1991.

-- T1.618-1991. *Integrated Services Digital Network (ISDN) - Core Aspects of Frame Protocol with Frame Relay Bearer Service.* Washington, D.C., June 1991.

Bradley, T., C. Brown, and A. Malis. *Multiprotocol Interconnect over Frame Relay. RFC 1490.* Menlo Park, California: Network Information Center (NIC), SRI International, January 1992.

Digital Equipment Corporation et al. *T1S1 - Standards based Frame Relay Specification with Common Enhancements.* Document Number 001-208966, Revision 1.0, September 1990.

The following publications provide a less technical introduction to frame relay:

Davidson, R., and N. Muller. *The Guide to SONET: Planning, Installing & Maintaining Broadband Networks.* New York: Telecom Library, Inc., 1991.

Goldstein, F. *ISDN in Perspective.* Reading, MA: Addison-Wesley, 1992.

Jennings, E., T. Jones, and K. Rehbehn. *The Buyer's Guide to Frame Relay Networking.* Netrix Corporation.

Chapter 3
Customizing Frame Relay

When you enable frame relay, default values are in effect for all parameters (see parameter descriptions in Appendix A). You may want to change these values, depending on your network requirements. The following sections describe how to customize frame relay for your network. They do not, however, correspond exactly with the order in which parameters appear in Site Manager. Appendix A does list parameters in the order in which they appear in Site Manager, and reproduces the pertinent Site Manager screens.

Using the MIB Object ID

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB Object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify parameter values you enter. Entering an invalid value can corrupt your configuration.

Adding Service Records

A service record is a data structure that allows flexible grouping and characterization of PVCs. You can add and delete service records from your frame relay interfaces. When you add a new service record, it automatically creates one PVC to which you must assign a DLCI number. To add a service record, complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **Add**.	The Frame Relay Service Add window opens.
5. Click on the **DLCI Number** parameter, and enter the DLCI number. Note that the **Service Name** parameter is already filled in. See pages A-13 and A-11 for descriptions of these parameters.	
6. Click on **OK.**	The Frame Relay Service List window reopens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
7. Add more service records as your network requires by repeating Steps 4 through 6. When you are finished, click on **Done.**	The Frame Relay Circuit Definition window opens.
8. Click on **Done** again**.**	You return to the Configuration Manager window.

Deleting Service Records

You can delete service records from your frame relay interfaces by completing the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the service record entry.	
5. Click on **Delete**.	Site Manager removes the service record entry from the Frame Relay Service List window.

Adding PVCs

You can add PVCs to already existing service records. You can add PVCs either individually, or in a range. If you want to add one PVC, enter one DLCI number. If you want to add several PVCs, enter the appropriate range of DLCI numbers in the format < *lowest DLCI number*> - < *highest DLCI number*> as shown in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The Frame Relay PVC List window opens.
5. Click on **Add**.	The Frame Relay PVC Add window opens.
6. Click on the **DLCI Number** parameter and enter the DLCI number, or, if you want to add more than one PVC, enter a range of numbers in the format *<lowest DLCI number> - <highest DLCI number>.*	
7. Click on **OK**.	The Frame Relay PVC List window reopens. Note that it now lists the PVCs you have just created.

Deleting PVCs

You can delete PVCs from already existing service records. After you delete a PVC, it may reappear on the list of active PVCs if the switch provider does not delete it. As soon as the switch provider removes the PVC, frame relay dynamically deletes the PVC from the list.

If the switch provider deletes a PVC that you manually configured, the circuit state is set to Invalid, and the PVC remains unused until you delete it from the interface by completing the steps in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The Frame Relay PVC List window opens.
5. Click on the PVC entry.	
6. Click on **Delete**.	The confirmation window closes. Site Manager removes the PVC entry from the Frame Relay PVC List window.

Moving PVCs from One Service Record to Another

You can move PVCs on the same line from one service record to another. Also, you can move PVCs to already existing or to new service records.

Site Manager Procedure	
You do this	**System responds**
1. Click on a port in the Configuration Manager window configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Select the DLCI of the PVC to be moved, and click on **Move**.	The Frame Relay PVC Move window opens.
6. Click on **OK**.	The FR Service Record Selection window opens.
7. Click on the target service record and click on **Select**.	The FR Service Record Selection window closes, revealing the change in the FR PVC List for Service window.

Selecting a Management Type

You can specify the management protocol that the router and the frame relay network use to communicate status information. Routers connected back to back also use a management protocol to exchange status information. The following list describes your options:

- *DLCMI None* provides no management interface between the router and the frame relay network. In the absence of management support, you must configure all PVCs manually.
- *Rev 1 LMI* provides user-side management services as specified by Revision 1 of the Local Management Interface standard.
- *ANSI T1.617D* provides user-side management services as specified in Annex D to ANSI standard T1.617-1991. This is the default value.

- *CCITT Annex A* provides user-side management services as specified by the ITU-T (formerly CCITT).
- *LMI Switch* offers limited management services for the DCE side of the connection as specified by Revision 1 of the Local Management Interface standard.
- *Annex D Switch* provides limited management services for the DCE side of the connection as specified in Annex D to ANSI standard T1.617-1991.
- *Annex A Switch* provides limited management services for the DCE side of the connection as specified by the ITU-T.

If you are connecting two routers back to back, use one of the DTE parameter options (Rev 1 LMI, ANSI T1.617D, CCITT Annex A) for the router acting as a DTE, and one of the DCE options (LMI Switch, Annex D Switch, Annex A Switch) for the router acting as the DCE. Although you can configure the router for the DCE side of a connection, the router cannot act as a full switch, and it will not perform complete bidirectional signaling.

The LMI Switch, Annex D Switch, and Annex A Switch options are primarily for troubleshooting.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the **Management Type** parameter. See **Help** or the parameter description on page A-3.	
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.

Selecting Address Type and Length

You can specify the DLCI address type and length that the router and the frame relay network use to direct packets to their destinations. The address type for the router and for the switch must be the same.

Selecting a DLCI Address Type

Your options for the DLCI address type follow:

- *ADDR Q922* selects addressing as specified in the final version of the Q.922 standard. Q.922 provides for FECN, BECN, DE, and EA bits. While most Q.922 addresses are included within a 2-octet field, the standard allows for 3- and 4-octet address fields. This is the default.
- The *November draft of ADDR Q922* differs from ADDR Q922 in dropping the D/C bit from the extended (3- and 4-byte) forms. The D/C bit (DLCI or DL-Core Control Indication) is always 0.
- The *March draft of ADDR Q922* differs from ADDR Q922 in defining an 11-bit DLCI and dropping the DE bit from the second octet of the address field.
- *ADDR Q921* differs from ADDR Q922 MARCH 90 in that it does not use FECNs or BECNs, which means that it does not provide congestion control.

Selecting Address Length

Your options for the DLCI address length are 2, 3, or 4 bytes. See the illustrations of frame relay headers in Figure 2-2 and Figure 2-3 to understand the distinctions among these types. To specify address length, complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the following parameters, using **Help** or the parameter descriptions on page A-4: • **Address Type** • **Address Length**	
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.

Monitoring the Connection

You can monitor the status of your frame relay network connection by setting:

- Time intervals for the router to send messages that verify the integrity of the link
- The number and frequency of error messages that can occur before the connection terminates

Polling Interval

The *polling interval* specifies the interval between status inquiry messages that the router transmits. Status inquiry messages cause a network response in the form of a link integrity verification message or full status message. Successful completion of the request/response “handshake” verifies the status of the router/frame relay network link. We recommend that you accept the default value, 10 seconds. If the default value does not match what the network requests, enter a value that is appropriate for your network in the range of 5 to 30 seconds. The polling interval does not function if you set the Mgmnt Type parameter to DLCMI None.

Full Enquiry Interval

The *full enquiry interval* specifies the interval between full status inquiry messages that the router transmits. Full status inquiry messages cause the network to send a full status report message, which lists all PVCs, PVC status (active or inactive, and new or previously established).

The default value, 6, tells the router to send a full status inquiry every 6 polling intervals. For example, with a polling interval of 10 and a full enquiry interval of 6, the router transmits a full status inquiry every 60 seconds; with a polling interval of 20 and a full enquiry interval of 30, the router transmits a full status inquiry every 10 minutes (600 seconds). The full enquiry interval does not function if you set the Mgmnt Type parameter to DLCMI None.

Error Threshold and Monitored Events

Error threshold and *monitored events* together establish a criterion to evaluate the quality of the router’s frame relay network connection. The error threshold is the number of faulty status messages that must occur to terminate the connection. Monitored events is the number of status message exchanges, within which number those errors occur. For example, if you accept the default of 3 for the error threshold, and the default of 4 for monitored events, three status exchange errors in a sequence of four attempted exchanges brings the connection down. If you set error threshold to 5 and monitored events to 10, five status exchange errors in a continuous sequence of ten attempted exchanges brings the connection down.

Note: Error Threshold and Monitored Events do not function if you set Mgmnt Type to DLCMI None.

To specify error threshold and monitored events values, complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-5: • **Polling Interval** • **Full Enquiry Interval** • **Error Threshold** • **Monitored Events**	
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.

Enabling Multicast

The multicast feature sets up a separate DLCI that replicates broadcast packets and forwards them to the appropriate destinations. You can enable support for frame relay multicast service, but only if your frame relay subscription service provides multicast service. To enable multicast service, complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the **Multicast** parameter to **Enable**. See **Help** or the parameter description on page A-7.	
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.
7. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
8. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
9. Click on **Services**.	The Frame Relay Service List window opens.
10. Click on **PVCs**.	The FR PVC List for Service window opens.
11. Set the **Multicast** parameter to **Multicast**. See **Help** or the parameter description on page A-15.	
12. Edit other parameters if you want, and click on **Apply**.	
13. Click on **Done**.	You return to the main Configuration Manager window.

Configuring Hybrid Mode

Hybrid mode allows you to use the same PVCs for both routing and bridging. You configure hybrid mode by setting the Hybrid Mode parameter to ON. See Chapter 2 for an explanation of hybrid mode. To configure hybrid mode, complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Set the **Hybrid Mode** parameter to **ON**. See **Help** or the parameter description on page A-16.	
6. Edit other parameters if you want, and click on **Apply**.	
7. Click on **Done**.	You return to the main Configuration Manager window.

Controlling Congestion

Congestion occurs when a node receives more frames than it can process, or sends more frames than the transmission line can transport. You can enable congestion control on your network. When you enable congestion control, the router receives congestion notification messages from the PVC experiencing congestion, and drops all outbound traffic destined for that PVC until it no longer receives congestion notifications.

When you enable congestion control, you can set the length of time during which the router counts congestion notifications. You can also set the maximum number of congestion notifications that the router can receive during this time period. If the router receives this number of congestion notifications within the time period you specify, it stops transmitting data. The router resumes transmission when it stops receiving congestion notifications.

If you enable congestion control, all PVCs on the interface use congestion control and the values you specify for the congestion timer and congestion counter, unless you configure PVCs individually and either disable this feature or select other values for the congestion control parameters. To enable congestion control, complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-7: • **Congestion Control** • **Congestion Timer** • **Congestion Counter** • **Congestion Method** (applies only when you enable traffic shaping)	
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.
7. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
8. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
9. Click on **Services**.	The Frame Relay Service List window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
10. Click on **PVCs**.	The FR PVC List for Service window opens.
11. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-18: • **Congestion Control** • **Congestion Timer** • **Congestion Counter** • **Congestion Method** (applies only when you enable traffic shaping)	
12. Edit other parameters if you want, and click on **Apply**.	
13. Click on **Done**.	You return to the main Configuration Manager window.

Using Traffic Shaping

To use traffic shaping, you configure three PVC parameters: Committed Burst, Excess Burst, and Throughput. There is no Enable parameter as such. You may also want to edit values for the PVC Congestion Control and Congestion Method parameters. To enable traffic shaping, complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Select the appropriate service record and click on **PVCs**.	The Frame Relay PVC List window opens.
5. Click on a PVC that you want to configure for traffic shaping.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Configure the following traffic shaping parameters, using **Help** or the parameter descriptions that begin on page A-16: • **Committed Burst** • **Excess Burst** • **Throughput**	The parameters are now set to the values you chose.
7. Click on **Done**.	You return to the Frame Relay Service List window.
8. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
9. Click on **Done**.	You return to the main Configuration Manager window.

Enabling Compression

To use data compression with frame relay, first select WCP from the Protocols menu, and make sure the Compression Control parameter is set to Enable by completing the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Set the **Compression Control** parameter to **Enable**. See **Help** or the parameter description on page A-20.	
6. Edit other parameters if you want, and click on **Apply**.	
7. Click on **Done**.	You return to the main Configuration Manager window.

Grouping Service Records for Multiline

You can configure two or more service records to run in multiline mode. Service records that you group for multiline must:

- Reside on two separate physical ports.
- Have the same DLCI numbers.
- Not use hybrid mode.

Configure multiline mode by completing the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **Multiline** button.	The Services Multiline With window opens.
5. Click on the **Add** button.	The Add Multiline Services window opens.
6. Choose the frame relay interface you want to configure for multiline.	The frame relay interface entry becomes highlighted.
7. Click on **Select**.	The Add Multiline Services window closes. Site Manager moves the record of the frame relay interface from the Add Multiline Services window to the Services Multiline With window.
8. Set the **Multiline Algorithm to Choose Line** parameter. See the parameter description on page A-22.	
9. Click on **Apply**.	
10. Click on **Done**.	You return to the Frame Relay Service List window.

Removing Multiline Services

You can select circuits on which to remove multiline services. Complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the Multiline button.	The Services Multiline With window opens.
5. Choose the frame relay interface you want to remove in the Services Multiline With window.	The frame relay interface becomes highlighted.
6. Click on the **Remove** button.	Site Manager removes the record of the frame relay interface from the Services Multi-line with window.

See Chapter 2 for more information about multiline.

Deleting Frame Relay

To delete frame relay from *all* circuits on which it is currently configured, complete the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Delete Frame Relay**.	A confirmation window prompts "`Do you REALLY want to delete Frame Relay?`"
4. Click on **OK**.	The confirmation window closes, revealing the Configuration Manager window.

Appendix A
Site Manager Parameters

Interface Parameters

The Frame Relay Interface List window (Figure A-1) contains the parameters for the Frame Relay interfaces.

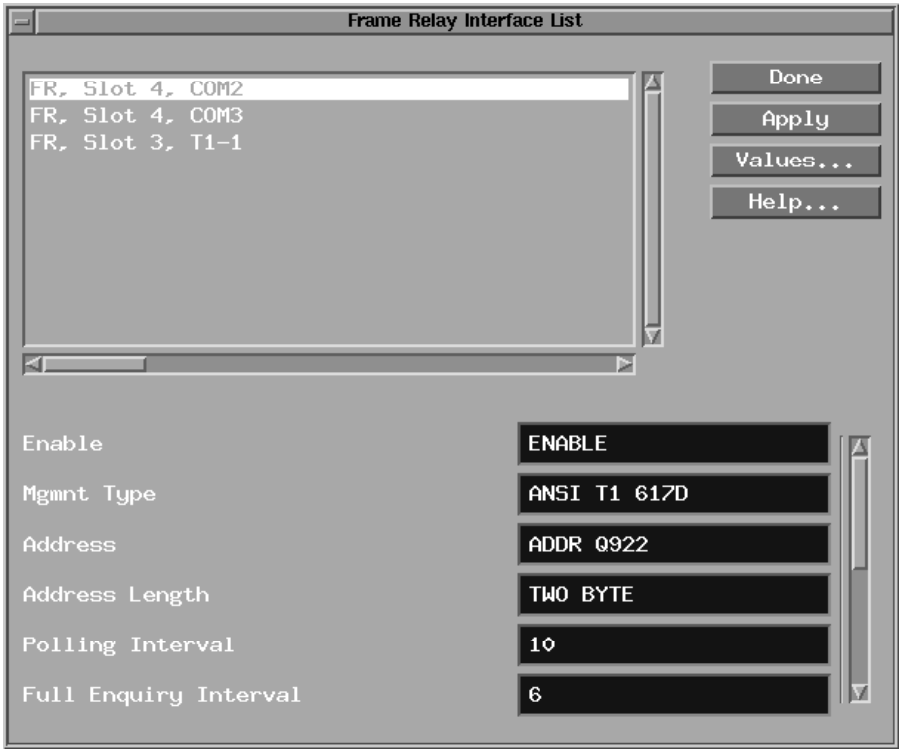

Figure A-1. Frame Relay Interface List Window

To access the window, complete the tasks in the following table.

Path to Frame Relay Interface List Window	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.

Parameter: Enable

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Enable

Options: Enable | Disable

Function: Enables or disables frame relay service on this port.

Instructions: Set to Disable if you want to disable frame relay service on this interface without deleting it. Set to Enable to reenable frame relay service, if you previously disabled it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.2

Parameter: Mgmnt Type

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: ANSI T1.617D

Options: DLCMI None | Rev 1 LMI | ANSI T1.617D | CCITT Annex A | LMI Switch | Annex D Switch | Annex A Switch

Function: Specifies the management protocol that the router and the frame relay network use to communicate status information. Routers connected back to back also use a management protocol to exchange status information.

DLCMI None provides no management interface between the router and the frame relay network. In the absence of management support, you must configure all PVCs manually.

Rev 1 LMI provides user-side management services as specified by Revision 1 of the Local Management Interface standard.

ANSI T1.617D provides user-side management services as specified in Annex D to ANSI standard T1.617-1991.

CCITT Annex A provides user-side management services as specified by the ITU-T (formerly CCITT).

LMI Switch offers limited management services for the DCE side of the connection as specified by Revision 1 of the Local Management Interface standard.

Annex D Switch provides limited management services for the DCE side of the connection as specified in Annex D to ANSI standard T1.617-1991.

Annex A Switch provides limited management services for the DCE side of the connection as specified by the ITU-T.

Instructions: Select the management protocol for the frame relay network. The LMI Switch, Annex D Switch, and Annex A Switch options are primarily for troubleshooting.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.6

Parameter: Address

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: ADDR Q922

Options: ADDR Q922 | ADDR Q922 November 90 | ADDR Q922 MARCH 90 | ADDR Q921

Function: Specifies the DLCI addressing type.

ADDR Q922 selects addressing as specified in the final version of the Q.922 standard. Q.922 provides for FECN, BECN, DE, and EA bits. While most Q.922 addresses are included within a 2-octet field, the standard allows for 3- and 4-octet address fields.

The November draft of ADDR Q922 differs from ADDR Q922 in dropping the D/C bit from the extended (3- and 4-byte) forms.

The March draft of ADDR Q922 differs from ADDR Q922 in defining an 11-bit DLCI and dropping the DE bit from the second octet of the address field.

ADDR Q921 differs from ADDR Q922 MARCH 90 in that it does not use FECNs or BECNs.

Instructions: Select the addressing type for the frame relay interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.8

Parameter: Address Length

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Two Byte

Options: Two Byte | Three Byte | Four Byte

Function: Specifies the length of the frame relay address field.

The length of this field determines the range of valid numbers for the DLCI number set in the Frame Relay PVC List window. See the DLCI Number parameter description for more details.

Instructions: Select the address length for the address field. This must match what the network specifies.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.9

Parameter: Polling Interval

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 10

Options: 5 to 30 seconds

Function: Specifies the interval between status inquiry messages that the router transmits. Status inquiry messages cause a network response in the form of a link integrity verification message or full status message. Successful completion of the request/response "handshake" verifies the status of the router/frame relay network link.

Instructions: We recommend that you accept the default value, 10 seconds. If the default value does not match what the network requests, enter a value that is appropriate for your network in the range of 5 to 30 seconds. Polling Interval does not function if you set Mgmnt Type to DLCMI None.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.10

Parameter: Full Enquiry Interval

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 6

Options: 1 to 255 polling intervals

Function: Specifies the interval between full status inquiry messages that the router transmits. Full status inquiry messages cause the network to send a full status report message, which lists all PVCs, the PVC status (active or inactive, and new or previously established). This parameter works with the Polling Interval parameter.

The default value, 6, tells the router to send a full status inquiry every 6 polling intervals. For example, with a polling interval of 10 and a full enquiry interval of 6, the router transmits a full status inquiry every 60 seconds; with a polling interval of 20 and a full enquiry interval of 30, the router transmits a full status inquiry every 10 minutes (600 seconds).

Instructions: Enter a value from 1 to 255, according to what the network dictates. Full Enquiry Interval does not function if you set Mgmnt Type to DLCMI None.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.11

Parameter: Error Threshold

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 3

Options: 0 to 2,147,483,647

Function: Together with the value of the Monitored Events parameter, establishes a criterion to evaluate the quality of the router/frame relay network connection.

If you accept the default values for both Error Threshold and Monitored Events, three status exchange errors in a sequence of four attempted exchanges will bring the connection down. With Error Threshold set to 5 and Monitored Events set to 10, five status exchange errors in a continuous sequence of ten attempted exchanges will bring the connection down.

After the network clears the connection, status exchanges continue, and the router monitors line integrity. When the number of consecutive, successful status exchanges is equal to the Error Threshold value, the router restores the frame relay connection.

Error Threshold and Monitored Events are nonfunctional if you set Mgmnt Type to DLCMI None.

Instructions: Enter the number of faulty status exchanges that will bring the connection down.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.1

Parameter: Monitored Events

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 4

Options: 0 to 2,147,483,647

Function: Together with the value of the Error Threshold parameter, establishes a criterion to evaluate the quality of the router/frame relay network connection. See the description of the Error Threshold parameter for more information.

Instructions: Enter the number of consecutive status exchanges you want the router to monitor.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.13

Parameter: **Multicast**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Disable

Options: Enable │ Disable

Function: Enables or disables support for frame relay multicast service.

Instructions: Set to Enable if your frame relay subscription service provides multicast service, and if this frame relay interface should receive multicast messages.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.16

Parameter: **Congestion Control**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Disable

Options: Enable │ Disable

Function: Enables or disables congestion control on this interface.

Instructions: Set to Enable to activate congestion control. This value tells the router to drop all outbound traffic destined for a PVC where congestion is occurring until the congestion clears. The value of this parameter affects all PVCs that you do not individually configure.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.22

Parameter: Congestion Timer

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 1

Options: 0.5 to 5 seconds, in 0.5-second intervals

Function: Specifies the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications set by the congestion counter parameter, the router stops transmitting data. The router resumes transmission once it stops receiving congestion notifications.

Instructions: Set the length of time the router should count congestion notifications from the network. If you set this parameter for a long time period, the router may be less likely to stop transmission for an intermittent congestion condition. However, the router may be slow to detect congestion, resulting in long transmission delays once the congestion has cleared. The value of this parameter applies to all PVCs that you do not individually configure.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.23

Parameter: Congestion Counter

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 20

Options: 1 through 500 notifications

Function: Indicates the maximum number of congestion notifications that the router can receive during the congestion timer period before it stops transmitting. If the router reaches the value set by this parameter, it determines the line is congested and stops transmitting.

Instructions: Specify the congestion count. The smaller the number, the more quickly the router detects congestion and stops transmitting. The value of this parameter applies to all PVCs that you do not individually configure.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.24

Parameter: Congestion Method

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Shutdown

Options: Shutdown │ Throttle │ Throttle Then Shutdown

Function: Specifies the method of congestion control:

- Shutdown terminates the VC when congestion occurs.
- Throttle queues traffic when congestion occurs; traffic resumes when congestion alleviates.
- Throttle Then Shutdown first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion.

Throttle and Throttle Then Shutdown are valid options only when traffic shaping is enabled.

Instructions: Select a setting appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.18

Service Record, DLCI, and PVC Parameters

The following sections describe the service record, DLCI, and PVC parameters and associated Site Manager screens:

- Required Service Name Parameter
- Required DLCI Parameter for Each PVC
- Default Parameters for Each PVC
- Optional Algorithm Parameter for Each Multiline Configuration

Required Service Name Parameter

The Frame Relay Service List window (Figure A-2) contains the Service Name parameter.

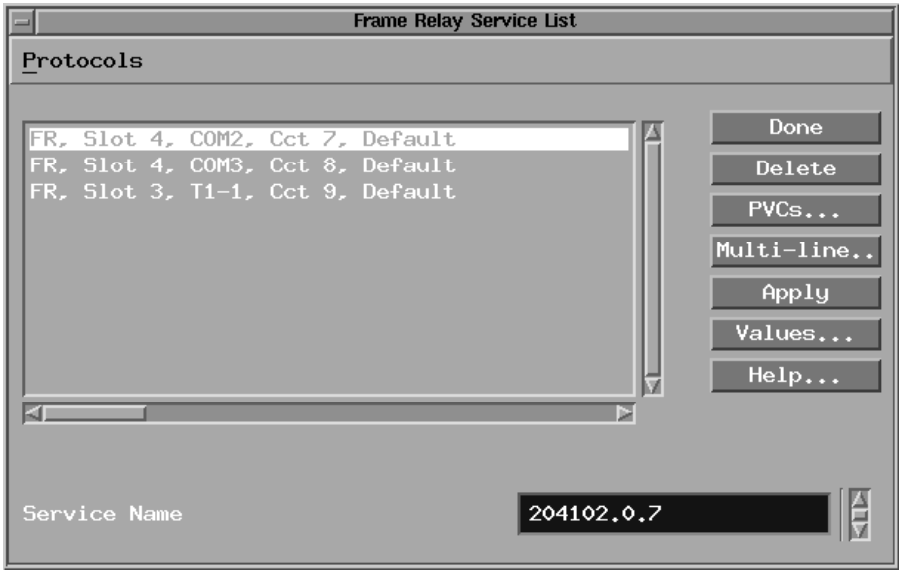

Figure A-2. Frame Relay Service List Window

To access the window, complete the tasks in the following table.

Path to Frame Relay Service List Window	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.

Parameter: Service Name

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window

Default: None

Options: <*line number*>.0.<*circuit number*>

Function: Identifies the service record.

Instructions: Site Manager assigns a unique name in the format given to each service record. There is no need to change this value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.7

Required DLCI Parameter for Each PVC

The Frame Relay PVC Add window (Figure A-3) contains the DLCI Number parameter.

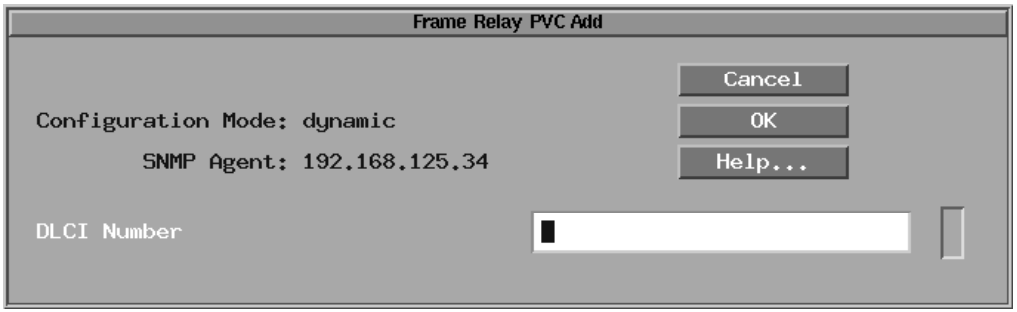

Figure A-3. Frame Relay PVC Add Window

To access the window, complete the tasks in the following table.

Path to Frame Relay PVC Add Window	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **PVCs** button.	The FR PVC List for Service window opens.
5. Click on the **Add** button.	The Frame Relay PVC Add window opens.

Parameter: DLCI Number

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window > **Add**

Default: None

Options: The frame relay switch provider assigns DLCI numbers. These assigned numbers are valid options.

Valid DLCI numbers vary based on the frame relay address length. The DLCI numbers that the switch provider assigns are generally in the following ranges:

2 byte -- 16 to 1007
3 byte -- 1024 to 6451
4 byte -- 131072 to 8257535

Function: Specifies the PVC identification number that the frame relay network uses to direct data. If you are running IP over frame relay, the router uses this number as the MAC address for an adjacent host. See *Configuring IP Services* for more information about adjacent hosts.

Instructions: Enter the decimal number that the frame relay provider assigns.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.4

Default Parameters for Each PVC

The FR PVC List for Service window (Figure A-4) contains the PVC parameters set automatically when you use the Add button to add a PVC.

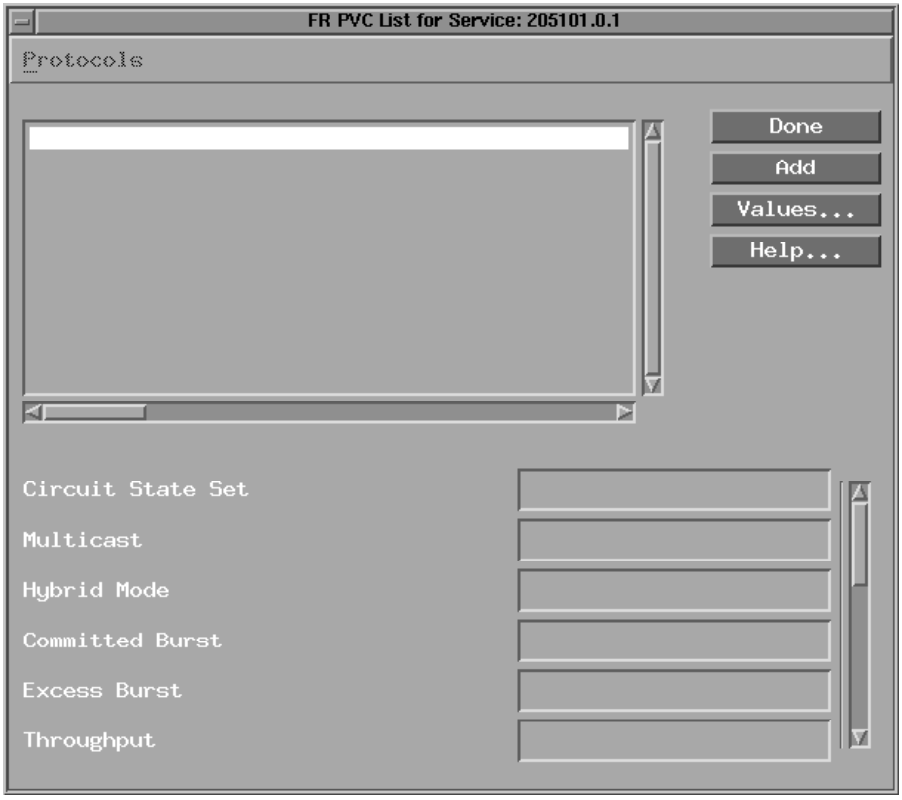

Figure A-4. FR PVC List for Service Window

To access the window, complete the tasks in the following table.

Path to FR PVC List for Service Window	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Interface List window opens.
4. Click on the **PVCs** button.	The FR PVC List for Service window opens.

Parameter: Circuit State Set

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window > **PVCs**

Default: Active

Options: Invalid │ Active │ Inactive

Function: Specifies the state of the PVC.

Instructions: Set to Active to indicate to a frame relay switch that the PVC is available for use. Set to Inactive to indicate that the PVC is configured, but not available for use, for example, before your switch provider actually activates the PVC. Choose Invalid if the PVC is configured, but the switch is unaware of it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.7

Parameter: Multicast

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window > **PVCs**

Default: Unicast

Options: Unicast │ Multicast

Function: Indicates whether this PVC is multicast or unicast.

Instructions: Set to unicast or multicast according to PVC type, as the frame relay switch provider instructs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.19

Parameter: Hybrid Mode

Path: Configuration Manager (select a connector) > Edit Connector window > **Edit Circuit** > Frame Relay Circuit Definition window > **Services** > Frame Relay Service List window > **PVCs >** Frame Relay PVC List for Service window

Default: OFF

Options: ON | OFF

Function: Allows you to use the same PVC for both routing and bridging.

Instructions: Set to ON if you want to enable both routing and bridging services. If not, accept the default.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.1.2.1.24

Parameter: Committed Burst

Path: Configuration Manager (select a connector) > Edit Connector window > **Edit Circuit** > Frame Relay Circuit Definition window > **Services** > Frame Relay Service List window > **PVCs >** Frame Relay PVC List for Service window

Default: 0

Options: 0 to 2,147,483,647 bits

Function: The maximum number of bits that a VC can transmit during the VC's burst period (Tc) when congestion is occurring. To enable traffic shaping, this parameter and the Throughput parameter (CIR) must both be greater than zero. The Committed Burst (Bc) value should be lower than the Throughput.

Instructions: Enter a value within the given range. We recommend that you set this parameter to 1/4 of the CIR unless this VC is sending frames larger than that size. If the VC is sending large frames, increase the value of this parameter to accommodate the size of those frames.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.16

Parameter: Excess Burst

Path: Configuration Manager (select a connector) > Edit Connector window > **Edit Circuit** > Frame Relay Circuit Definition window > **Services** > Frame Relay Service List window > **PVCs >** Frame Relay PVC List for Service window

Default: 0

Options: 0 to 2,147,483,647

Function: This value is added to the Committed Burst value to determine the maximum number of bits that may be transmitted during the VC's burst period when there is no congestion. The Excess Burst plus the Committed Burst must be less than or equal to the line speed.

Instructions: Enter a value within the given range.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.17

Parameter: Throughput

Path: Configuration Manager (select a connector) > Edit Connector window > **Edit Circuit** > Frame Relay Circuit Definition window > **Services** > Frame Relay Service List window > **PVCs >** Frame Relay PVC List for Service window

Default: 0

Options: 0 to 2,147,483,647

Function: The rate in bits per second at which data travels over this VC when no congestion is occurring. To enable traffic shaping, this parameter and the Committed Burst parameter must be set to values greater than zero.

Instructions: Your carrier supplies the CIR or throughput value, which you enter in this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.18

Parameter: Congestion Control

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window > **PVCs**

Default: Inherit

Options: Disable | Enable | Inherit

Function: Enables or disables congestion control on this interface.

Instructions: Set to Enable to activate congestion control. This value tells the router to drop all traffic destined for a congested PVC until the congestion clears. Select Disable to deactivate congestion control. Accept the default, Inherit, if you want the Congestion Control setting for this PVC to match the setting you specify for the frame relay Interface Congestion Control parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.25

Parameter: Congestion Timer

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window > **PVCs**

Default: 1

Options: 0.5 to 5 seconds, in 0.5-second intervals

Function: Specifies the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications set by the Congestion Counter parameter, the router stops transmitting data. The router resumes transmission once it stops receiving congestion notifications.

Instructions: Set the length of time the router should count congestion notifications from the network. If you set this parameter for a long time period, the router may be less likely to stop transmission for an intermittent congestion condition. However, the router may be slow to detect congestion, resulting in long transmission delays once the congestion has cleared.

If you set the Congestion Control parameter to Inherit, the PVC uses DLCMI for congestion control, not the value of this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.27

Parameter: Congestion Counter

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window > **PVCs**

Default: 20

Options: 1 through 500 notifications

Function: Sets the maximum number of congestion notifications that the router can receive during the Congestion Timer period before it stops transmitting.

Instructions: Specify the congestion count. The smaller the number, the more quickly the router detects congestion and stops transmitting. Note, however, that if you set the Congestion Control parameter to Inherit, the PVC uses DLCMI for congestion control, not the value of this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.28

Parameter: Congestion Method

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window > **PVCs**

Default: Inherit

Options: Shutdown │ Throttle │ Throttle Then Shutdown │ Inherit

Function: Specifies the method of congestion control.

- Inherit specifies that this VC will use the value of the Interface Congestion Method parameter.
- Shutdown terminates the VC when congestion occurs.
- Throttle queues traffic when congestion occurs; traffic resumes when the congestion alleviates.
- Throttle Then Shutdown first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate the congestion.

Throttle and Throttle Then Shutdown are valid options only when traffic shaping is enabled.

Instructions: Choose a setting appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.33

Parameter: Compression Control

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window > **PVCs**

Default: Enable

Options: Enable | Disable

Function: Enables or disables data compression for this service record.

Instructions: Accept the default, Enable, or select Disable if you decide not to use data compression for this service record.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.29

Optional Algorithm Parameter for Each Multiline Configuration

The Services Multiline With window (Figure A-5) contains the Multiline Algorithm to Choose Line parameter.

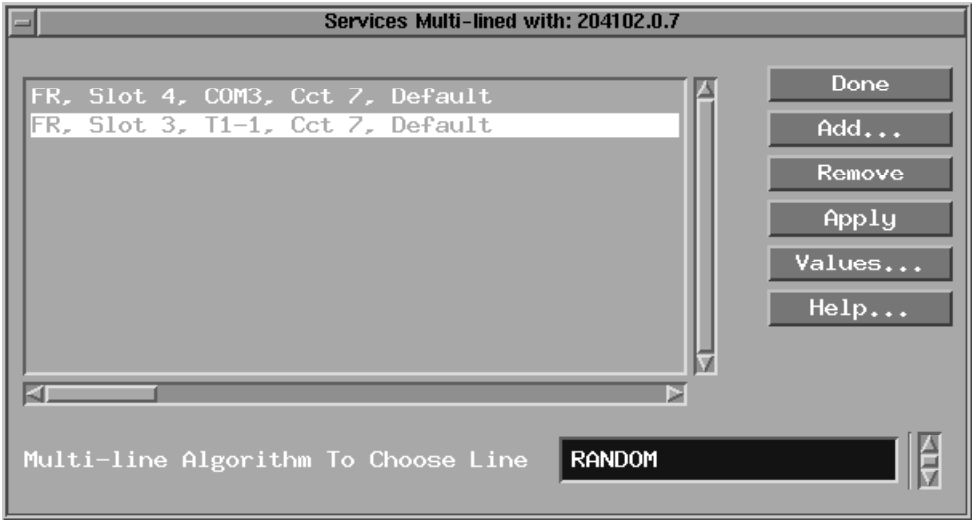

Figure A-5. Services Multi-line with Window

To access the window, complete the tasks in the following table.

Path to Services Multi-line with Window	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **Multiline** button.	The Services Multi-line with window opens.

This window lets you:

- Click on **Add** to add multiline services to a circuit. The Add Multiline Services window opens (Figure A-6). Click on a circuit entry and click on **Select**. When you do this, the circuit entry moves from the Add Multiline Services window to the Services Multiline With window. The Add Multiline Services window closes.
- Specify how a multiline circuit distributes traffic by setting the Multiline Algorithm to Choose Line parameter.

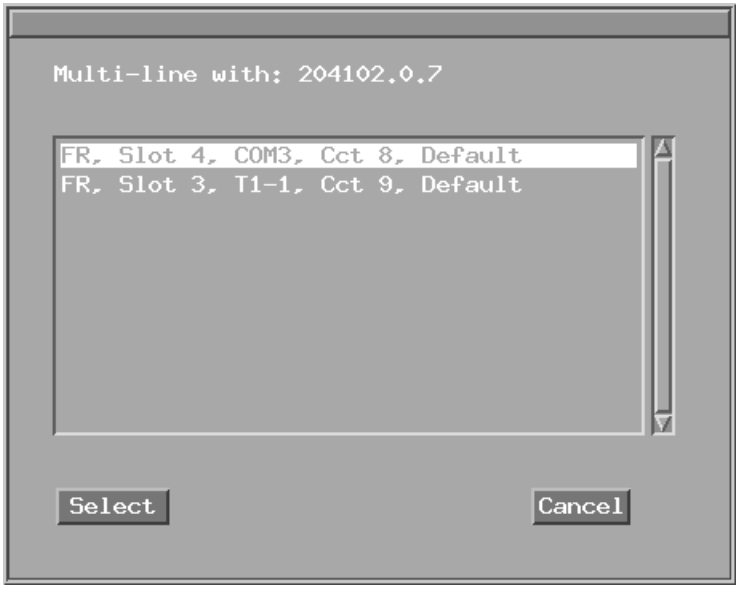

Figure A-6. Add Multiline Services Window

Parameter:	**Multiline Algorithm to Choose Line**
Path:	Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > **Services** > Frame Relay Service List window > **Multiline**
Default:	None
Options:	Random | Address Based
Function:	Specifies how the multiline circuit distributes traffic over its data paths.
Instructions:	Select Random to send data alternately over the two paths. This method ensures even distribution among the lines, but the packets arrive out of sequence. Select Address Based if the traffic between the same source and destination address pair is always going over the same data path. This method ensures the data arrives in sequence.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.4.1.1.23

Appendix B
Frame Relay Default Settings

This appendix lists the default parameter settings for frame relay services. Use the Configuration Manager to edit any of the default settings listed here.

Table B-1. Frame Relay Interface Parameters

Parameter	Default
Enable	Enable
Mgmnt Type	ANSI T1.617D
Address	Addr Q922
Address Length	Two Byte
Polling Interval	10 seconds
Full Enquiry Interval	6
Error Threshold	3
Monitored Events	4
Multicast	Disable
Congestion Control	Disable
Congestion Timer	1 second
Congestion Counter	20 notifications
Congestion Method	Shutdown

Table B-2. Frame Relay Service Record, DLCI, and PVC Parameters

Parameter	Default
Service Name	None
DLCI Number	None
Circuit State Set	Active
Multicast	Unicast
Hybrid Mode	OFF
Committed Burst	0
Excess Burst	0
Throughput	0
Congestion Control	Inherit
Congestion Timer	1 second
Congestion Counter	20 notifications
Congestion Method	Inherit
Compression Control	Enable

Table B-3. Multiline Parameter

Parameter	Default
Multiline Algorithm to Choose Line	None

Index

Q

R

S

T

V

W