Configuring DLSw Services

BayRS Version 13.00
Site Manager Software Version 7.00

BCC Version 4.05

Part No. 303523-A Rev. 00
October 1998

Bay Networks Where Information Flows.™

Bay Networks Where Information Flows.™

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FRE, LN, Optivity, PPX, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayRS, BaySecure, BayStack, BayStream, BCC, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, FN, IP AutoLearn, PathMan, RouterMan, SN, SPEX, Switch Node, System 5000, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

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

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

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

Chapter 2
DLSw Implementation Notes

Chapter 3
DLSw Configuration Overview

Chapter 4
Starting DLSw

Chapter 5
Editing DLSw Parameters

Chapter 6
Using DLSw Prioritization

Appendix A
DLSw Default Settings

Appendix B
Criteria for DLSw Prioritization

Appendix C
Troubleshooting DLSw

Index

Figures

Tables

Preface

This guide describes Data Link Switching (DLSw) and what you do to start and customize DLSw services on a Bay Networks® router.

Before You Begin

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

- Install the router (see the installation guide 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 BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)

Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.
Example: If the command syntax is:

ping *<ip_address>*, you enter:
ping 192.32.10.12

bold text

Indicates text that you need to enter and command names and options.
Example: Enter **show ip** {**alerts** | **routes**}

Example: Use the **dinfo** command.

braces ({})

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.
Example: If the command syntax is:

show ip {**alerts** | **routes**}, you must enter either:
show ip alerts or **show ip routes**.

brackets ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.
Example: If the command syntax is:

show ip interfaces [**-alerts**], you can enter either:
show ip interfaces or **show ip interfaces -alerts**.

italic text

Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.
Example: If the command syntax is:

show at <*valid_route*>
valid_route is one variable and you substitute one value for it.

`screen text`

Indicates system output, for example, prompts and system messages.
Example: `Set Bay Networks Trap Monitor Filters`

separator (>)

Shows menu paths.
Example: Protocols > IP identifies the IP option on the Protocols menu.

vertical line (|)

Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.
Example: If the command syntax is:

show ip {**alerts** | **routes**}, you enter either:
show ip alerts or **show ip routes**, but not both.

Acronyms

APPN	Advanced Peer-to-Peer Networking
BAN	Boundary Access Node
BNI	Boundary Node Identifier
BNN	Boundary Network Node
DLSw	data link switching
DLCI	data link connection identifier
FDDI	Fiber Distributed Data Interface
FEP	front-end processor
FRAD	Frame Relay Access Device

FIFO	first-in first-out
IP	Internet Protocol
LLC	Logical Link Control
MAC	media access control
MTU	maximum transmission unit
NCP	network control program
QLLC	Qualified Logical Link Control
RH	request header
RIF	routing information field
RNR	receiver not ready
RR	receiver ready
PVC	permanent virtual circuit
SAP	service access point
SDLC	Synchronous Data Link Control
SNA	Systems Network Architecture
SRB	source route bridging
SSP	Switch-to-Switch Protocol
TH	transmission header
TCP/IP	Transmission Control Protocol/Internet Protocol
VTAM	virtual telecommunications access method
XID	exchange identification

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, or information about educational services, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

Or telephone the Bay Networks Technical Solutions Center at:

800-2LANWAN

Chapter 1
Data Link Switching Overview

This chapter presents information about Data Link Switching (DLSw), as follows:

- DLSw Networking Overview
- RFC 1795 Support
- DLSw Version 2 Unicast UDP Support
- RFC 2166 Multicast Support
- DLSw Single-Switch and Dual-Switch Services
- SDLC Support
- Frame Relay Support
- QLLC Support
- DLSw/APPN Boundary Function
- DLSw Backup Peer Support
- DLSw Filtering

You should review this chapter if you are responsible for configuring DLSw on one or more Bay Networks routers. If you are already familiar with DLSw concepts, you can go directly to Chapter 2, “DLSw Implementation Notes,” for more detailed information about DLSw on Bay Networks routers.

DLSw Networking Overview

DLSw provides a standards-based mechanism for reliably transporting connection-oriented SNA and NetBIOS data across a network. Originally defined in RFC 1434, and currently in RFC 1795 with additional enhancements defined in DLSw Version 2 and RFC 2166, DLSw resolves the issues associated with transporting SNA and NetBIOS information across a multiprotocol backbone.

Specifically, DLSw:

- Prevents sessions from timing out due to slow network response time
- Automatically reroutes traffic around failed links
- Improves response time by reducing network overhead
- Enables multiple locations to interconnect without requiring a network manager to reconfigure existing bridges

Additionally, the Bay Networks DLSw implementation provides several benefits, including:

- Bay Networks symmetric multiprocessor architecture, providing a highly scalable and reliable implementation
- Advanced flow control, ensuring that the router-based network delivers information as reliably as existing SNA networks
- Integrated SDLC-to-LLC2 conversion, enabling the customer to reduce the cost of front-end processor (FEP) ports (for example, 3745), maintenance and software
- RFC 1490 (LLC2 over Frame Relay) support, enabling a Bay Networks router to communicate across a Frame Relay network directly to a front-end processor or other device that supports this protocol
- DLSw prioritization, allowing preferred DLSw traffic to receive higher priority than other traffic

The Bay Networks DLSw implementation is fully interoperable with RFC 1434, RFC 1795, and RFC 2166 DLSw implementations.

DLSw runs on all Bay Networks router platforms using local and wide area network facilities, including:

- LLC2 media, including Ethernet, Token Ring, Frame Relay, and ATM LANE
- Other media using source route bridging (SRB) formats, including FDDI, SMDS, Frame Relay, Point-to-Point (PPP), and ATM (RFC 1483)
- SDLC links in point-to-point and multipoint configurations
- X.25 links using the Qualified Link Level Control (QLLC) protocol

You can use DLSw services to support connections between SNA and NetBIOS systems on one type of network (such as Token Ring/802.5) and systems on different types of networks (such as Frame Relay).

Note: In this manual, the term LAN refers to all SRB types of LANs and transparent bridge Ethernet/802.3 LANs. SRB LANs include, but are not limited to, Token Ring/802.5, FDDI, Ethernet/802.3, SMDS, Frame Relay, and other synchronous media protocols. See *Configuring Bridging Services* for more information on the media that SRB supports.

RFC 1795 Support

RFC 1795, called DLSw Version 1, is an implementation of DLSw developed by a consortium of vendors. RFC 1795 supersedes the original DLSw specification, RFC 1434. Starting with Version 11.0, Bay Networks DLSw routers support RFC 1795. These routers are fully compatible with Bay Networks routers that support the original RFC 1434 specification with Version 10.0 or earlier software.

Differences Between RFC 1795 and RFC 1434

Based on RFC 1434, RFC 1795 describes features that were not originally published, as well as modifications to the standard. RFC 1795 includes:

- Modified frame format for session setup, including a field for the largest frame size.
- Directed broadcast CANUREACH and ICANREACH control frames. This feature reduces broadcasting over the network.

- Capabilities exchange, allowing routers to exchange resource information about each other. Capabilities exchange flows operate in three categories:
  - Fixed information, such as an organization’s software version
  - Customized information, where one router transfers the information to another router
  - Negotiation, where routers negotiate the use of proprietary functions (and only if both routers support the functions under negotiation)
- Rate-based pacing, a new standard for flow control between routers. Flow control allows a DLSw router to inform another router to slow down or stop sending data when the receiving buffer(s) fill up. Rate-based flow control uses a windowing mechanism that allows the routers to send more or fewer packets, based on the state of the last receive window. If the router successfully receives the last transmission, it informs the sending router to continue to send more packets. Flow control is essential for successful delivery of SNA and NetBIOS data.

DLSw Version 2 Unicast UDP Support

DLSw Version 2 and RFC 2166 are terms that can typically be used interchangeably. However, Bay Networks refers to DLSw Version 2 slightly differently. Bay Networks implementation, called DLSw Version 2, offers only Unicast UDP support, while the RFC 2166 implementation provides full multicast support.

Unicast UDP support is provided beginning with BayRS Version 11.02. This implementation allows:

- The initial session establishment request (CanuReach) to be sent via Unicast UDP (as opposed to using TCP as in RFC 1434 and RFC 1795)
- Peer type configuration (TCP, UDP, and Unknown peers)
- You to configure dual uni-directional or single bi-directional TCP connections

The DLSw RFC Version parameter allows you to set up your configuration for DLSw Version 2. A router that you configure for DLSw Version 2 can also communicate with routers running RFC 1434 and RFC 1795 implementations.

UDP Explorer Frames

If a TCP/IP session is not active, the local router can send UDP explorer frames across the network to locate the destination MAC address. When the local router finds the destination MAC address, the destination router returns a UDP response. The local router, as well as the router returning the UPD response, then establish a TCP/IP session between them. Using UDP explorer frames allows the sending router to “explore” the network before opening a TCP session, keeping a single router available to support a larger network.

TCP/IP sessions between routers establish across the network when a router locates a destination MAC address. When established, a TCP/IP session remains active between the routers until there are no remaining SNA/NetBIOS sessions, or if a TCP connection is idle over a configured time period.

If the local router cannot find the destination MAC address (no UDP response), the local router establishes TCP sessions with all entries in the Peer Table using either RFC 1795 or RFC 1434 protocol standards if the destination MAC is an unknown peer type.

You can configure DLSw to use UDP explorer frames to establish TCP/IP sessions with DLSw peers by setting the Transport Type parameter.

TCP, UDP, and Unknown Peer Types

With DLSw Version 2 unicast, you can configure DLSw peers as TCP, UDP, or Unknown. If the peer type is unknown, the local router sends UDP explorer frames to establish a connection. If the local router does not receive a UDP response after a number of attempts, the local router will try to fall back to earlier DLSw RFCs to establish the connection.

If the peer type is TCP, then a TCP connection establishes when you start the local router. If the peer is UDP, a TCP connection establishes after the UDP explorer frames are correctly exchanged.

Refer to Chapter 5 for information on the Transport Type and SNA Fallback Attempts parameters.

Single TCP/IP Connection

DLSw Version 2 uses a single full-duplex TCP session to transport data. Using a single full-duplex TCP/IP session instead of two half-duplex sessions reduces the amount of time and memory required to establish the TCP connection.

RFC 2166 Multicast Support

In addition to IP unicast broadcast services, DLSw provides IP multicast support. The capability to send and receive both IP multicast traffic and IP unicast traffic makes the Bay Networks implementation of DLSw fully compliant with RFC 2166.

RFC 2166 is an implementation of DLSw that was developed by the APPN Implementors Workshop, a consortium of vendors.

RFC 2166 provides:

- Improvements for scalability by allowing:
  - The initial session establishment request (CanuReach) to be sent using Multicast IP
  - Only single bi-directional TCP connection to be used
  - TCP connections to established (and disconnected) on demand and as needed
- Reason codes with the HALT_DL and HALT_DL_NOACK SSP messages to provide more diagnostic information

Differences Between RFC 2166 and RFC 1795

The following comparison of RFC 2166 with earlier DLSw RFCs 1434 and 1795 shows how RFC 2166 reduces the amount of broadcast traffic on the network.

- Under RFCs 1434 and 1795, an end station (an SNA or NetBIOS application) that wants to establish a network connection first sends a DLSw SSP CanuReach (or NETBIOS_NQ) message to all routers that are part of the DLSw network. In a large network with many end stations, these connection attempts result in a large number of packets traveling on the network. In addition, under RFCs 1434 and 1795, TCP connections must be constantly maintained between all participating routers within the DLSw network.

- Under RFC 2166, network connections are established only when needed and maintained only as long the end stations require. In addition, end stations use multicast IP to send the initial CanuReach (or NetBIOS) messages, thus reducing the amount of traffic on the network.

By default, DLSw operates in RFC 1434 mode. You can use Site Manager to configure DLSw in RFC 2166 multicast mode. For instructions, see “Configuring DLSw for IP Multicasting” in Chapter 4.

Configuring IP Multicast Protocols on the Router

A router configured for DLSw with IP multicasting support must also be running:

- IP
- IGMP
- DVMRP, MOSPF, or both

You must configure IP on at least one slot on the router and assign an IP address to each DLSw slot as described in Chapter 4.

For complete information about IP multicasting and instructions for configuring IGMP, DVMRP, and MOSPF on the router, see *Configuring IP Multicasting and Multimedia Services*.

Assigning an IP Multicast Group Address to a Slot

In an IP multicasting network, a sender---or *source*---of IP multicast datagrams addresses each datagram to a *group* of receivers. An IP multicast group address is a Class D address (the high-order bits are set to 1110) from 224.0.0.0 to 239.255.255.255.

Note: Do not use addresses 224.0.0.0 through 224.0.0.255; these addresses are used for control purposes only.

On a router configured for DLSw multicasting, each DLSw slot is associated with an IP multicast group address. The router in Figure 1-1, for example, is running DLSw on slot 3. The network administrator has assigned the group address 224.0.10.0 to slot 3.

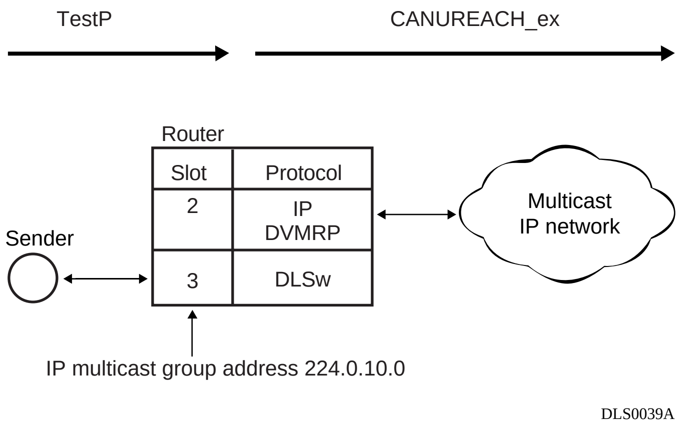


Figure 1-1. Addressing a Message to an IP Multicast Group

When DLSw receives a TestP message, the following steps occur:

1. DLSw converts the TestP message into a CANUREACH_ex message.
2. DLSw uses the IP multicast group address associated with slot 3 (224.0.10.0) as the destination address of the CANUREACH message.
3. DLSw passes the message to IP running on slot 2.
4. IP sends the message to the IP multicast network.

When the router receives a CANUREACH_ex message on a slot configured with IP, the reverse sequence occurs (Figure 1-2):

1. The router receives a CANUREACH_ex message.
2. IP determines that the CANUREACH_ex message is addressed to multicast group 224.0.10.0.
3. IP forwards the message to DLSw on slot 3.
4. DLSw converts the CANUREACH_ex message to a TestP message and sends it out a DLSw interface to the receiver.

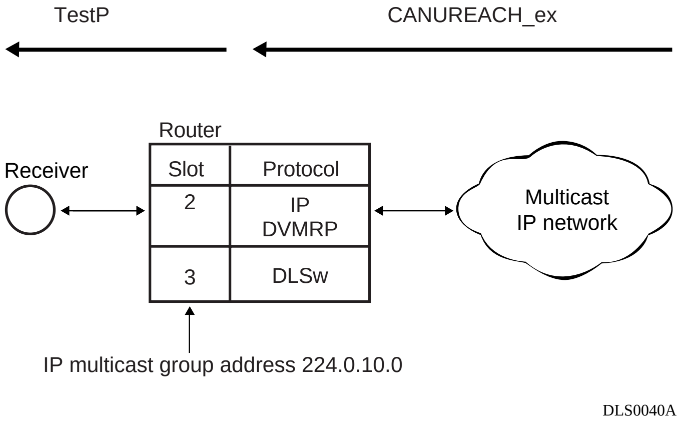


Figure 1-2. Receiving a Message Addressed to a Multicast Group

You can use Site Manager to specify an IP multicast group address and associate it with a DLSw slot or slots. For instructions, see “Configuring DLSw for IP Multicasting” in Chapter 4.

Sample Connection Using DLSw and IP Multicasting

Figure 1-3 shows a pair of routers running DLSw in RFC 2166 mode. On router A, IP and DVMRP are running on slot 2, and DLSw is running on slot 3. On router B, DLSw is running on slot 2, and IP and DVMRP are running on slot 3.

Router A connects to end station 1 through a DLSw interface on slot 3. Router A has an IP interface on slot 2 to the IP multicast network. Routers B and C are configured identically. Both connect to hosts through a DLSw interface on slot 2. Both have an interface to the IP network on slot 3.

On router A, the network administrator has assigned IP multicast group address 224.0.10.0 to DLSw slot 3. On router B, the network administrator has assigned group address 224.0.10.0 to DLSw slot 2

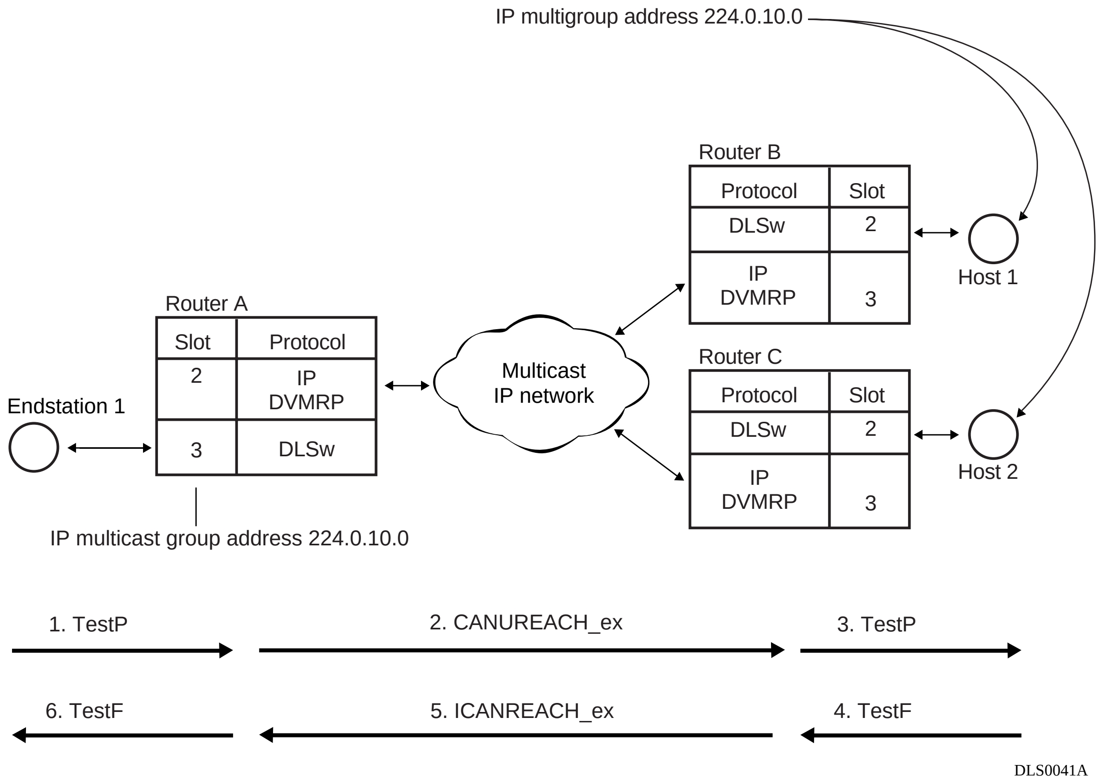


Figure 1-3. Multicast DLSw

When end station 1 generates an SNA TestP message, the following steps occur:

1. Router A receives the TestP message on slot 3.
2. Router A multicasts a CANUREACH_ex message on slot 2, using the group address 224.0.10.0.
3. Router B and C receive the CANUREACH_ex message and forward the message to slot 3, configured with the IP multicast group address.
4. Router B sends a TestP message on slot 3 to host 1.
5. Router C sends a TestP message on slot 3 to host 2.
6. Host 1 responds to the TestP message by sending a TestF message.
7. Router B receives the TestF message on slot 3.
8. Router B sends an ICANREACH_ex message on slot 2. (Router B sends this message in an IP unicast datagram.
9. Router A receives the ICANREACH_ex unicast message on slot 2 and forwards it to DLSw slot 3.
10. Router A sends a TestF message to end station 1.

DLSw Single-Switch and Dual-Switch Services

Bay Networks routers that you configure to support DLSw services can operate in two modes:

- A DLSw single-switch configuration involving a single local router with two (or more) interfaces configured for DLSw
- A DLSw dual switch-to-switch configuration involving paired routers, each connected to an intervening TCP/IP network

A Bay Networks router simultaneously supports both single- and dual-switch operation. Figure 1-4 illustrates DLSw single-switch and dual switch-to-switch networks.

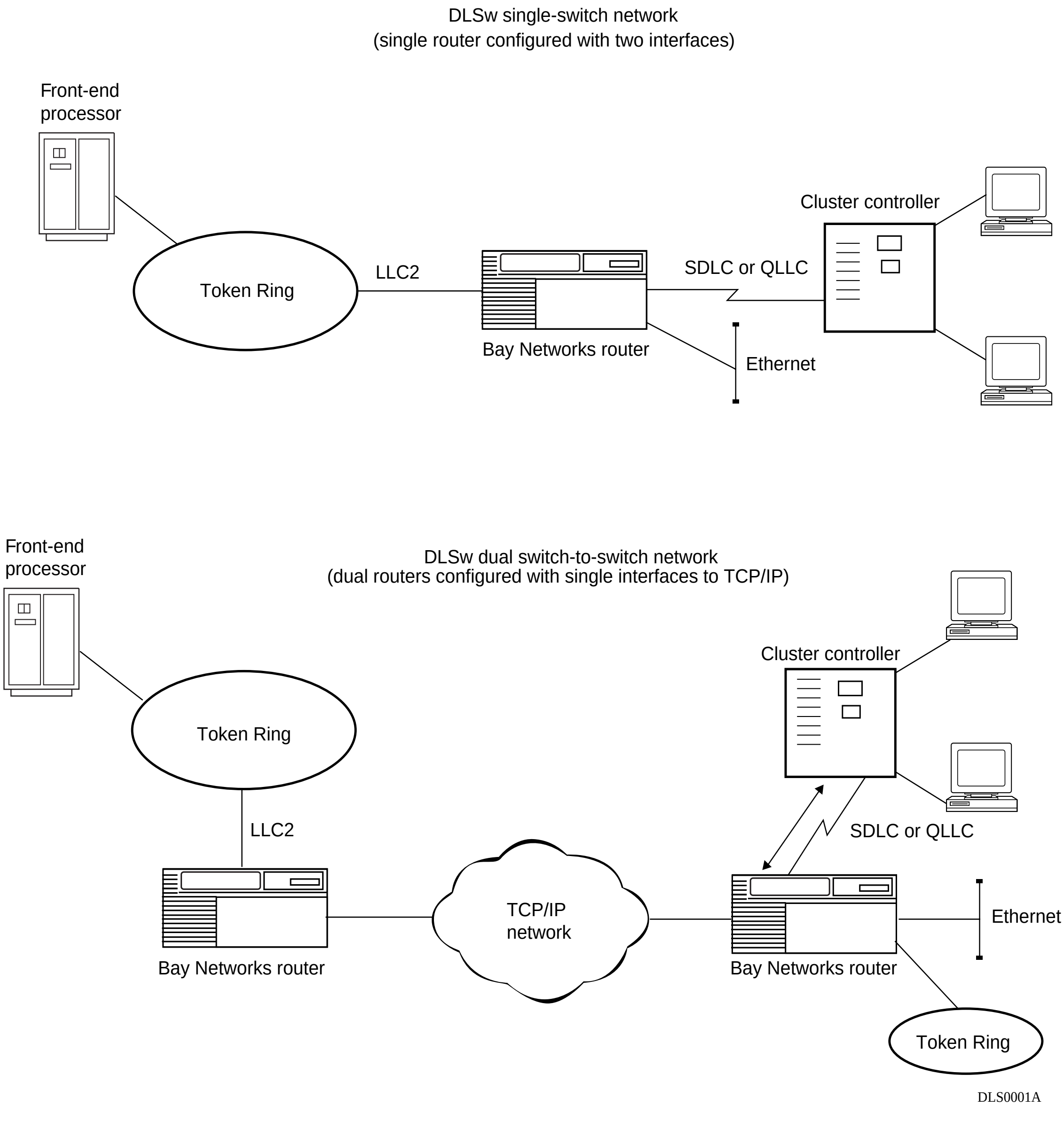


Figure 1-4. DLSw Single-Switch and Dual Switch-to-Switch Networks

Single-Switch Services

DLSw single-switch services enable the router to perform link level conversion, while providing services to ensure session integrity. Examples of single-switch conversions include:

- SDLC to Token Ring
- SDLC to Frame Relay (RFC 1490)
- Token Ring to Ethernet
- Ethernet to Bridged SNA over Frame Relay
- QLLC to Token Ring

Single-switch configurations provide services to attached devices and networks to ensure session availability, including:

- Local acknowledgment and termination of the LLC2, SDLC, or QLLC session
- 802.5 routing information field (RIF) caching
- MAC address and NetBIOS name caching

Figure 1-5 illustrates a sample network using a single Bay Networks router. The router can communicate with an IBM SNA processor, or other LAN gateway.

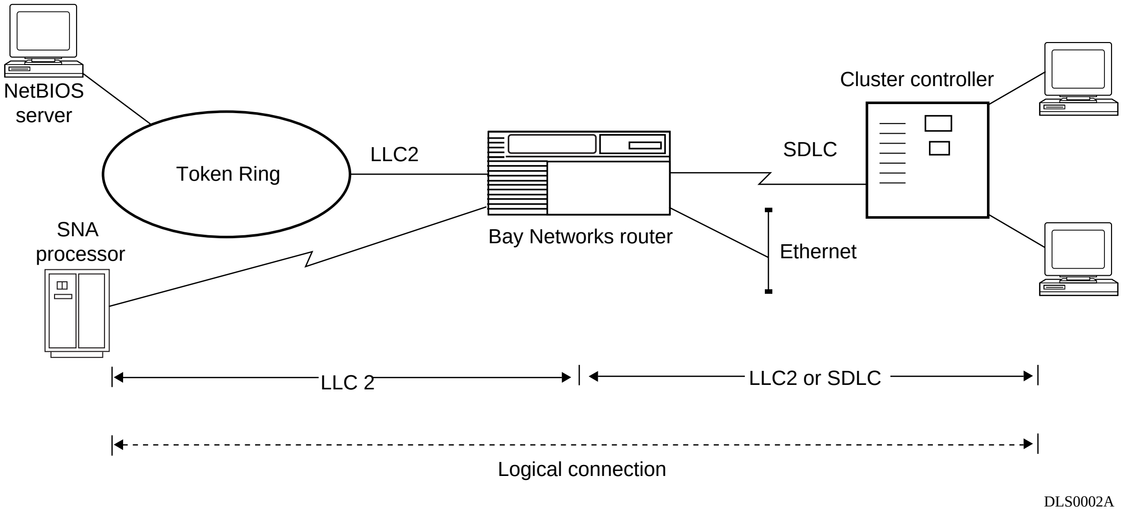


Figure 1-5. Bay Networks Single-Switch Router

There are three important types of single-switch conversion:

- FRAD operation
- SDLC-to-LLC2 conversion
- QLLC-to-LLC2 conversion

FRAD Operation

Single-switch services enable a Bay Networks router to function as a Frame Relay Access Device (FRAD). SNA devices are typically connected over a LAN or SDLC connection to the router, providing local termination. The router first connects to the Frame Relay (or other wide area) network, and then to an SNA processor using the Boundary Network Node (BNN) or the Boundary Access Node (BAN). BNN is the RFC 1490 standard. Refer to the “Frame Relay Support” section of this chapter for more information on BNN and BAN.

SDLC-to-LLC2 Conversion

Using single-switch conversion enables the router to convert incoming SDLC traffic into the appropriate format for forwarding to an attached LAN or Frame Relay network. The conversion does not require an intervening WAN.

Figure 1-6 illustrates a network using adjacent routers, each performing single-switch conversion. Between single switch routers, the LLC2 protocol is used.

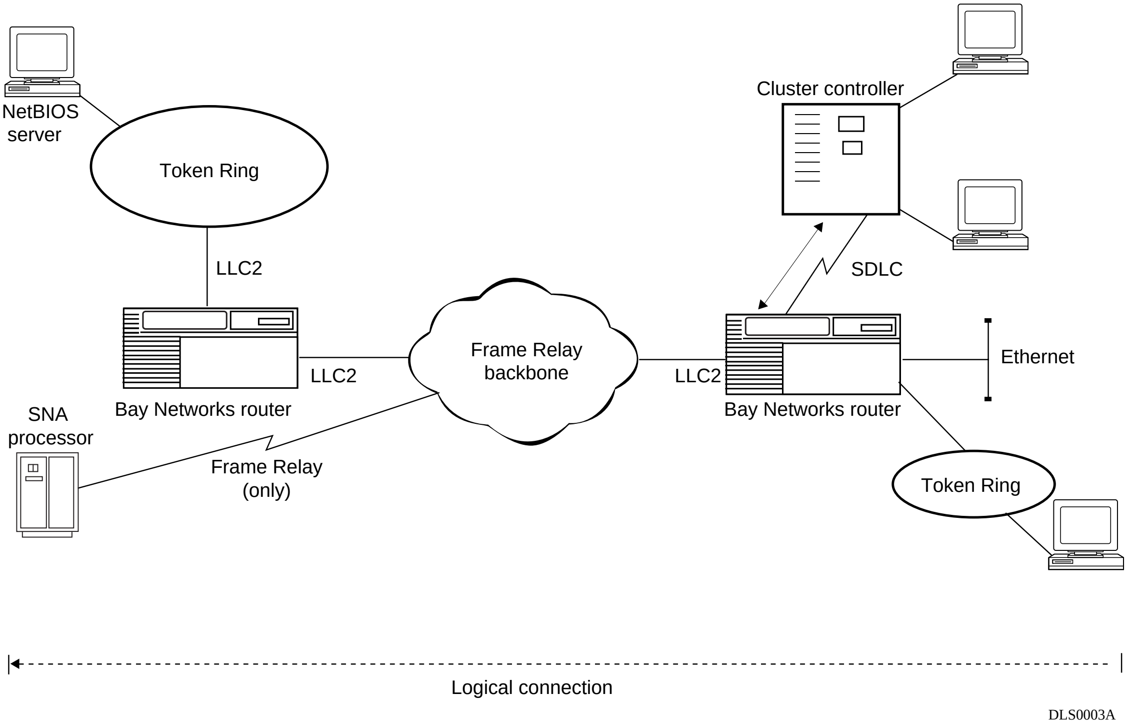


Figure 1-6. Bay Networks Adjacent Single-Switch Routers

QLLC-to-LLC2 Conversion

Using single-switch conversion enables the router to convert incoming QLLC traffic (received over an X.25 network) into the appropriate format for forwarding to an attached LAN or Frame Relay network. The conversion does not require an intervening WAN.

Dual-Switch Services

DLSw dual-switch services allow SNA and NetBIOS traffic to share a multiprotocol backbone. The DLSw standard specifies TCP/IP as the standard transport mechanism for SNA and NetBIOS across an internetwork.

DLSw dual-switch services uses TCP/IP between routers, unlike adjacent single-switch routers using LLC2. DLSw dual-switch services provide

- IP routing, permitting delivery over any available path
- TCP services, providing reliable data delivery, reduced network overhead, and flow control mechanisms to manage traffic

Packets are carried to an attached Bay Networks DLSw node where the data is translated into SSP datagrams. The data is then routed over the multiprotocol backbone to a remote Bay Networks DLSw node using an IP routing protocol. When the SSP datagram reaches the remote Bay Networks DLSw node, it is translated into the appropriate frame and carried to its destination.

Figure 1-7 shows how SNA devices use DLSw dual-switch services to communicate over TCP/IP. This differs from adjacent single-switch operation, which uses LLC2 on the backbone.

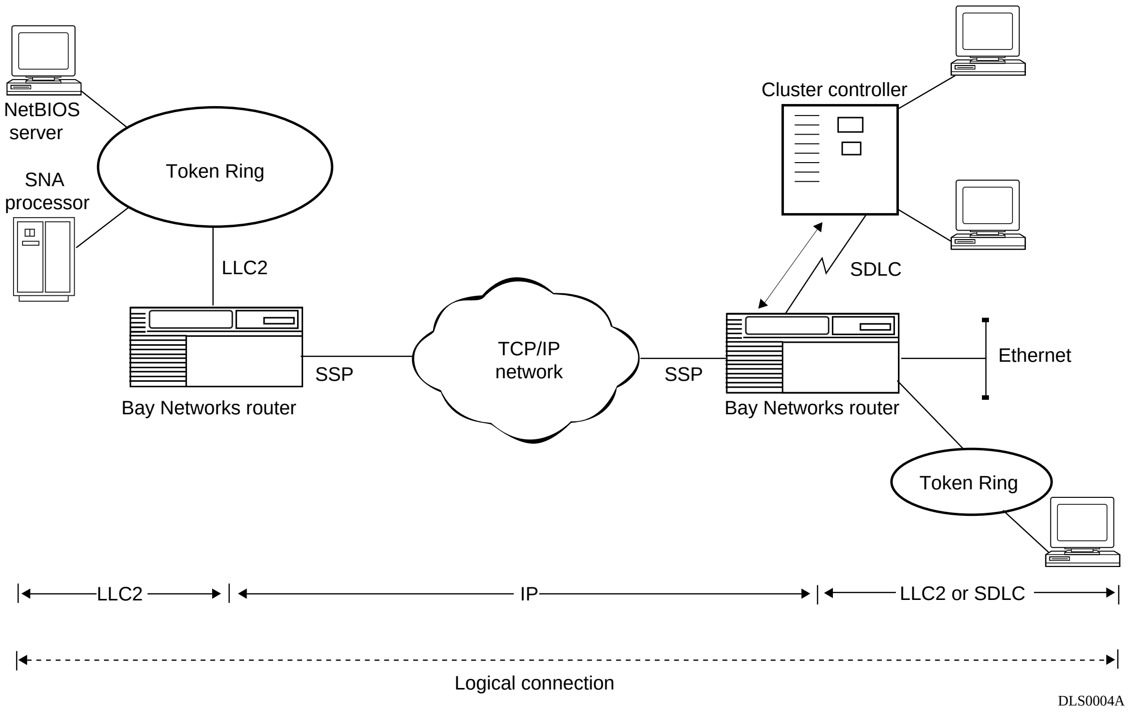


Figure 1-7. DLSw Dual-Switch Services for SNA Devices on LANs

SDLC Support

Integrated SDLC support merges the SDLC traffic with the multiprotocol traffic of LANs into a single network backbone. SDLC operates in DLSw single-switch routers, or in dual switch-to-switch networks, as illustrated in Figure 1-4.

Integrated SDLC conversion enables existing SDLC traffic to share a backbone network with LAN traffic without an intervening TCP/IP network. Traffic enters the DLSw router as SDLC and goes out the router as LLC2 over Token Ring or Ethernet. The destination endstation can reside on the Token Ring or Ethernet network directly connected to that DLSw router. SRB can forward the traffic through the network to a destination host or endstation. In this network, the local router performs the SDLC conversion, and forwards the traffic across the network to the host (Figure 1-8).

DLSw integrated SDLC supports devices configured as primary or secondary link stations to the router. A link station is a logical connection between adjacent nodes, where one node is a primary link station and the other node is a secondary link station.

When configured as an SDLC primary device, the router polls downstream cluster controllers, such as the IBM 3174 and the IBM 5394. When configured as a secondary device, the router responds to polls from the primary device.

You can use integrated SDLC in a point-to-point or multipoint topology. Point-to-point connects one SDLC device to another. Multipoint connects several secondary SDLC devices to one primary SDLC device. You specify the topology when you configure SDLC on the synchronous circuit.

For more information on the Bay Networks SDLC implementation, see *Configuring SDLC Services*.

Primary SDLC Support

A Bay Networks router configured as a primary device on an SDLC link can:

- Control the data link
- Issue commands
- Initiate error recovery procedures
- Serve as a PU 1.0, PU 2.0, or PU 2.1 device

The primary link station addresses and sends command frames to any or all secondary link stations on the network. Each frame carries the individual or group address of the station or stations to which the frame is directed. A secondary link station receives commands and responds to primary link station polls.

In both single and dual switch-to-switch networks, you must map the addresses of the SDLC devices to Token Ring/802.5 addresses. To map the addresses, you configure the SDLC devices as local devices, enabling them to appear to the network as natively attached LAN devices. Chapter 5 describes how to configure local devices.

Figure 1-8 illustrates DLSw single- and dual-switch networks where Bay Networks routers perform as primary SDLC nodes.

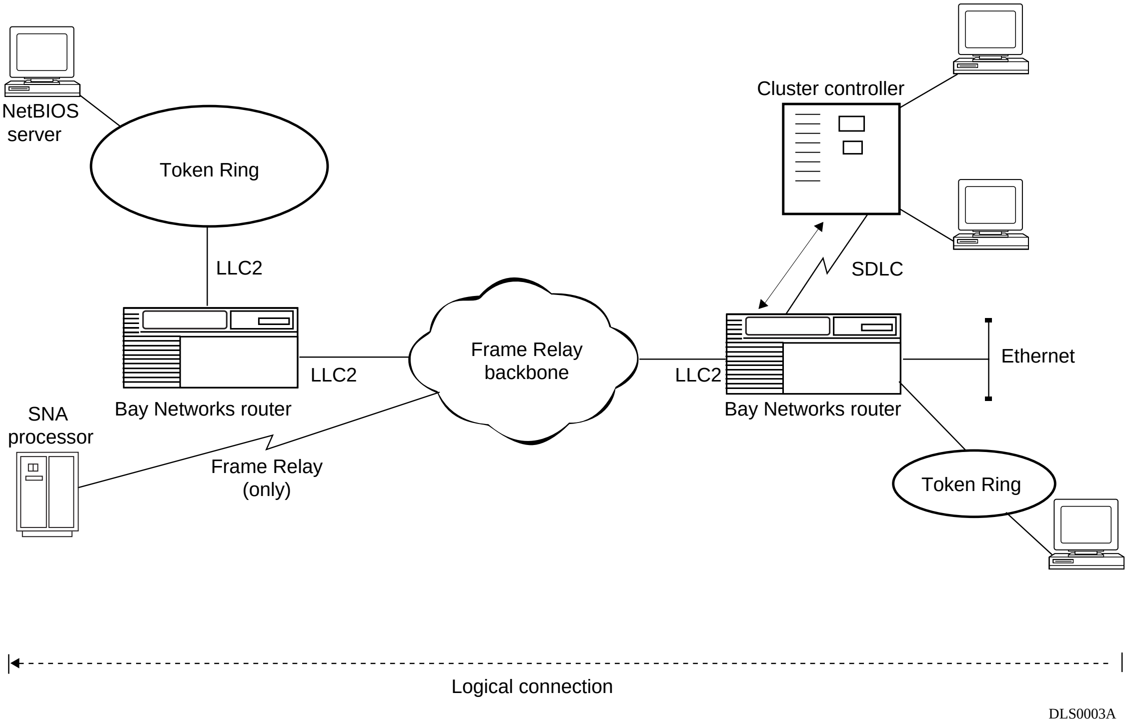


Figure 1-8. Primary SDLC Routers in Single-Switch DLSw Networks

Secondary SDLC Support

A Bay Networks router acting as a secondary device on an SDLC link can:

- Support a single or multiple SDLC link communicating to an FEP or other SNA host
- Allow SNA devices attached to multiple remote routers to share a single SDLC link to the FEP
- Attach to the FEP directly (using a null modem cable) or via a leased line

Figure 1-9 illustrates DLSw single- and dual-switch networks where Bay Networks routers serve as secondary SDLC nodes.

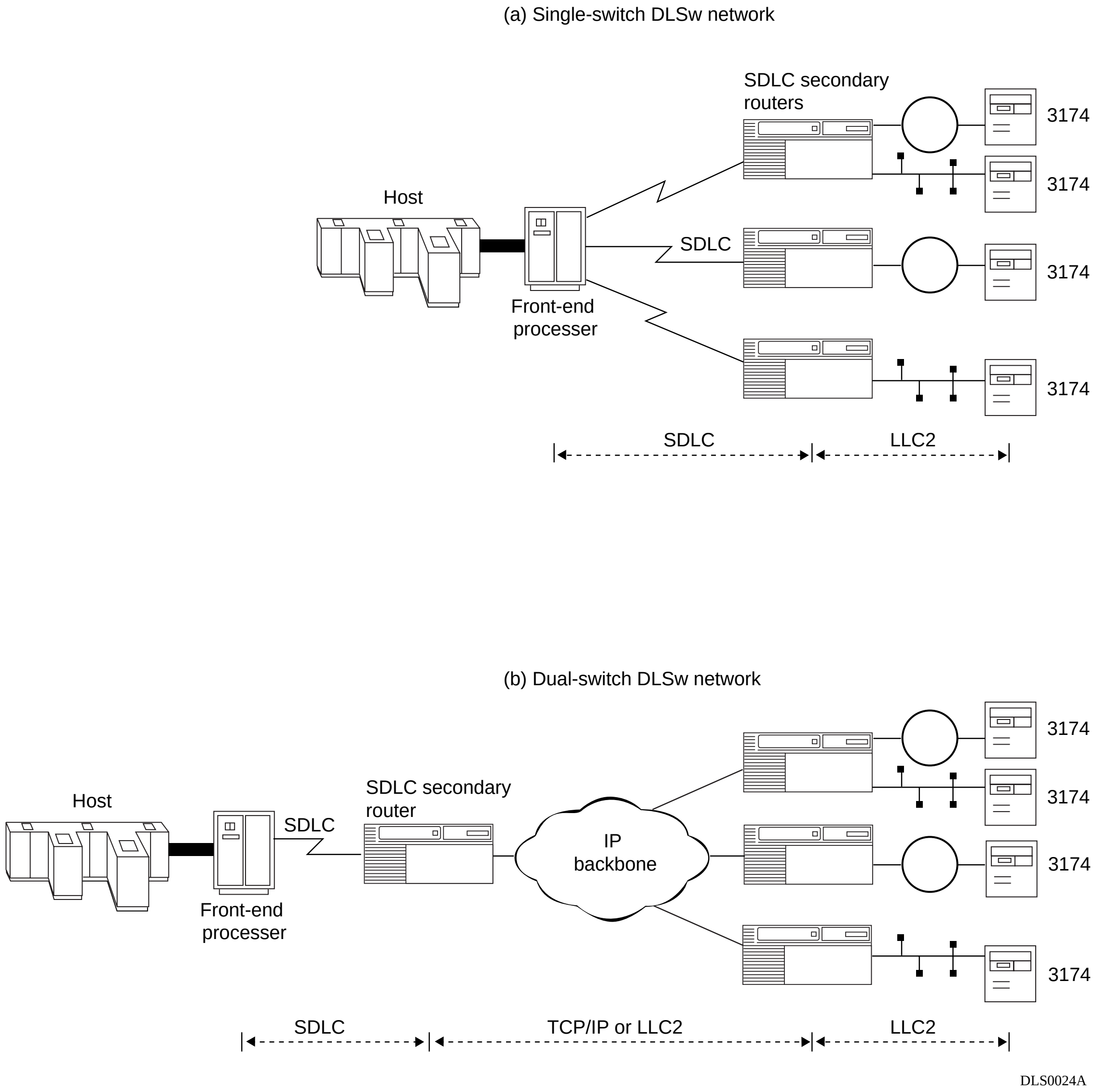


Figure 1-9. Secondary SDLC Routers in (a) Single- and (b) Dual-Switch DLSw Networks

Combining Primary and Secondary SDLC

Using primary and secondary SDLC services, a network can transport existing SDLC traffic over a router-based topology that:

- Enables existing SDLC traffic to use a high-speed multiprotocol backbone network
- Simplifies the migration to a router-based network, by incorporating SDLC traffic into the multiprotocol backbone without converting the existing endstations
- Locally acknowledges the SDLC protocol at each side of the router-based network, eliminating polling and acknowledgment traffic from the network backbone
- Allows high-speed links into the SNA host, improving response time

Figure 1-10 illustrates primary and secondary SDLC using single- and dual-switch services.

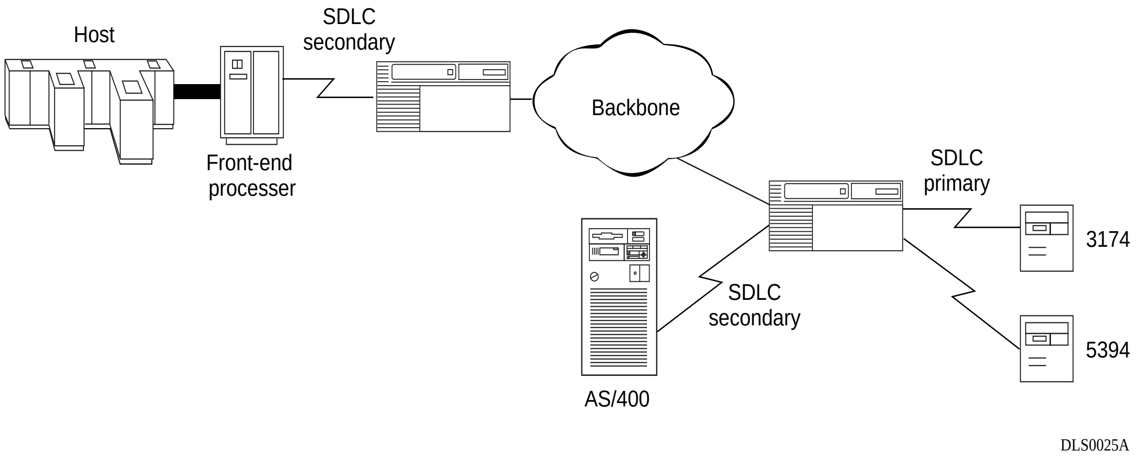


Figure 1-10. Combining Primary and Secondary SDLC

Frame Relay Support

Figure 1-11 illustrates the connection of a host through a Frame Relay network, in a configuration with multiprotocol traffic to other locations.

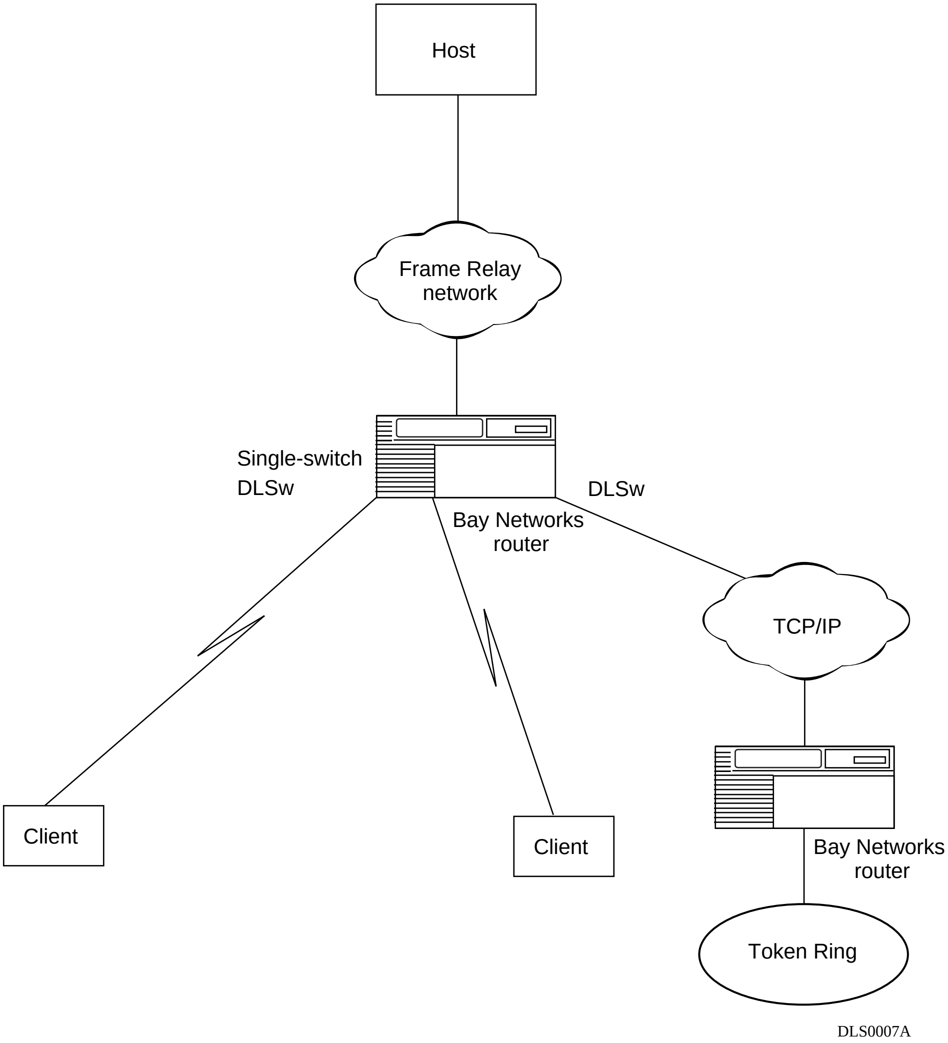


Figure 1-11. Sample Frame Relay Network

Bay Networks provides two ways to communicate directly with an SNA processor (such as an IBM 3745 or AS/400) over Frame Relay:

- Boundary Network Node (BNN)
- Boundary Access Node (BAN)

Boundary Network Node (RFC 1490)

BNN refers to RFC 1490, Routed SNA over Frame Relay. This implementation of LLC2 also complies with the Frame Relay Forum 3 (FRF.3), “Multiple Protocol Encapsulation over Frame Relay Implementation Agreements,” which defines how SNA traffic traverses a Frame Relay network.

BNN allows native SNA traffic (originating from SDLC, LAN- or WAN-attached devices) to communicate directly over public or private Frame Relay networks with an SNA processor. Devices can communicate with intermediate routing nodes, or in a single-switch configuration function as a FRAD.

Since BNN does *not* carry the destination and source MAC addresses in the network packets, the BNN format carries the fewest number of bits per packet and yields low network overhead. Therefore, you must explicitly define the PVC to carry the packet to its destination. You do this with the LLC2 Frame Relay Mapping Table. The mapping table consists of three fields:

- DLCI
- Remote (or Destination) MAC
- Local MAC (or Source) MAC

Each entry requires that you specify the Remote MAC, Local MAC, or both. A packet that matches this entry is then forwarded to the specified DLCI.

Boundary Access Node

BAN is an IBM router enhancement. BAN refers to the RFC 1490 specification for Bridged SNA over Frame Relay. The associated IBM NCP 7.3 enhancement is called the Boundary Node Identifier (BNI).

Since BAN carries the destination and source MAC addresses in the network packets, this format carries more bits per packet and requires less configuration.

Standard BAN uses the SRB frame format with local termination. Bay Networks routers select BAN source route encapsulation when you configure the Frame Relay network.

QLLC Support

QLLC provides reliable transport for SNA devices connected over an X.25 network. This support enables QLLC-attached devices to connect to a non-X.25 backbone, and allows non-QLLC devices to connect to an X.25 network. Both single- and dual-switch DLSw networks can operate over X.25 links using QLLC.

For detailed information about configuring QLLC prior to adding DLSw single- and dual- switch services, refer to *Configuring X.25 Services*.

DLSw/APPN Boundary Function

The DLSw/APPN boundary function (BF) allows DLSw to provide remote communications via an IP backbone and provide access over this backbone from enterprise-level applications using an APPN network.

The DLSw/APPN boundary function is implemented within a central APPN network node. The BF accepts traditional PU2 traffic supported by DLSw and routes it over APPN to the appropriate partner, typically a mainframe-based application.

DLSw/APPN Network Configurations

The DLSw/APPN boundary function can reside wherever your APPN backbone network is located.

In Figure 1-12, for example, the DLSw/APPN boundary function resides in an enterprise router located within the domain of the APPN mainframe or AS/400 data center. The corporate network is an IP network.

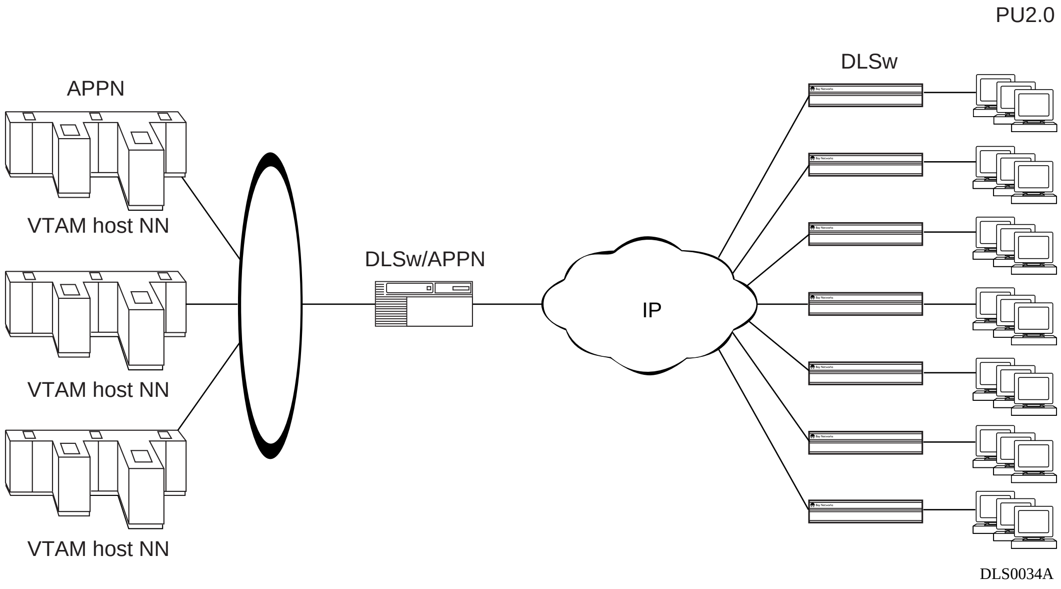


Figure 1-12. Data Center APPN Network

In Figure 1-13, the boundary function resides in a regional location. This enterprise-wide network has an APPN backbone. The regional location connects to the backbone through an IP network.

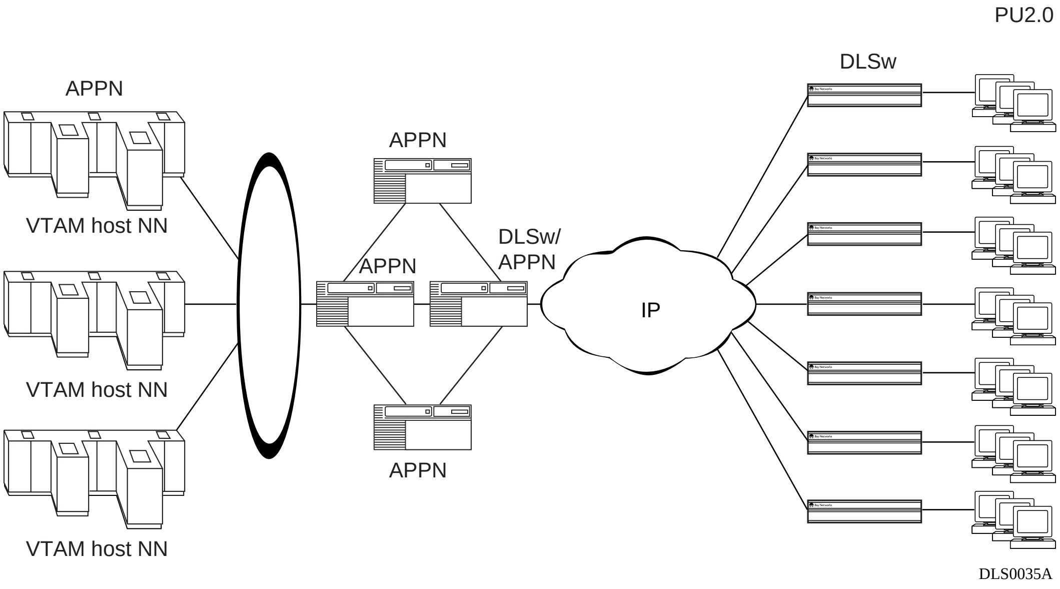


Figure 1-13. Enterprise APPN Network

DLSw/APPN Components

APPN and DLSw pass messages back and forth by means of a virtual circuit (VCCT) at the data link level. Figure 1-14 shows the relationship between APPN, DLSw, and the VCCT through which they exchange messages.

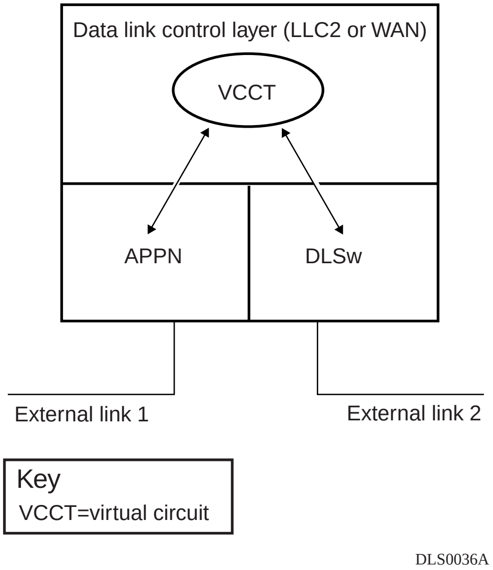


Figure 1-14. Boundary Function Virtual Circuit

APPN and DLSw send and receive messages on external links 1 and 2 and pass messages to each other through the virtual circuit.

The DLSw/APPN boundary function allows DLSw to provide remote communications via an IP backbone and provide access over this backbone from enterprise-level applications using an APPN network.

In Figure 1-15, router 1 is running the DLSw/APPN boundary function. Router 2 is running DLSw only. The path between the host on router 1 and the PU2.0 device on router 2 passes through all the components involved in a communication between the host and the device. (DLUR, a component within APPN, is required because the 3174 system is configured as PU2.0.)

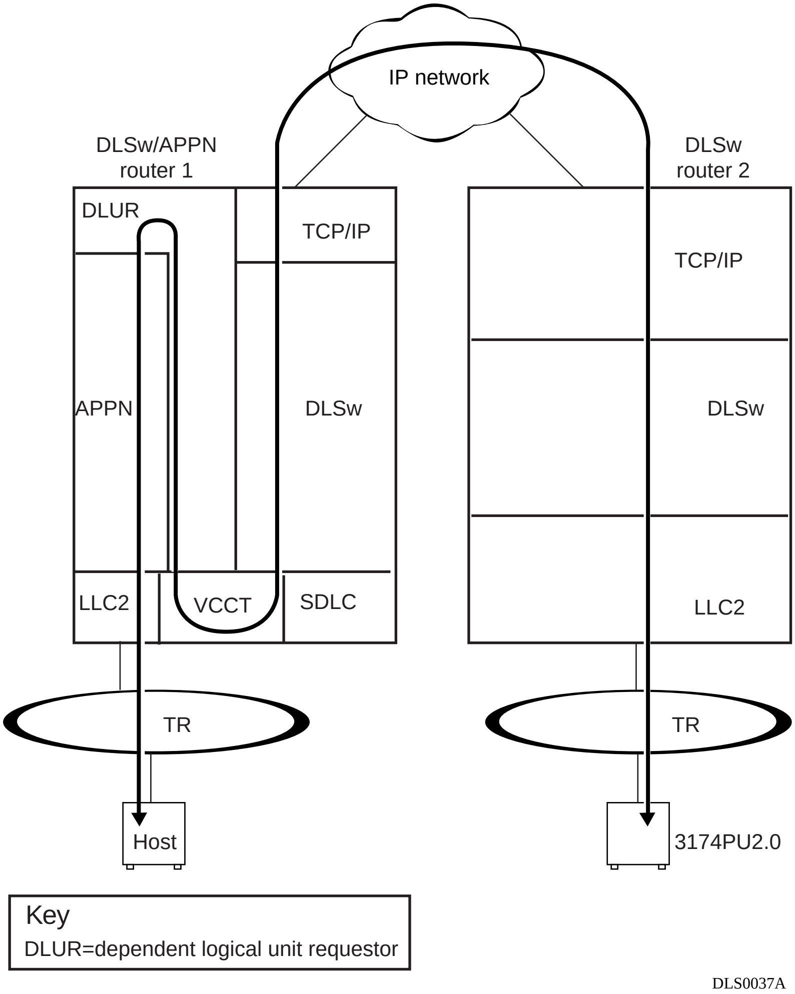


Figure 1-15. End-to-End Connection Using a DLSw/APPN Router and a DLSw Router

DLSw Backup Peer Support

If a TCP connection to the primary peer cannot be established, DLSw can establish a TCP connection to a backup peer, if one is configured. When DLSw starts up, if a TCP connection to the primary peer cannot be established, DLSw checks whether a backup peer IP address is configured, and then initiates a new TCP connection to the backup peer. The TCP connection to the backup peer remains established as long as it is needed or until the maximum up time period has expired, in which case the TCP connection is brought down. DLSw will bring down a backup peer connection if there are no established DLSw connections or if the DLSw connections are idle (i.e., no data has passed).

If a TCP connection with the primary peer is established, but then the primary peer goes down, DLSw attempts to start another SNA session by sending a message to the primary peer. If the TCP connection with the primary peer does not re-establish, the DLSw checks whether a backup peer is configured, and then initiates a new TCP connection to the backup peer.

You can configure backup peers for the following DLSw versions: RFC 1434, RFC 1795, DLSw Version 2.0 (Unicast), or RFC 2166 (Multicast). You select a version using the DLSw RFC Version parameter from the DLSw Basic Global Parameters window. For instructions on using this parameter, refer to Chapter 4.

For instructions on configuring a backup peer for RFC 2166 (Multicast), refer to Chapter 4. For instructions on configuring a backup peer for the other DLSw versions, see Chapter 5.

DLSw Filtering

Bay Networks provides two prioritization mechanisms that affect DLSw traffic:

- DLSw prioritization
- Protocol prioritization

DLSw Prioritization

DLSw prioritization allows you to prioritize traffic within DLSw based on predefined or user-defined fields. Examples of DLSw prioritization criteria include

- Source and destination SAP. Use this field to assign NetBIOS traffic (SAP 0xF0) to a lower priority than SNA traffic.
- Source and destination MAC address. Use this field to provide host-bound traffic preference over other traffic.
- Any field in the SNA Transmission Header (TH) and Response/Request Header (RH). Use this field to provide Class Of Service (COS) priority preference.

You can also prioritize traffic based on any values within the headers and data packets.

For detailed information about DLSw prioritization, refer to Chapter 6, “Using DLSw Prioritization.”

Protocol Prioritization

You can use protocol prioritization to transmit DLSw traffic before other traffic on an individual synchronous line interface. You can prioritize specific types of DLSw traffic, such as:

- Ethernet
- Frame Relay
- SDLC
- Token Ring
- Other SRB traffic

➡ **Note:** You can apply both circuit-level and TCP-level prioritization to DLSw traffic. Note that TCP-level prioritization alone does not give DLSw traffic precedence over other routing protocols. For information about circuit-level prioritization, refer to *Configuring Traffic Filters and Protocol Prioritization*.

For More Information About DLSw

The following publications provide more detailed technical information about DLSw services:

- Dixon, Roy C., and Kushi, David M. *Data Link Switching: Switch-to-Switch Protocol, RFC 1434*, March 1993.

- IBM Corporation. *NetBIOS Frames Protocol, IBM Local Area Technical Reference, SC30-3383-03*, December 1990.
- International Standards Organization. *ISO 8802-2/IEEE Std 802.2 International Standard, Information Processing Systems, Local Area Networks, Part 2: Logical Link Control*, December 31, 1989.
- International Standards Organization. *ISO/IEC DIS 10038 DAM 2, MAC Bridging, Source Routing Supplement*, December 1991.
- Wellfleet Communications. *Integrating SNA & Multiprotocol LAN Networks, A Complete Guide*, March 1993.
- Wells, L., and Bartky, A. *Data Link Switching: Switch-to-Switch Protocol, RFC 1795*, April 1995.
- Bryant, D., and Brittain, P. *DLSw v2.0 Enhancements, RFC 2166*, June 1997.
- Synchronous Data Link Control Concepts, GA27-3093-04, IBM Corp. 1979, 1992.
- Bay Networks. *Configuring SDLC Services*, September 1997.

Chapter 2
DLSw Implementation Notes

This chapter provides important information about the Bay Networks DLSw implementation. You should review this chapter if you are configuring DLSw on a network for the first time. It covers the following topics:

- DLSw and Other Subsystems
- Combining DLSw and SRB
- DLSw and Bridging Services
- Parallel Bridge and DLSw Paths
- Multiple DLSw Peers on a LAN
- Memory Requirements
- TCP Considerations
- Flow Control
- DLSw Prioritization
- Protocol Prioritization
- Backup Peers

DLSw and Other Subsystems

A DLSw network configuration uses the services of other network subsystems. When you select DLSw on an interface, the router software automatically selects these required subsystems. In some configurations, the software requires that you edit the parameters associated with these subsystems. Some parameters have default values that you can either accept or edit. To simplify the editing of additional parameters from multiple subsystems, the software combines these parameters with the DLSw configuration screens.

Selecting DLSw may enable the following subsystems:

- A data link control subsystem, such as LLC2 (for LAN media and Frame Relay), SDLC, QLLC, or APPN Boundary Function
- SRB or bridge subsystems
- TCP and IP subsystems (dual-switch only), where DLSw uses TCP/IP to ensure reliable data delivery

Additionally, when you enable DLSw for the first time on a Bay Networks router, the software automatically displays a set of DLSw screens. These screens display parameters that DLSw requires before it can successfully communicate on the network. These parameters include:

- DLSw global
- DLSw interface
- Slot table

Combining DLSw and SRB

A router running DLSw can communicate with a router running in an SRB configuration. Multiple SRB networks can be interconnected locally or across a TCP/IP backbone using DLSw (Figure 2-1).

DLSw with SRB allows up to 13 total hops. This means that seven hops are allowed on each side of the DLSw network, with one hop reserved exclusively for DLSw. All other rules for configuring SRB networks using Bay Networks routers apply. For detailed information on SRB, refer to *Configuring Bridging Services*.

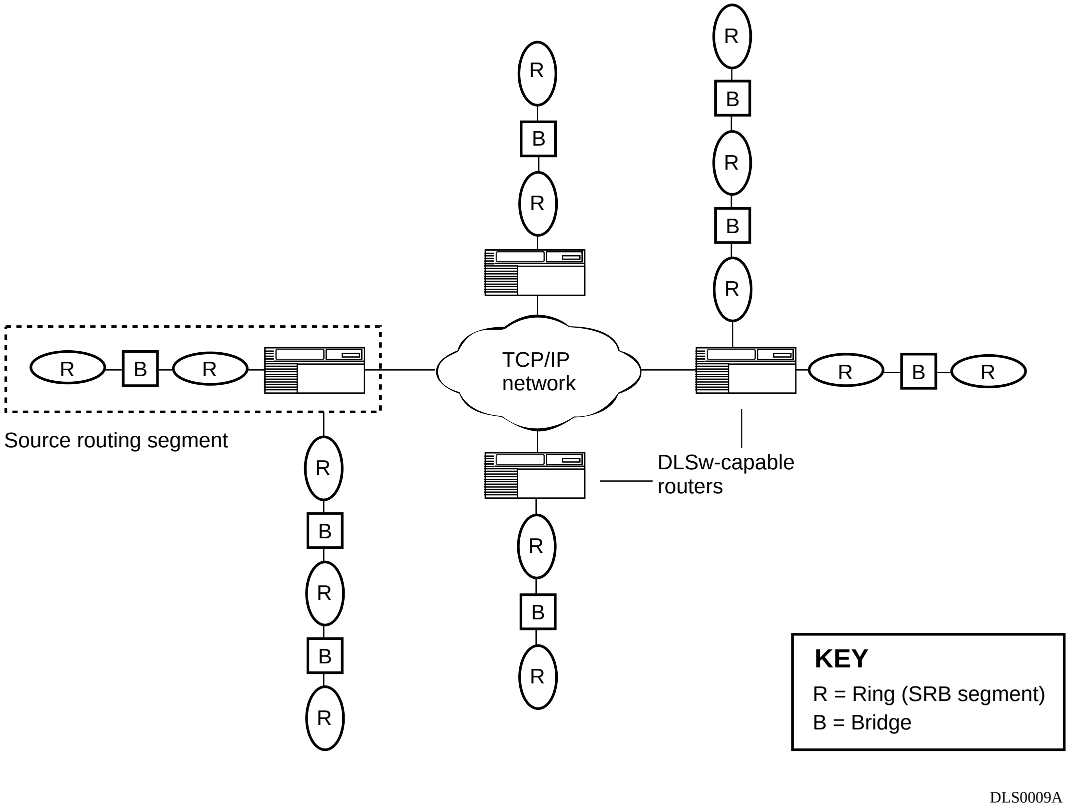


Figure 2-1. DLSw-Capable Routers on an IP Backbone

For Frame Relay networks to use SRB, you must configure the DLSw router for BAN to use source route encapsulation. Figure 2-2 illustrates a sample DLSw and SRB network.

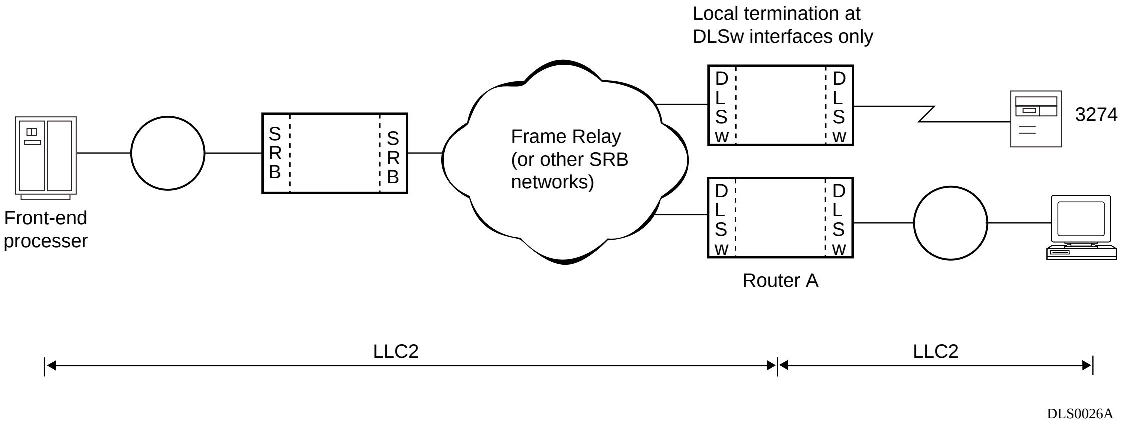


Figure 2-2. Sample DLSw and SRB Network

For mixed topologies, an end-to-end connection path includes an SRB and a non-SRB LAN. In such cases, do not exceed the maximum number of SRB LAN and bridge elements allowed on the SRB LAN side of the connection path. For detailed information on SRB, refer to *Configuring Bridging Services*.

Virtual Rings

Just as each physical Token Ring in a source routing network has an associated ring ID, the DLSw network has a *virtual ring ID*. You enter this ring ID with the IP Virtual Ring parameter.

The virtual ring also has an associated MTU size. The Virtual Ring MTU parameter specifies a maximum size for frames sent from local systems to systems on remote source routing networks. Use as a value for the MTU the *smallest* frame size supported on any remote source routing segment in your network.

You can access and edit the IP Virtual Ring and Virtual Ring MTU parameters through the DLSw Global Parameters window.

➡ **Note:** Site Manager requires you to enter a value for the IP Virtual Ring parameter, even if your network includes only Ethernet/802.3 circuits configured for access to DLSw services.

Count the IP virtual ring as one ring in each source routing segment attached to your TCP/IP network. You count the IP virtual ring first rather than last, to avoid configuring source routing segments that already contain more than eight ring elements.

DLSw and SRB on a Circuit

On an SRB circuit with DLSw services enabled (Figure 2-3), the following rules apply:

- Upon receiving an explorer frame that contains a DLSw-specific destination SAP address, DLSw and SRB attempt concurrently to locate the requested program entity.
  - DLSw searches the network for a route to the target system by forwarding the packet to all local DLSw interfaces and all known remote DLSw routers.
  - SRB looks for a bridged path to the target system using standard source route bridge broadcasts.
- DLSw or SRB, whichever receives a response first, takes precedence. The slower subsystem ceases any further attempts to support a connection to the target program.

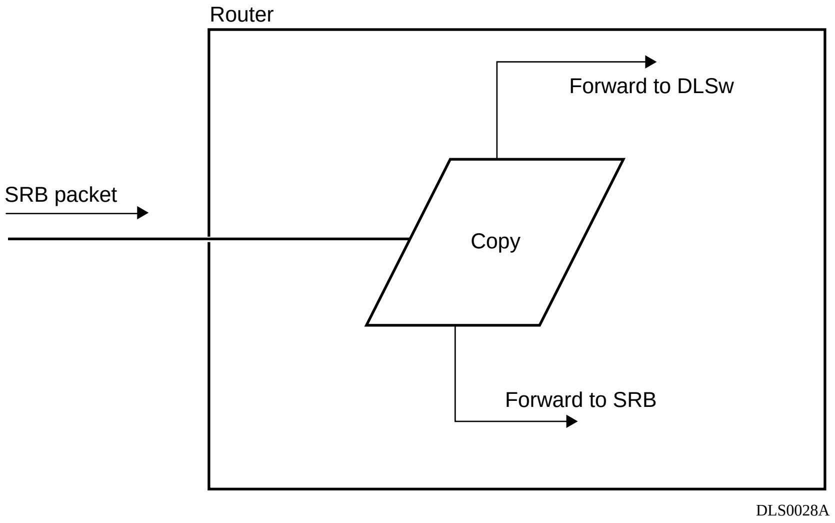


Figure 2-3. DLSw and Source Route Bridging on SRB Circuits

DLSw and Bridging Services

This section presents the different types of bridging services that coexist on a circuit with DLSw, and explains any differences in TEST or explorer frame handling on these circuits. This information is useful when you examine traffic on LANs locally attached to the router.

DLSw on an Ethernet/802.3 Circuit

The router supports DLSw configured on an Ethernet/802.3 circuit. The DLSw software provides bridging services between Ethernet/802.3 LAN segments locally attached to the same router.

The DLSw interface takes precedence over the transparent bridge interface whenever the destination SAP address identified in a TEST frame received from the local circuit already exists in the router's DLSw configuration. In this case, only the DLSw interface:

- Captures the locally received TEST frame
- Attempts to locate the destination SAP address specified in that frame

The transparent bridge interface on the same circuit with DLSw never sees TEST frames that contain destination SAP addresses intended for DLSw (Figure 2-4). However, SAP addresses intended for DLSw can pass from one local Ethernet interface to another over DLSw. Therefore, non-DLSw SAPs will be transparently bridged between transparent bridge interfaces, while DLSw forwards SAPs between interfaces.

You configure transparent bridge services independently of DLSw services on the router, as appropriate for the topology of your network.

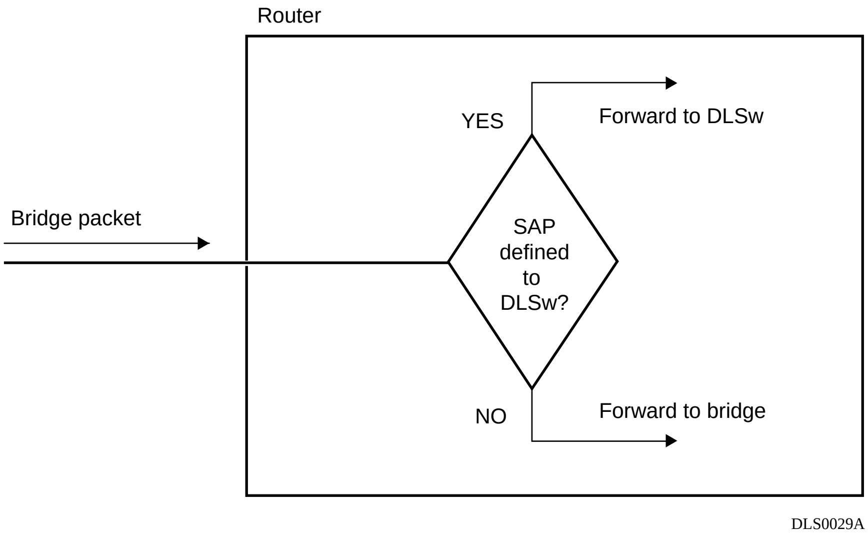


Figure 2-4. DLSw and Transparent Bridging on Ethernet/802.3 Circuits

DLSw with Translation Bridge

The router supports DLSw and translation bridge services on an Ethernet/802.3 circuit (Figure 2-5). You configure translation bridge services independently of DLSw services on the router, as appropriate for the topology of your network.

To an end-user system on an SRB circuit, the translation bridge looks like a source routing bridge. To an end-user system on an Ethernet/802.3 circuit, the translating bridge looks like a transparent bridge.

.

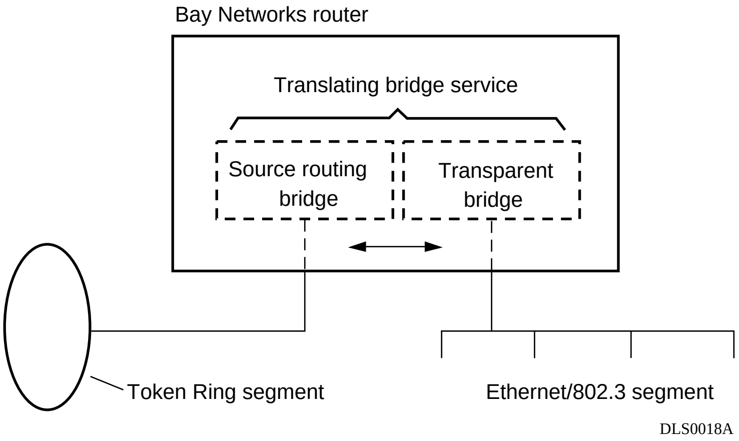


Figure 2-5. Translation Bridge Services

The translation bridge service:

- Supports communication between systems on SRB and Ethernet/802.3 segments locally attached to the same router
- Maps between SRB and Ethernet/802.3 framing requirements

Using DLSw Independently of the Translation Bridge

You can use DLSw independently of the translation bridge to allow an Ethernet-attached device to communicate with a device attached to an SRB network such as Token Ring. DLSw provides local termination, while the translation bridge provides the end-to-end connection. The translation bridge supports the bridge media, while DLSw supports the Ethernet networks.

In (Figure 2-6), Router A uses DLSw to convert traffic between the locally attached Ethernet and Token Ring interfaces. Additionally, the Token Ring and Ethernet-attached devices can communicate with Ethernet devices attached to Router C using DLSw.

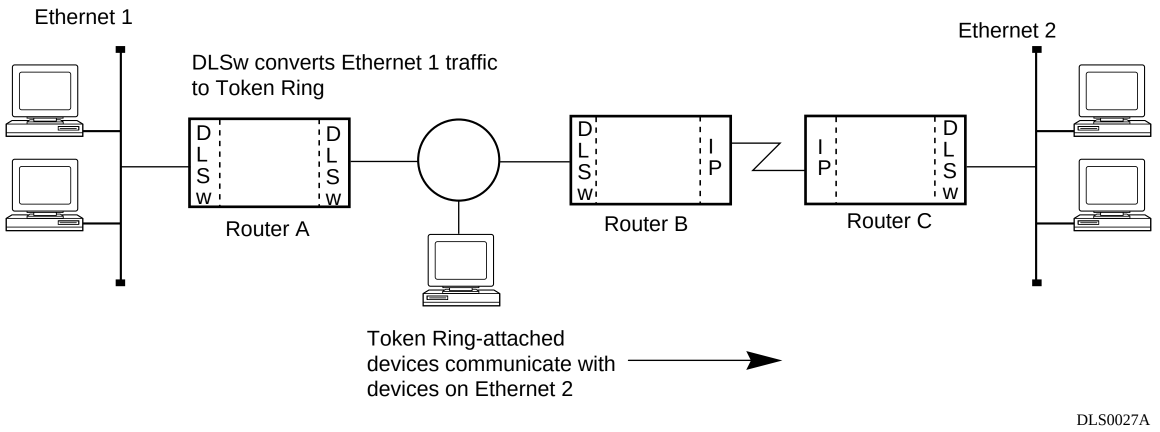

Ethernet 1
DLSw converts Ethernet 1 traffic to Token Ring
DLSw
DLSw
Router A
DLSw
IP
Router B
IP
DLSw
Router C
Ethernet 2
Token Ring-attached devices communicate with devices on Ethernet 2
DLS0027A

Figure 2-6. Independent DLSw/Translation Bridge Network

Parallel Bridge and DLSw Paths

If a valid bridging path already exists between two LANs, *do not* configure a parallel DLSw connection path between the same two LANs (Figure 2-7). Parallel data paths allow frames to traverse the LANs twice which, in turn, may confuse systems on the associated LAN segments.

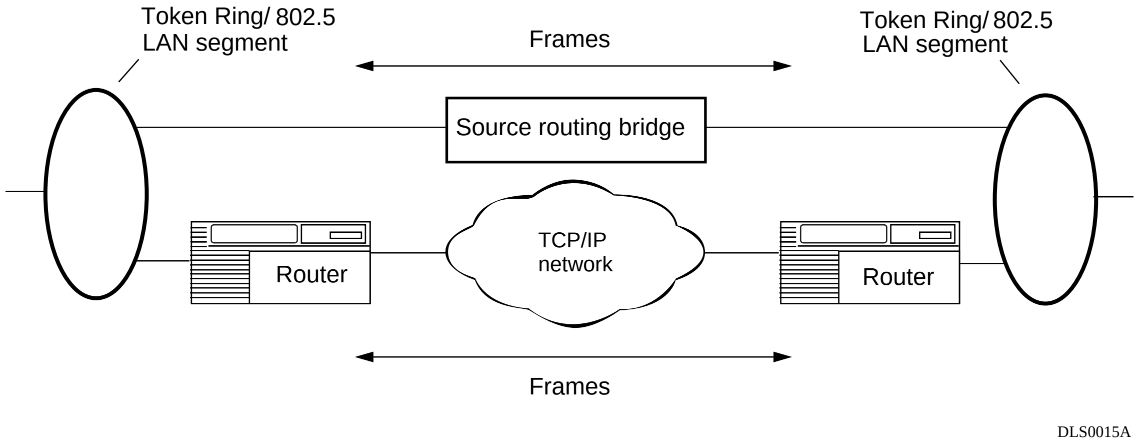


Figure 2-7. DLSw Services in Parallel with a Source Routing Bridge

Multiple DLSw Peers on a LAN

You can configure two or more DLSw nodes on the same SRB LAN. With this configuration, each DLSw peer reaches a different set of remote NetBIOS and SNA systems. In this case:

- Do *not* define a TCP connection between these Data Link Switches.
- Assign the same virtual ring IDs to each peer.

Taking these precautions prevents frames sent by one DLSw node from propagating through the other DLSw node on the same SRB LAN.

➡ **Note:** Do not configure multiple data link switches on an Ethernet/802.3 LAN. DLSw over Ethernet/802.3 LANs does not provide loop prevention.

Memory Requirements

DLSw provides buffering of LLC2 packets in single-switch mode, and additional buffering of TCP packets in dual-switch mode. Therefore, DLSw can use a significant amount of memory.

To limit the memory consumption, Bay Networks provides several mechanisms, including:

- LLC2 Max Links parameter, allowing the network administrator to limit the number of LLC2 stations *per interface*. Refer to *Configuring LLC Services*.
- DLSw Max Slot Sessions parameter, allowing the network administrator to limit the number of LLC2 stations *per slot*. See Chapter 5 for instructions on accessing and editing the Max Slot Sessions (DLSw global) parameter.

For more information about DLSw memory usage, contact the Bay Networks Technical Support Center.

TCP Considerations

TCP timers allow you to configure DLSw to periodically give TCP data to transmit if a connection is inactive for a period of time. The mechanism by which TCP determines a lost connection (either a failed link with no rerouting possible, or the remote router is unavailable) is based on TCP attempts to deliver this data. If TCP does not receive an acknowledgment after a series of retries, it declares the connection down and informs DLSw. DLSw then manages the currently active sessions.

There are four main configuration parameters associated with TCP timers:

- KeepAlive Time
- KeepAlive Retry Timer
- KeepAlive Retries
- TCP Inact Time

For information about the parameters, refer to Chapter 3.

Flow Control

DLSw uses the following three flow control mechanisms to provide reliable end-to-end delivery of packets:

- LLC2 flow control
- TCP flow control
- DLSw RFC 1434 fixed and RFC 1795 adaptive pacing

TCP and LLC2 continue to assert flow control until congestion clears on a given TCP connection.

The default settings for system parameters relevant to LLC2 and TCP flow control are suitable for the majority of your DLSw service requirements.

LLC2 Flow Control

The LLC2 protocol interface provides a bidirectional window and a SAP credit allocation, that together manage flow control on individual LLC2 connections between the router and LAN-attached SNA or NetBIOS systems.

The SAP window attempts to limit the number of outstanding frames queued for transmission to a remote endstation from a local endstation at this SAP address, as follows:

1. As the local endstation sends frames that the remote endstation has yet to acknowledge, a counter on the remote DLSw switch increments.
2. When this counter reaches half the value specified in the SAP Window parameter, the remote DLSw switch sends a flow control indication back to the local DLSw switch. This step is actually part of DLSw RFC 1434 fixed flow control.
3. The local DLSw switch sends RNRs (receiver not ready) to the local endstation to control the flow of the session.
4. As the remote endstation acknowledges frames, the counter on the remote DLSw switch decrements.
5. After the remote endstation acknowledges all outstanding frames, the remote DLSw switch sends an end-flow-control indication back to the local DLSw switch.
6. The local DLSw switch then sends RR (receiver ready) to the local endstation, thereby allowing it to send more frames.

TCP Flow Control

Each pair of TCP connections between DLSw peers carries data from many LLC2 sessions. When congestion occurs on the TCP/IP network between DLSw peers, TCP:

- Reduces or closes its transmit window
- Signals the local and remote LLC2 interfaces to assert flow control on any LLC2 connections associated with the congested TCP connections

DLSw Flow Control

A counter on the remote DLSw switch increments as the local endstation sends frames that the remote endstation has yet to acknowledge. When the counter reaches half the value specified in the SAP Window parameter, the remote DLSw switch sends a flow control indication back to the local DLSw switch. For RFC 1434, the flow control indication is an Enter Busy SSP message.

DLSw Packaging

In DLSw dual-switch configurations, packaging allows multiple DLSw frames (consisting of user data and the DLSw SSP header) to be placed into a single TCP/IP frame. This provides two performance benefits:

- Reduces the number of TCP/IP encapsulation program executions. This results in fewer router cycles when processing DLSw information.
- Reduces the amount of TCP/IP overhead per DLSw frame. Instead of 52 bytes of overhead per information frame (32 for TCP, 20 for IP), a single TCP/IP package carries multiple frames.

With DLSw packaging, a packet may be delayed for a short period while the router waits to see whether there are any more packets routed to the same destination peer. This delay may increase network latency. However, the performance benefits increase the number of packets that can be delivered across the network, increasing response time. DLSw packaging is important for networks with many LAN/WAN segments and for networks with slow WAN links.

For information on configuring DLSw packaging parameters, refer to Chapter 5.

DLSw Prioritization

Bay Networks routers enable you to prioritize DLSw traffic by configuring priority queues for DLSw peers. You apply DLSw prioritization by using outbound filters. For information on DLSw prioritization, refer to Chapter 6.

Protocol Prioritization

You can use protocol prioritization to transmit DLSw traffic before other traffic on an individual synchronous line interface. To use protocol prioritization, create a filter, as follows:

- Criteria = TCP source port
- Range = 2065 - 2067
- Action = high queue

This ensures that SNA and NetBIOS traffic receives preference on the network. For more information about how to access and configure traffic filters for DLSw services, refer to *Configuring Traffic Filters and Protocol Prioritization*.

Backup Peers

The backup peer feature allows you to use a backup peer if the TCP connection to the primary peer cannot be established. The TCP connection to the backup peer remains established as long as it is needed or until the maximum up time period has expired, in which case the TCP connection is brought down. DLSw will bring down a backup peer connection if there are no established DLSw connections or if the DLSw connections are idle (i.e., no data has passed).

You can configure backup peers for the following DLSw versions: RFC 1434, RFC 1795, DLSw Version 2.0 (Unicast), or RFC 2166 (Multicast). You select a version using the DLSw RFC Version parameter from the DLSw Basic Global Parameters window. For instructions on using this parameter, refer to Chapter 4.

To configure backup peers, you select Yes at the Backup Config parameter on the DLSw Multicast Configuration window or the DLSw Peer Configuration window. This enables the rest of the backup peer parameters.

The Backup Peer Type parameter defines how the session attempts to establish a TCP connection using the backup peer. The valid values are:

- RFC 1795 - Send the request for connection over TCP only
- V20 (Unicast - TCP) - Send the request for connection over TCP only.
- V20 (Unicast - Unknown) - Send the request for connection over UDP; the backup peer can fall back to RFC 1795 mode.
- V20 (Unicast - UDP) - Send the request for connection over UDP, one TCP connection is expected; the backup peer cannot fall back to RFC 1795 mode.
- RFC 2166 (Multicast) - Send the request for connection to the multicast address configured in the Backup IP Address field.

The Backup Peer Type cannot exceed the global DLS RFC type on the router. For example, if the DLSw global RFC type for the router is RFC 2166 (Multicast), the backup peer can be any of the available values. If the RFC type is V2.0 Unicast, the backup peer cannot be multicast. If the RFC type is RFC 1795, the backup peer cannot be multicast, V2.0 UDP, V2.0 Unknown, or V2.0 TCP.

For more instructions on configuring a backup peer for RFC 2166 (Multicast), refer to Chapter 4. For instructions on configuring a backup peer for the other DLSw versions, see Chapter 5.

Chapter 3
DLSw Configuration Overview

This chapter provides general information about configuring DLSw on Bay Networks routers, including:

- Adding Single-Switch DLSw Services
- Adding Dual-Switch DLSw Services
- Configuring SDLC Lines and Devices
- Configuring DLSw over Frame Relay
- Configuring Predefined MACs and Names
- Configuring DLSw Packaging
- Configuring DLSw Prioritization
- Configuring DLSw Backup Peers
- Configuring DLSw for IP Multicast

When you configure DLSw for single- and dual-switch services, you must set the DLSw basic global and basic interface parameters for your network. The parameters that you edit will depend on the type of interface you are configuring.

To tune DLSw single- and dual-switch services, use the DLSw advanced global and advanced interface parameters.

Adding Single-Switch DLSw Services

When configuring a DLSw single-switch network, DLSw is enabled on each relevant interface. Using single-switch mode allows communication between:

- Devices attached to different local interfaces on the same router. For example, an SDLC-attached 3274 control unit can communicate with a local LAN-attached SNA server (Figure 3-1).
- A local device and an SNA device directly attached to a Frame Relay network. An SNA device connected to Router B (Figure 3-1) can communicate with the AS/400 using either BNN or BAN protocols.
- SNA and NetBIOS devices attached to different routers, each running DLSw. For example, a NetBIOS client attached to Router A can communicate with the NetBIOS server connected to Router B (Figure 3-1). The connection can cross multiple routers running DLSw. Since DLSw is running on the WAN interface, the router operates as single-switch DLSw.

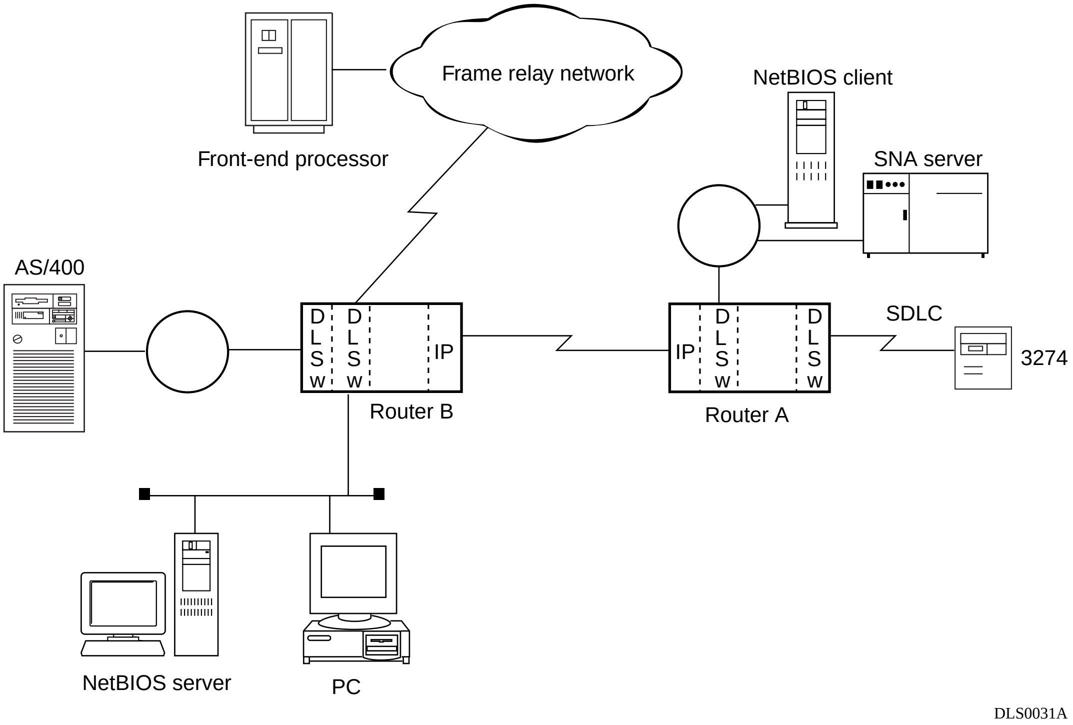


Figure 3-1. DLSw Single-Switch Network Example

Single-Switch Configuration Requirements

To configure single-switch DLSw services on the router, you define:

- DLSw basic global parameters
- DLSw advanced global parameters (optional)
- DLSw SAP Table entries (optional)

DLSw Basic Global Parameters

In single-switch configurations, DLSw requires that you specify a value for the DLSw Virtual Ring ID parameter. Optionally, you can change all other parameters that appear in the DLSw Basic Global Parameters window.

DLSw Virtual Ring ID

The IP Virtual Ring parameter specifies a standard ring number (0x001 through 0xFFE) that SRB uses to identify traffic that DLSw places on the SRB LAN. This ring number is the first entry in the packet’s routing information field (RIF). The ring number must be unique within the network. Generally, Bay Networks routers should use the same value. For this parameter, Bay Networks recommends the value 0xFFD, if it is available.

DLSw RFC Version

The DLSw RFC Version parameter lets you specify the RFC implementation you want to run on the router: RFC 1434, RFC 1795, DLSw Version 2.0 (Unicast), or RFC 2166 (Multicast).

NetBIOS Support

The NetBIOS parameter lets you specify whether this router supports NetBIOS traffic and adds the NetBIOS SAP entry 0xF0 to the SAP Table. Select Yes if you want to use NetBIOS.

DLSw Advanced Global Parameters

All parameters that appear in the DLSw Advanced Global Parameters window are optional. However, you can edit the Virtual Ring MTU and the Max Slot Sessions parameters to tune a DLSw single-switch network.

Virtual Ring MTU

The Virtual Ring MTU parameter allows you to limit the size of packets traversing the network. Based on the value that you specify, the router enters the appropriate maximum MTU into any SRB explorer packet that uses DLSw services.

Max Slot Sessions

DLSw provides buffering of LLC2 packets in single-switch mode. Therefore, DLSw can use a significant amount of memory. To limit the memory consumption, edit the DLSw Max Slot Sessions parameter to limit the number of LLC2 stations *per slot*.

DLSw SAP Table

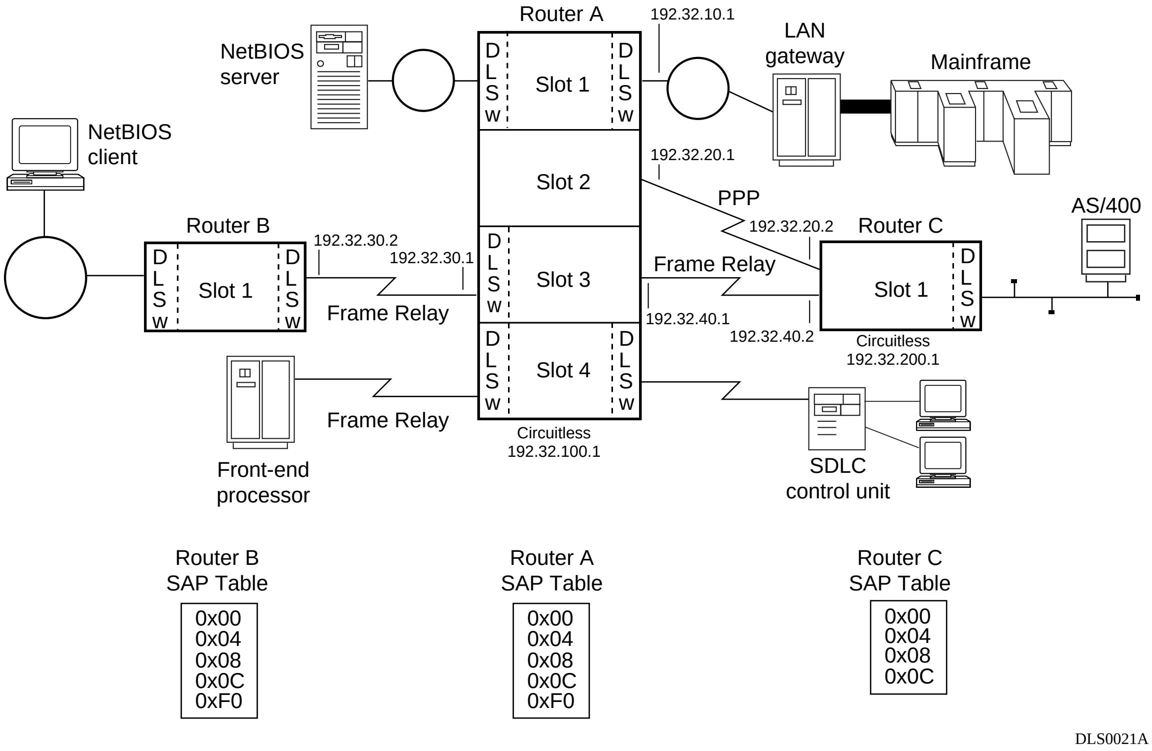
Every data packet contains a 1-byte destination SAP and source SAP. You can select whether DLSw affects packets based on SAPs that are defined to DLSw. Each router maintains an independent list of DLSw SAP addresses in a global DLSw SAP Table. Use the Configuration Manager to access and edit the DLSw SAP Table.

Each DLSw SAP Table entry has a unique hexadecimal value. The default SAP Table includes SAPs 00, 04, 08, and 0C (hexadecimal). This is sufficient for most SNA applications. To support NetBIOS, edit the DLSw NetBIOS Support parameter and specify Yes to add SAP F0 to the table.

Figure 3-2 shows a sample network with three routers running DLSw. This network uses the following values in the SAP Tables:

- Router A, the central site router, supports both SNA and NetBIOS traffic. SNA session traffic uses SAP 04, and NetBIOS traffic uses F0. Additionally, SNA requires SAP 00 for session initiation. These hexadecimal values (00, 04, F0) must exist in the SAP Table.
- Router B, the remote site, supports NetBIOS traffic only. SAP F0 is the only required entry in the SAP Table. By default, the SAPs 0x004, 0x008, and 0x00C appear in the table.
- Router C, a regional site, supports SNA traffic only. In this example, SNA requires SAPs 00 and 04 in the SAP Table.

Note that SNA traffic can use other SAPs. Most SNA traffic uses SAP 04.



Router B SAP Table	Router A SAP Table	Router C SAP Table
0x00	0x00	0x00
0x04	0x04	0x04
0x08	0x08	0x08
0x0C	0x0C	0x0C
0xF0	0xF0	

Figure 3-2. Sample Network with SAP Table Definitions

Refer to Chapter 5 for more information about accessing and editing the DLSw SAP Table.

Adding Dual-Switch DLSw Services

When configuring DLSw dual-switch services, DLSw is enabled only on interfaces supporting LAN-, SDLC-, QLLC-, or APPN Boundary- attached devices. The links between routers are configured for IP routing. DLSw is *not* configured on these links.

Figure 3-3 illustrates a DLSw dual-switch network. In this network:

- Dual-switch services are used between routers. Any SNA device attached to Router A can communicate with the AS/400 or FEP connected to Router B.
- Single-switch conversion can be used between DLSw interfaces on Router A, as well as between the DLSw interfaces on Router B. This allows the AS/400 to communicate with the FEP.
- The connection between Router A and Router B can be any medium that supports IP.

Intermediate routers that are located between Router A and Router B must transport IP packets using IP routing. DLSw is not required by the intermediate node.

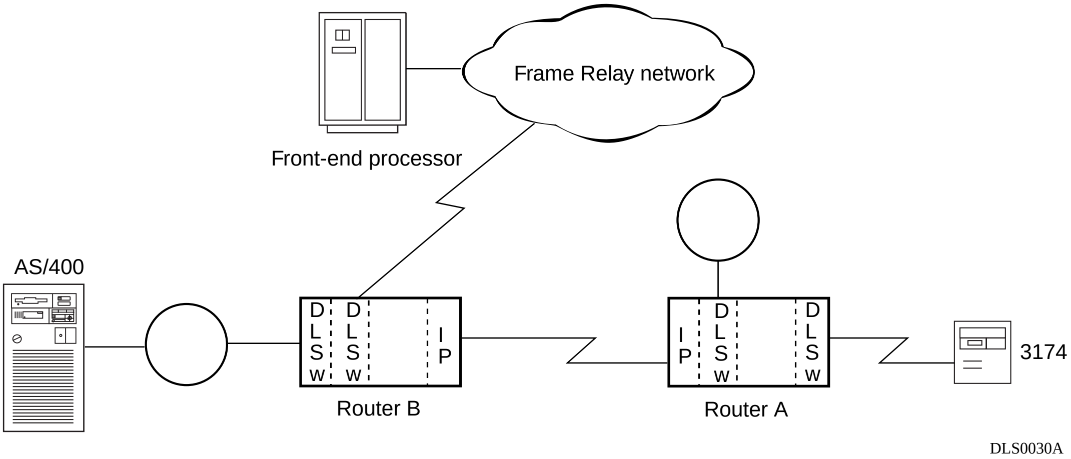


Figure 3-3. DLSw Dual-Switch Network Example

Dual-Switch Configuration Requirements

To configure dual-switch DLSw services on the router, you define:

- DLSw basic global and basic interface parameters
- DLSw advanced global and advanced interface parameters
- DLSw Slot Table entries
- DLSw Peer IP Table entries

DLSw Basic Global and Basic Interface Parameters

In dual-switch configurations, DLSw requires the same global parameters as single-switch DLSw. Dual-switch configurations also require that you use the following parameters:

- DLSw Peer IP Address (optional)
- DLSw Slot IP Address
- DLSw RFC Version

Refer to the “DLSw Peer IP Table” section for information about DLSw peers; refer to the “DLSw Slot Table” section for information about configuring DLSw slots.

You can also use the DLSw RFC Version parameter to select a specific implementation of DLSw to run on the router. DLSw RFCs include:

- RFC 1434
- RFC 1795
- DLSw Version 2
- RFC 2166

Refer to Chapter 5 for information about the DLSw RFC Version parameter.

DLSw Advanced Global Parameters

In dual-switch configurations, you may want to edit those parameters that directly tune network performance, such as:

- TCP Window Size
- KeepAlive Time
- Reject Unconfigured Peers
- Mac Cache Age
- TCP Inact Time

TCP Window Size

The TCP Window Size parameter informs DLSw about how much data can be outstanding on a TCP connection. The size of the window affects performance, latency, flow control, and memory usage. A larger window causes less flow control to occur with a possible increase in latency. Editing the TCP Window Size parameter affects new TCP session establishment only. Existing sessions are unaffected.

Generally, networks with slower line speeds require smaller window sizes, while networks with faster line speeds benefit from larger windows. The default value is acceptable for most networks. A TCP Window Size setting of 5000 octets may be appropriate for low-speed lines (or networks running over low speed lines). For high-speed lines, you may want to increase this value, or use the default value of 8000.

KeepAlive Time

The TCP KeepAlive Time parameter specifies how often the router sends a signal to the peer router to check that the peer router is working correctly and can receive messages. You enable the parameter by specifying a nonzero value.

When a keepalive packet goes unacknowledged by the remote peer, retransmission begins at the local peer router. You should tune the keepalive interval based on the total time it takes to send and receive acknowledgment from the remote peer.

Since keepalive packets are sent only on idle lines, increasing the keepalive interval may decrease the cost of an idle network. In busy networks, the keepalive interval is not necessary. Frequent traffic for TCP transmission performs the same function as a keepalive setting.

In busy networks, the DLSw keepalive is not necessary. Frequent traffic for TCP transmission performs the same function as a keepalive setting. For example, frequent NetBIOS broadcast traffic functions as a TCP keepalive.

Reject Unconfigured Peers

The Reject Unconfigured Peers parameter allows you to limit the addition of new DLSw sessions. If you set the parameter to Reject, the router establishes sessions only with those routers that are defined in the DLSw Peer IP Table. If you set the parameter to Accept, the router allows new DLSw sessions with any router that requests a session.

Generally, routers connected to devices that initiate SNA/NetBIOS sessions (usually routers located at remote sites in a hub configuration) must have a configured Peer IP Table, allowing a parameter setting of Reject. Routers that learn about remote locations and devices dynamically (such as central site routers) do not have a configured Peer IP Table. These routers should have a Reject Unconfigured Peers parameter setting of Accept.

MAC Cache Age

The MAC Cache Age parameter allows you to specify the maximum number of seconds that inactive MAC addresses can exist in the MAC-to-DLSw Peer mapping cache. You enter an interval to limit the amount of memory that inactive MAC cache entries consume for DLSw services on the router. While the address is inactive, no CANUREACH messages are transmitted for the MAC address. Once the age timer expires, CANUREACH messages can be transmitted again.

TCP Inact Time

Specifies the period of inactivity to elapse before terminating a TCP connection. Inactivity may result after a prior session has terminated, or if no data has been transferred. The TCP Inact Time parameter functions with DLSw Version 2 and RFC 2166 and with configured DLSw backup peers. This parameter operates with the TCP Inact Method parameter.

DLSw Slot Table

Each slot on a Bay Networks router running DLSw acts as an independent data link switch. You identify each slot by assigning a *unique* IP address for the slot. This mapping is done in the DLSw Slot Table. Each entry in the table consists of a DLSw slot number plus the address of the IP interface that you allocate for that slot.

The router uses this IP address to establish the TCP sessions between peers in a DLSw network. Generally, the IP address that you select is either the circuitless IP address or the IP address of any interface on this slot. However, it is acceptable to use the IP address of any interface on any slot.

For configurations that do not have as many physical IP interfaces as DLSw slots, add IP addresses to one or more IP-capable interfaces. If required, a single interface can support multiple IP addresses. For example, you might want to do this in large SDLC configurations, because IP cannot be configured on SDLC interfaces. For more information on configuring multiple IP addresses, see *Configuring IP Services*.

Note: You can use the circuitless IP interface address for one (and only one) DLSw-capable slot. Using the circuitless IP interface allows TCP connections for DLSw services on that slot to be less dependent on the availability of specific physical circuits or data links. Bay Networks recommends that you set the Keepalive Time parameter to a nonzero value when using the circuitless IP address. For more information about the circuitless IP interface, refer to *Configuring IP Services*.

Note: If you configure RFC 2166, you must specify the IP multicast address for the DLSw Slot Table.

Figure 3-4 shows a sample network with three routers running DLSw. Although many options exist for the Slot Table, this network uses the following values:

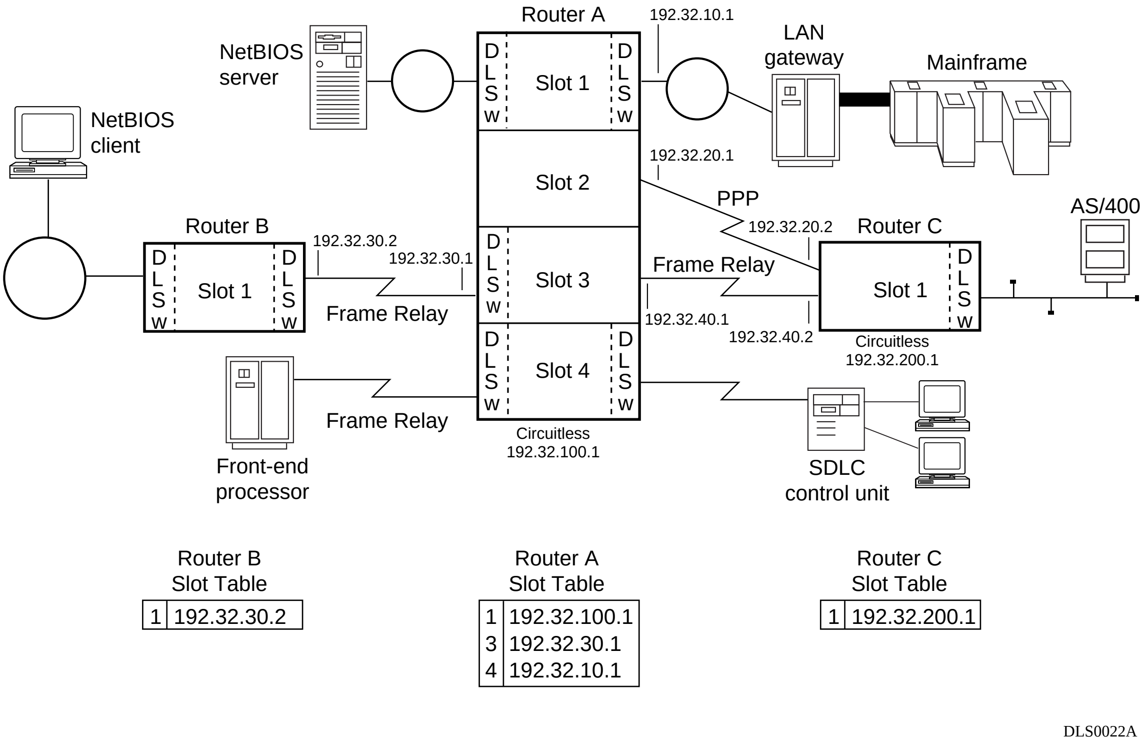
- Router A, the central site router, has three slots running DLSw, as follows:

-- Slot 1: Represented by the circuitless IP address. This provides the highest availability for Token Ring devices.

-- Slot 3: Represented by the IP address of the directly attached Frame Relay interface.

-- Slot 4: Represented by an IP address of a Token Ring interface on Slot 1. It is acceptable to use any other IP address existing on this router to represent this slot.

- Router B, a remote site connected to the central site using Frame Relay, is a single-slot router running single-switch DLSw. The IP address of the Frame Relay interface represents this slot in the Slot Table.
- Router C, a regional site connected to the central site using multiple links, is a single-slot router running dual-switch DLSw. The circuitless IP address represents this slot in the Slot Table.



Router B Slot Table

1	192.32.30.2

Router A Slot Table

1	192.32.100.1
3	192.32.30.1
4	192.32.10.1

Router C Slot Table

1	192.32.200.1

Figure 3-4. Sample Network with Slot Table Definitions

You enter slot information in the DLSw Slot IP Table during the initial configuration procedure. Refer to Chapter 5 for more information about accessing and editing the DLSw Slot IP Table.

DLSw Peer IP Table

TCP/IP sessions exchange information between devices attached to each router. Data link switches that connect to the same TCP/IP network are called *DLSw peers*. Each DLSw peer is represented by an IP address.

On Bay Networks routers, each slot that you configure with DLSw services functions as an independent DLSw peer. Other vendors may offer RFC 1434/1795-compliant products that support either single or multiple DLSw peers internally. For example, each IBM 6611 processor in your network serves as a single DLSw peer that you must define on the router.

In each router, you can define a list of peers identifying remote routers with which a DLSw session can be initiated. These are called *configured peers*, and are defined in the DLSw Peer IP Table.

Configured Peers

A configured peer is a remote data link switch, represented by an IP address, that is predefined in the local router. You define a configured peer by specifying its unique IP address in the Site Manager DLSw Peer IP Table.

IP addresses in the local router’s Peer IP Table must also appear in the Slot Table of a remote router.

A configured peer can receive broadcast frames directly from DLSw peers in a local router.

The local router issues broadcast frames triggered by client demand for connection services. Responses to these broadcasts enable the local router to:

- Identify DLSw peers that can reach the requested remote NetBIOS or SNA system
- Manage (open, restart, and close) TCP connections to the DLSw peer that can reach the requested SNA or NetBIOS system

Once a router knows that a DLSw peer can reach a specific system, the router can address frames directly to that peer and avoid unnecessary broadcast traffic on the TCP/IP network.

You typically define as configured peers:

- One slot in each DLSw-capable remote Bay Networks router in your TCP/IP network to which broadcast traffic must be forwarded
- Any other peer in your TCP/IP network that complies with RFC 1434, RFC 1795, or DLSw Version 2

You define each configured peer by specifying its unique IP address on the TCP/IP network.

With RFCs 1434 and 1795, once you initialize DLSw services, the local router establishes two TCP connections (one for transmitting, one for receiving) between each local DLSw-capable slot and every configured peer in the TCP/IP network. Remote DLSw peers on the network follow the same procedure. DLSw uses TCP ports 2065 and 2067.

Peer Types

For V2.0, you can define a specific transport type to a DLSw peer, specifically:

- TCP
- UDP
- Unknown

Peers that you define as TCP or UDP will cause the local router to use TCP or UDP explorer frames respectively and exclusively to establish connections with the peer router. A peer that you define as Unknown causes the local router to use UDP explorer frames to locate the destination MAC address of the peer before establishing the TCP connection. If the TCP connection cannot be made, or if there is no UDP response, DLSw performs fallback attempts to earlier RFC protocols to establish the connection. If all connection attempts fail regardless of the RFC used, a connection can be made to a configured DLSw backup peer, described in the next section.

For information about configuring peer types and fallback attempts, refer to the Transport Type and SNA Fallback Attempts parameters in Chapter 5.

Backup Peers

A backup peer receives all DLSw-related broadcast frames for a given router or network processor if the primary peer router is unavailable or cannot be reached over a TCP connection. When you specify the Backup IP Address, DLSw places the entry in the Backup Peer IP Table.

There are seven Backup Peer IP Table parameters that allow you to manage a router that you want to use when the local router cannot connect to a primary DLSw peer:

- Backup IP Address
- Backup Peer Type
- Backup Max Up Time
- Backup Hold Down Time
- Backup Start Time
- Backup End Time
- Backup Delete

For information about configuring backup peers, refer to Chapter 5.

Simplifying the Peer IP Table

Bay Networks provides two mechanisms for reducing the number of required entries in the DLSw Peer IP Table. These are:

- Broadcast peers
- Unconfigured peers

Broadcast Peers

It is not necessary to enter more than one peer per remote router into the Peer IP Table. The entry representing the remote router is the *broadcast peer* for that router. Only broadcast peers normally receive broadcast frames from another router. However, all DLSw peers on a remote Bay Networks router can both receive and respond to broadcast frames that the broadcast peer in that router forwards internally.

Unconfigured Peers

A Bay Networks router running DLSw can respond to requests from remote routers to initiate DLSw sessions, even if the local router's Peer IP Table does not contain the remote peer definition. When DLSw establishes a session to a remote slot, DLSw dynamically adds the slot to the list of known peers. Any remote DLSw peer that the router learns dynamically is an *unconfigured peer.* A router's Peer IP Table does not list the unconfigured peers.

DLSw supports unconfigured peers only if you set the DLSw Reject Unconfigured Peers parameter to Accept.

When a local DLSw peer (Bay Networks or otherwise) receives a broadcast response from a non-broadcast peer on a Bay Networks router, the local peer opens a DLSw connection to the unconfigured peer.

Figure 3-5 shows a sample network of three routers running DLSw. This network uses the following Peer IP Table entries:

- Router A's Peer IP Table has a single entry, as follows:
  - The DLSw single-switch communication with Router B does not require an entry in the Peer IP Table.
  - The connection to Router C uses dual-switch DLSw. You must create an entry in the Peer IP Table so that Router A can forward DLSw broadcasts to Router C. Router A's Peer IP Table contains the circuitless IP address of Router C (192.32.200.1), since this value is the only value in Router C's Slot Table.
- Router B communicates to Router A via a single-switch connection. You do not need a Peer IP Table for Router B.
- Router C communicates with Router A using dual-switch mode. Router C's Peer IP Table contains the circuitless IP address of Router A (192.32.100.1). However, you can use any IP address in Router A's Slot Table instead of the circuitless IP address.

When using dual-switch mode, you do not configure DLSw on the links between the routers. You must configure IP on these interfaces.When communicating using single-switch mode, you must configure DLSw on the connecting interfaces.

Note that either link from Router A to Router C can transport DLSw traffic. Standard IP routing determines the link over which these routers communicate.

Multicast IP Entries (RFC 2166)

When you configure a multicast IP entry, you do not need to configure DLSw peer entries because configuring a multicast IP entry allows for TCP connections to be established.

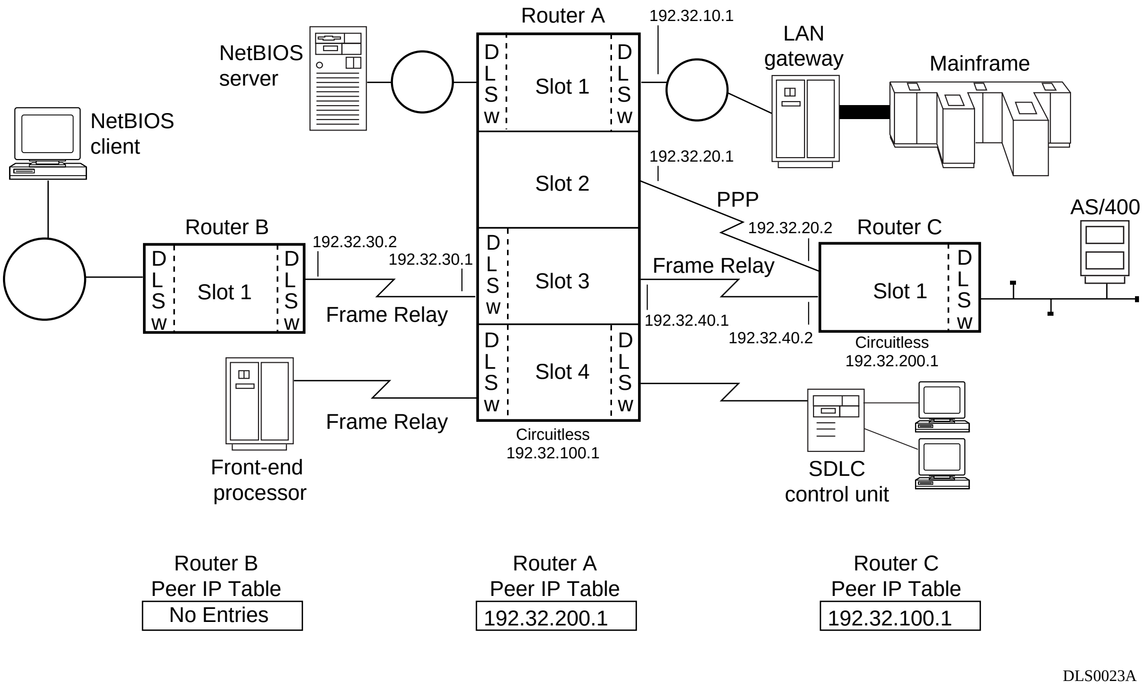


Figure 3-5. Sample Network with Peer IP Table Definitions

Configuring SDLC Lines and Devices

This section describes the objects that you define when you configure DLSw SDLC-attached devices on the router, specifically:

- SDLC line parameters
- DLSw Local Devices

SDLC Line Parameters

DLSw uses the SDLC Line Parameters to determine the characteristics of the link. You must set these parameters to allow the router to communicate with the SNA equipment. The major parameters are:

- Clock Source
- Internal Clock Speed
- Sync Line Coding

For information about configuring SDLC line parameters, refer to Chapter 4.

Local Devices

DLSw uses local device entries to define SDLC-attached SNA physical units (PUs) to the router. NetBIOS does not support SDLC-attached devices.

To take advantage of integrated SDLC services in DLSw, you must define the SDLC devices that you want to appear as natively attached to the LAN. When you define such devices, you map the devices to LAN MAC and SAP addresses.

You can add local devices at the following times:

- When you add SDLC to a synchronous circuit and add the DLSw protocol to that circuit.
- When you edit a synchronous circuit that already has SDLC and DLSw on it.
- When you edit DLSw interface parameters. In this case, the interface whose parameters you edit must already have at least one local device defined on it.

Several local device parameters must match other entries in the router, or in the attached SDLC device. These include:

- Link Address (hex)
- PU Type
- IDBLOCK and IDNUM
- XID Format
- Source (Host) MAC (hex)
- Destination (Host) MAC (hex)
- Source (Virtual) SAP (hex) and Destination (Host) SAP (hex)

For information about these parameters, refer to Chapter 4.

For each local device that you add, Site Manager creates a corresponding SDLC link station, which is how SDLC sees the local device. Site Manager assigns several default parameter values to the link station. For information about how to access and change the link station parameters, see *Configuring SDLC Services*.

Once you add local devices, you can access and change the local device parameters, as described in Chapter 5.

Configuring DLSw over Frame Relay

When configuring DLSw over Frame Relay, IBM provides two types of Frame Relay support:

- Boundary Network Node (BNN) -- RFC 1490 or Routed SNA
- Boundary Access Node (Bridged SNA)

Bay Networks routers select BNN or BAN when you configure the DLSw/Frame Relay network. When configuring a Frame Relay interface for DLSw, a message prompts you to select either BNN or BAN.

Boundary Network Node (RFC 1490)

Because BNN format does not carry the destination MAC address, incoming LAN frames must be forwarded to a specific PVC for delivery to the host. The router uses a Frame Relay Mapping Table to get the destination MAC address. The table has three fields:

- DLCI, which represents a Frame Relay PVC
- Remote MAC, which is the destination MAC address
- Local MAC, which is a source MAC address

There is one Frame Relay Mapping Table for each physical Frame Relay interface. Each entry must have a value specified for the Local MAC, Remote MAC, or both. Incoming LLC2 packets (such as LAN packets) are checked against the entries in this table. If a match occurs, the router forwards the frame only to the DLCI specified. If no entry is found, then the information is not forwarded out this interface as a BNN packet.

See *Configuring LLC Services* for more information about the Frame Relay Mapping Table.

Boundary Access Node (BAN)

BAN frames use a standard RFC 1490 Bridged 802.5 Over Frame Relay format. Since this is a source-routed frame, you must enable SRB on this interface. When you select BAN, SRB is automatically enabled and you must configure it. Specifically:

- If SRB has not been previously configured on the router, the SRB Global Parameters screen appears.
- The SRB Interface Parameters screen appears.

See *Configuring Bridging Services* for more information about configuring SRB.

Configuring Predefined MACs and Names

Bay Networks routers in your network learn about the locations of remote NetBIOS and SNA systems that are accessible through DLSw services in two ways:

- Through a dynamic process, where DLSw inspects incoming frames to learn the location of remote endstations. This is a DLSw default mechanism.
- Through static definitions where the network administrator defines the location of NetBIOS and SNA systems attached to remote LANs. Static definitions are never required, but may be used to reduce the amount of broadcast messages traversing the network.

Dynamically Learned Remote Systems

Bay Networks routers cache (dynamically learn) the MAC address and NetBIOS name of remote systems.

Local Bay Networks routers receive frames that contain information about the DLSw peer IP address of each remote system that uses DLSw services. This information is learned from broadcast frames (TESTs, XIDs, and NetBIOS) generated by the remote endstations or applications. The router stores this information in separate NetBIOS and MAC caches.

The router uses the learned IP address to locally specify the DLSw peer that can reach the desired endstation. The cache is not used for forwarding traffic during the first LLC2 session, but will be used in new sessions with that endstation.

You can set a timer value that determines when NetBIOS or MAC cache entries are removed from the router. The timer parameters are NetBIOS Cache Age and MAC Cache Age. When the cached entry goes unused for the specified cache age time, or becomes unreachable to new queries, it is removed from the cache and subsequent frames are broadcast to all configured peers.

The router refreshes a cache entry when DLSw services establish a connection to the NetBIOS or SNA system associated with that entry. The router resets the appropriate Cache Age timer to its maximum wait interval.

Statically Defined Remote Systems

To reduce DLSw broadcasts, you can statically define the IP addresses of DLSw peers that can reach remote systems or applications associated with specific NetBIOS names or MAC addresses. These addresses augment any information that the router's MAC and NetBIOS caching mechanisms learn dynamically.

Static entries can exist in two tables:

- Default MAC Peer IP Table -- Each entry contains a MAC address and the IP address of a DLSw peer that can forward packets to this MAC address.
- Default NetBIOS Peer IP Table -- Each entry contains the NetBIOS name and the IP address of the DLSw peer to which this Net BIOS device is connected.

In the local router's Default NetBIOS Peer IP Table, enter the IP address of the remote peer associated with any remote NetBIOS application that you need to reach through DLSw services. Each entry in this table associates the name of a NetBIOS client with the IP address of the DLSw peer that can reach that client.

In the router's Default MAC Peer IP Table, enter the peer IP address of the DLSw peer associated with any remote SNA system or application that you need to reach through DLSw services. Each entry in this table associates the MAC address for an SNA system with the IP address of the DLSw peer that can reach that system.

Unlike dynamically learned entries, statically defined entries remain until you delete them from the Default NetBIOS Peer IP Table or the Default MAC Peer IP Table.

See Chapter 5 for more information about editing the Default NetBIOS Peer IP Table and the Default MAC Peer IP Table.

Configuring DLSw Packaging

Packaging allows multiple DLSw frames (consisting of user data and DLSw’s SSP header) to be placed into a single TCP/IP frame. Packaging enhances router performance and is important for networks with many LAN/WAN segments.

DLSw packaging uses three tuning parameters, all located on the DLSw Global Parameters screen:

- Maximum Package Size
- Packaging Threshold
- Packaging Timeout

For detailed information about configuring the DLSw packaging parameters, refer to Chapter 5.

Configuring DLSw Prioritization

DLSw prioritization is an outbound filtering mechanism that allows you to assign preference to specific types of traffic supported by DLSw. DLSw Prioritization does not affect traffic as it enters the router, but affects the sequence in which data leaves the router slot.

DLSw prioritization uses the following parameters:

- Protocol Priority
- Max Queue Buffers
- Max Queue Size

You can define these parameters in two places:

- For configured peers, you define the parameters independently for each remote peer (each entry in the Peer Table). These are referred to as specific queues.
- For unconfigured (learned) peers, the default values appear on the Global DLSw PP Parameters/Defaults window. Because these are the default queues, the displayed values are also the defaults for the configured peers.

For detailed information about accessing and configuring the DLSw prioritization parameters, refer to Chapter 6.

Configuring DLSw Backup Peers

When you configure a primary peer, you can configure a peer to backup the primary peer connection. The backup peer feature allows you to configure a backup peer IP address, a maximum up time allowed for the backup connection, a hold down time that indicates the amount of time to wait before considering that the primary connection is down and starting the backup connection, and a time interval to ensure that no backup connection starts during a specified start and end time.

The backup peer feature uses the following parameters:

- Backup Config
- Backup IP Address
- Backup Peer Type
- Backup Max Up Time (sec)
- Backup Hold Down Time (sec)
- Backup Start Time (hhmm)
- Backup End Time (hhmm)

For detailed information about accessing and configuring the DLSw backup peer parameters for an RFC 2166 (multicast) peer, see Chapter 4.

For detailed information about accessing and configuring the DLSw backup peer parameters for an RFC 1434, RFC 1795, or V2.0 peer, see Chapter 5.

Configuring DLSw for IP Multicast

To configure DLSw for IP multicasting, you must:

- Configure DLSw to run in RFC 2166 multicast mode
- Enable IGMP
- Supply an IP multicast group address
- Assign the IP address connected to the multicast network to a DLSw slot

For detailed information about accessing and configuring DLSw IP multicasting, refer to Chapter 4.

Chapter 4
Starting DLSw

This chapter describes how to enable DLSw services. It assumes that you have read *Configuring and Managing Routers with Site Manager* and completed the following steps:

1. Opened a configuration file
2. Specified router hardware if this is a local-mode configuration file
3. Selected the connector on which you are enabling DLSw

When you enable DLSw, you must specify some parameters; the Configuration Manager supplies default values for the others. If you want to edit the other parameters, see Chapter 5, “Editing DLSw Parameters.”

Appendix A provides a quick reference to the default DLSw parameter settings. You may want to review these settings before editing your DLSw configuration.

Starting DLSw on an Interface

To start DLSw on an interface, begin at the Select Protocols window and select DLSw. The Select Protocols window appears after you select a connector on which you are configuring DLSw.

The steps you take to enable DLSw services depend on whether you are starting DLSw for the first time or a subsequent time.

Starting DLSw the First Time

When you first start DLSw, you use Site Manager to edit parameters that DLSw requires before it can process network traffic. Depending on the type of network interface you are configuring, DLSw displays a series of screens. Table 4-1 lists each type of network interface, the Site Manager screens that appear for that interface, and the required parameters that you must specify before DLSw can start.

Table 4-1. DLSw Startup Screens and Required Parameters

Network Interface	Site Manager Screen	Required Parameters/Options
Ethernet	• DLSw Basic Global Parameters	DLSw Virtual Ring ID For dual-switch: DLSw Peer IP Address (add only)
	• DLSw Basic Interface Parameters	For dual-switch: DLSw Slot IP Address
Token Ring (or other SRB)	• DLSw Basic Global Parameters	SR Internal LAN ID, SR Bridge ID, DLSw Virtual Ring ID For dual-switch: DLSw Peer IP Address (add only)
	• DLSw Basic Interface Parameters	SR Interface Ring ID For dual-switch: DLSw Slot IP Address
SDLC	• SDLC Line Parameters	All parameters required; Clock Source, Internal Clock Speed, Sync Line Coding, Cable Type, RTS Enable
	• DLSw Basic Global Parameters	DLSw Virtual Ring ID For dual-switch: DLSw Peer IP Address
	• DLSw Basic Interface Parameters	For dual-switch: DLSw Slot IP Address
	• DLSw Local Device Configuration/Add	All parameters required

(continued)

Table 4-1. DLSw Startup Screens and Required Parameters *(continued)*

Network Interface	Site Manager Screen	Required Parameters/Options
Frame Relay (Routed SNA, RFC 1490, LLC over Frame Relay)	• BNN (RFC 1490) or BAN (LLC/SRB) • DLSw Basic Global Parameters • DLSw Basic Interface Parameters • LLC2 Frame Relay Mapping/ Add	Select BNN. DLSw Virtual Ring ID For dual-switch: DLSw Peer IP Address For dual-switch: DLSw Slot IP Address DLCI, Remote MAC, Local MAC
Frame Relay (Bridged SNA, RFC 1490, LLC over SRB)	• BNN (RFC 1490) or BAN (LLC/SRB) • DLSw Basic Global Parameters • DLSw Basic Interface Parameters	Select BAN. SR Internal LAN ID, SR Bridge ID, DLSw Virtual Ring ID For dual-switch: DLSw Peer IP Address (add only) SR Interface Ring ID For dual-switch: DLSw Slot IP Address

Table 4-1. DLSw Startup Screens and Required Parameters *(continued)*

Network Interface	Site Manager Screen	Required Parameters/Options
QLLC	• QLLC Mapping Parameters	Map Entry, Adjacent DTE/DCE X.121 Address, Adjacent MAC Address, Partner DTE/DCE X.121 Address, Partner MAC Address
	• DLSw Basic Global Parameters	DLSw Virtual Ring ID For dual-switch: DLSw Peer IP Address
	• DLSw Basic Interface Parameters	For dual-switch: DLSw Slot IP Address
APPN Boundary Function	• APPN Local Node Parameter	Local Node Name
	• APPN Configuration Parameters	MAC Address, SAP
	• DLSw Basic Global Parameters	DLSw Virtual Ring ID For dual-switch: DLSw Peer IP Address
	• DLSw Basic Interface Parameters	SR Interface Ring ID For dual-switch: DLSw Slot IP Address
	• APPN Advanced Global Parameters	Default DLUS Name, Default Backup DLUS Name, Max Send BTU Size, Max Receive BTU Size
	• VCCT Configuration Parameter	Slot Number

Setting the DLSw Basic Global Parameters

This section describes the DLSw basic global parameters if you are configuring DLSw over:

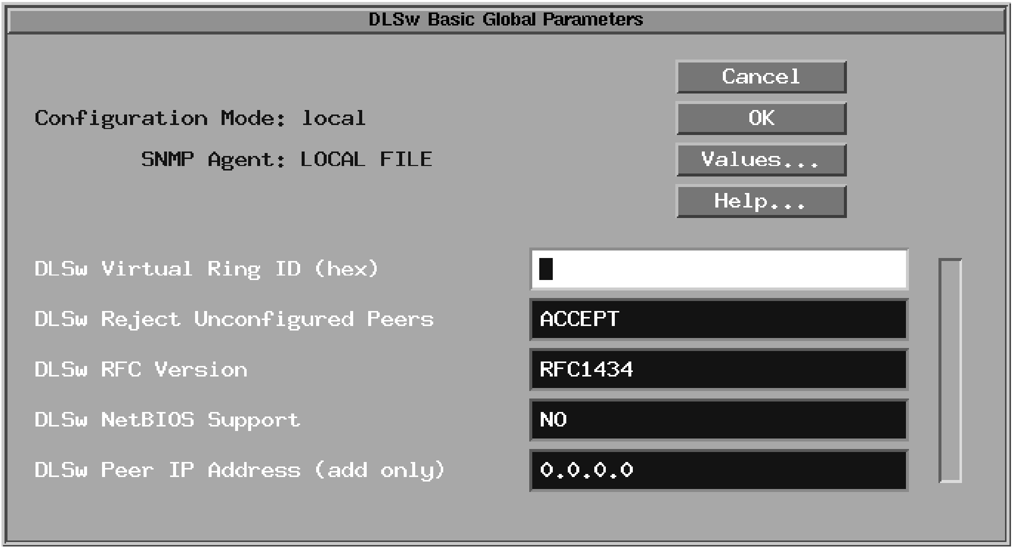
- Ethernet
- SDLC
- Frame Relay BNN (Routed SNA, RFC 1490, or LLC over Frame Relay)
- QLLC
- Boundary Function

After you select DLSw from the Select Protocols window, the DLSw Basic Global Parameters window appears (Figure 4-1).

To set the DLSw global parameters, follow these steps:

1. **Edit the DLSw Virtual Ring ID and the DLSw RFC Version parameters.**
2. **For dual-switch networks, specify the DLSw Peer IP Address.**
3. **Click on OK.**

Optionally, you can edit the remaining parameters on the DLSw Basic Global Parameters window. These parameters are also available from the Protocols > DLSw > Basic Global menu path.



DLSw Basic Global Parameters

Configuration Mode: local

SNMP Agent: LOCAL FILE

DLSw Virtual Ring ID (hex)

DLSw Reject Unconfigured Peers ACCEPT

DLSw RFC Version RFC1434

DLSw NetBIOS Support NO

DLSw Peer IP Address (add only) 0.0.0.0

Figure 4-1. DLSw Basic Global Parameters Window

Following are descriptions of the basic global parameters.

Parameter: **DLSw Virtual Ring ID**

Default: None

Options: Any valid, unassigned ring number from 1 to 4095 (0x001 to 0xFFF) in hexadecimal format

Function: Specifies a standard ring number that SRB uses to identify traffic that DLSw places on the SRB LAN. This ring number is the first entry in the packet's routing information field (RIF).

Instructions: The ring number must be unique within the network. However, all Bay Networks routers on the network can use the same value. The number must be

- Unique among any other ring IDs, group LAN IDs, or internal LAN IDs assigned in the network
- The same as the virtual ring number used by all other DLSw peers on the same TCP/IP network

Entering a hexadecimal value for this mandatory parameter prepares the router for DLSw services on Token Ring/802.5 circuits. (Enter a value even if you are presently configuring DLSw services on Ethernet/802.3 circuits only.) Bay Networks recommends the value 0xFFD if this value is available.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.5

Note: The DLSw Virtual Ring ID parameter provides compatibility with SRB networks locally attached to the router. Site Manager requires you to enter a value for the DLSw Virtual Ring ID, even if you are configuring DLSw services on non-SRB segments locally attached to the same router.

Parameter:	**DLSw RFC Version**
Default:	RFC1434
Options:	RFC1434 | RFC1795 | V2.0 (Unicast) | RFC2166 (Multicast)
Function:	Selects the RFC implementation to run on the router: RFC 1434, RFC 1795, DLSw Version 2.0 (Unicast), or RFC 2166 (Multicast).
Instructions:	Click on Values and select RFC 1434, RFC 1795, V2.0, or RFC 2166. Refer to Chapter 1 for detailed information on these RFCs.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.28

Parameter:	**DLSw Peer IP Address (add only)**
Default:	0.0.0.0
Options:	Any valid, 32-bit IP address of the form *network.host* (using dotted-decimal notation)
Function:	Specifies the IP address of a remote DLSw peer. Once added to the DLSw peer table, this address defines a “configured peer” on the local router. Configured peers receive all DLSw-related broadcast frames for a given router or network processor.
Instructions:	Enter the IP address at which the configured peer will receive all DLSw-related broadcast frames. This parameter is optional in single-switch DLSw configurations.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.3

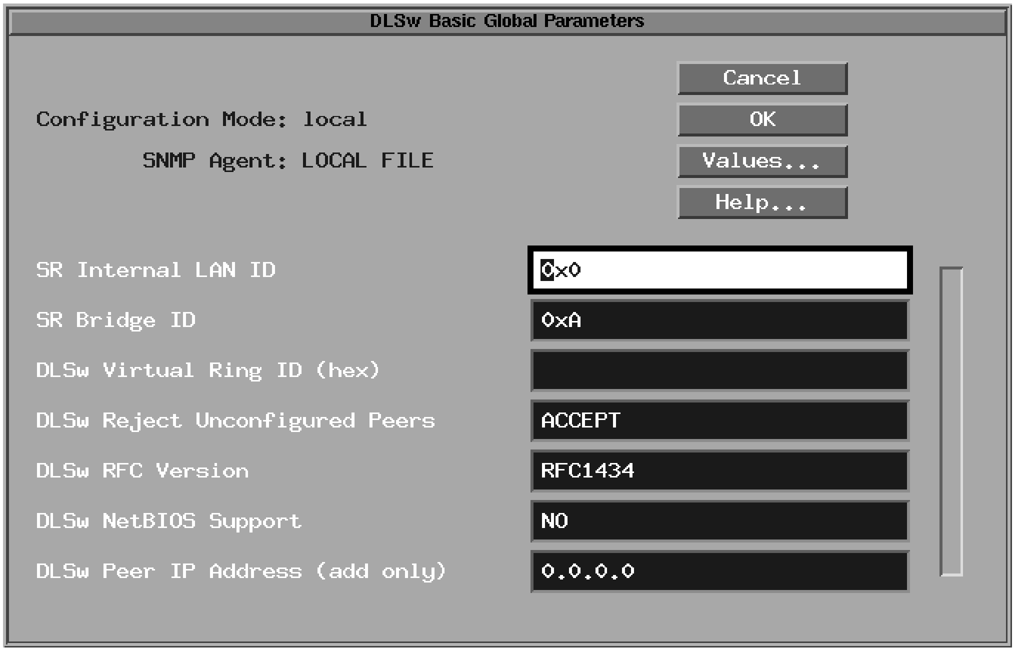
Setting the SRB Basic Global Parameters

This section describes the DLSw basic global parameters if you are configuring DLSw over:

- Token Ring (or other SRB network)
- Frame Relay BAN (Bridged SNA, RFC 1490, or LLC over SRB)

Adding Source Routing Parameters for Token Ring

When you add DLSw to a Token Ring circuit, you first set the source routing global parameters. If you have not yet enabled source routing on any circuit, the first window to appear is the DLSw Basic Global Parameters window (Figure 4-2). If you have enabled source routing on some other circuit, the first window to appear is the DLSw Basic Interface Parameters window (Figure 4-5 on page 4-12).



DLSw Basic Global Parameters

Configuration Mode: local

SNMP Agent: LOCAL FILE

SR Internal LAN ID: 0x0

SR Bridge ID: 0xA

DLSw Virtual Ring ID (hex):

DLSw Reject Unconfigured Peers: ACCEPT

DLSw RFC Version: RFC1434

DLSw NetBIOS Support: NO

DLSw Peer IP Address (add only): 0.0.0.0

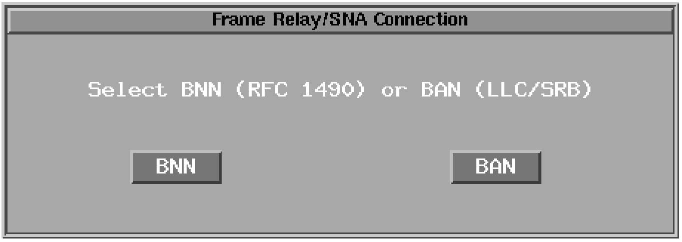
Figure 4-2. DLSw Basic Global Parameters Window (for SRB)

See *Configuring Bridging Services* for detailed information about configuring the following source routing parameters:

- SR Internal LAN ID
- SR Bridge ID

Adding Source Routing Parameters for Frame Relay BAN

When you configure DLSw over Frame Relay BAN, the Frame Relay/SNA Connection window (Figure 4-3) allows you to specify the type of encapsulation formats to be used on the Frame Relay interface.



Frame Relay/SNA Connection

Select BNN (RFC 1490) or BAN (LLC/SRB)

Figure 4-3. Frame Relay/SNA Connection Window

To configure Bay Networks proprietary SRB over Frame Relay using the RFC 1490 Bridging Standard:

1. **Click on BAN.**

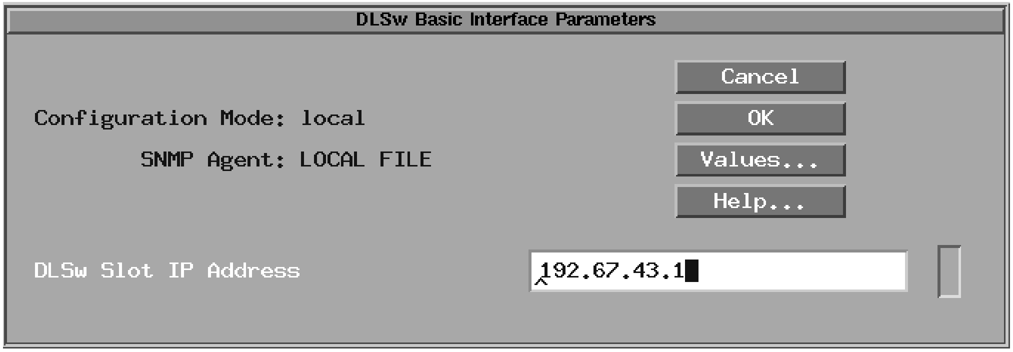
   The DLSw Basic Global Parameters window opens (refer to Figure 4-2).

2. **Edit the SR Internal LAN ID and SR Bridge ID parameters.**

See *Configuring Bridging Services* for detailed information about configuring the source routing parameters.

Setting the DLSw Basic Interface Parameters

The DLSw Basic Interface Parameters window (Figure 4-4) allows you to configure IP addresses on DLSw slots on the router for dual-switch configurations.



DLSw Basic Interface Parameters

Configuration Mode: local

SNMP Agent: LOCAL FILE

DLSw Slot IP Address 192.67.43.1

Figure 4-4. DLSw Basic Interface Parameters Window

To add an IP address to a DLSw slot:

1. **Enter the IP address of the DLSw slot.**

   See the parameter description that follows.

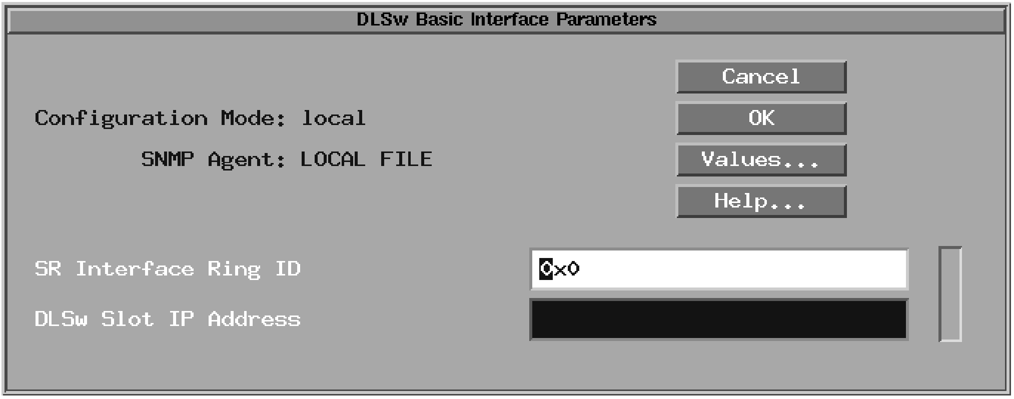
2. **Click on OK.**

Parameter:	**DLSw Slot IP Address**
Default:	0.0.0.0
Options:	Any IP address specified in dotted-decimal notation
Function:	Specifies a unique IP address for each slot running DLSw on the router. The address cannot be reused on another slot. The IP address specifies where the TCP connection for DLSw terminates.
Instructions:	Enter the appropriate IP address. If a circuitless IP address is configured, use that address for this parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.3.1.3

Setting the DLSw Basic Interface Parameters for SRB

If you are configuring a DLSw slot for a Token Ring or Frame Relay BAN network, Site Manager displays the DLSw Basic Interface Parameters window (Figure 4-5) with the SR Interface Ring ID parameter.

See *Configuring Bridging Services* for detailed information on the SR Interface Ring ID parameter.



Configuration Mode: local

SNMP Agent: LOCAL FILE

SR Interface Ring ID 0x0

DLSw Slot IP Address

Figure 4-5. DLSw Basic Interface Parameters Window (for SRB)

Mapping Frame Relay Addresses

If you are configuring a Frame Relay BNN (Routed SNA):

1. **Select BNN from the Frame Relay/SNA Connection Window.**
2. **Edit the DLSw basic global and basic interface parameters, as described earlier.**
3. **When the LLC2 Frame Relay Mappings window opens (Figure 4-6), click on Add.**

   The LLC2 Frame Relay Mapping Add window appears (Figure 4-7).

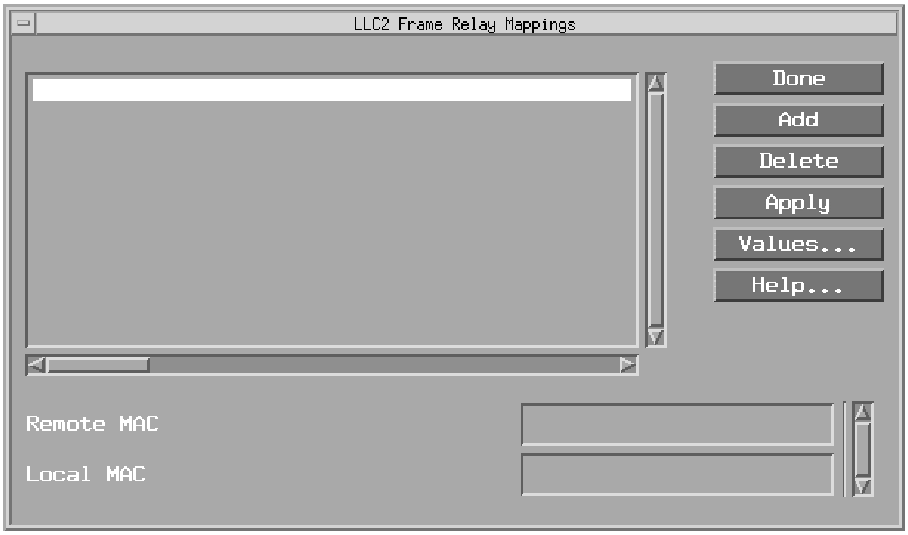
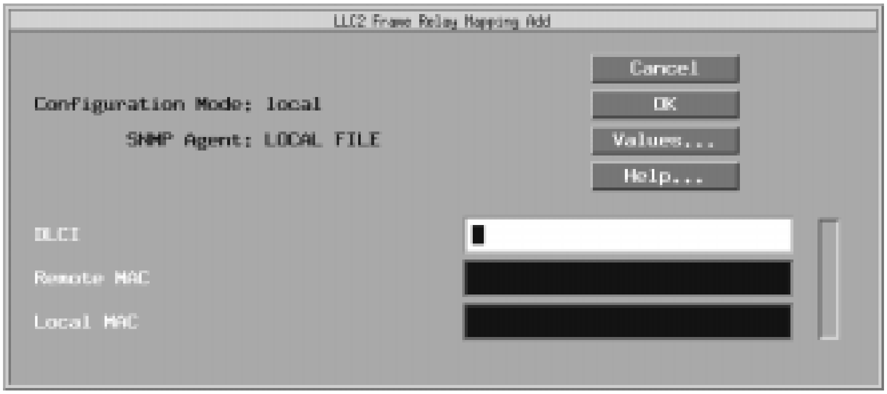


Figure 4-6. LLC2 Frame Relay Mappings Window



Configuration Mode: local

SNMP Agent: LOCAL FILE

Figure 4-7. LLC2 Frame Relay Mapping Add Window

4. **Specify the DLCI, Remote MAC, and Local MAC parameters, as described next.**
5. **Click on OK.**

   The Configuration Manager returns to the LLC2 Frame Relay Mappings window, which now lists the selected circuit.

For more information about mapping DLCIs to MAC addresses, refer to *Configuring LLC Services*.

Parameter: **DLCI**

Default: None

Options: Standard data link connection identifier (DLCI) numbers in hexadecimal format

Function: Provides the number of the virtual circuit to which you are mapping the local or remote MAC address.

Instructions: Enter a hexadecimal DLCI number assigned by your system administrator or Frame Relay provider.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.6.9.1.3

Parameter: **Remote MAC**

Default: None

Options: Standard MSB Token Ring MAC addresses

Function: Provides the remote MAC address, mapping outgoing requests for this MAC address corresponding to the DLCI value. The remote MAC address must be unique, with only DLCI mapping for the specific MAC address.

Instructions: Enter the remote MAC address of the host. If you need to specify the real hardware address of the host, enter it as an octal string.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.6.9.1.5

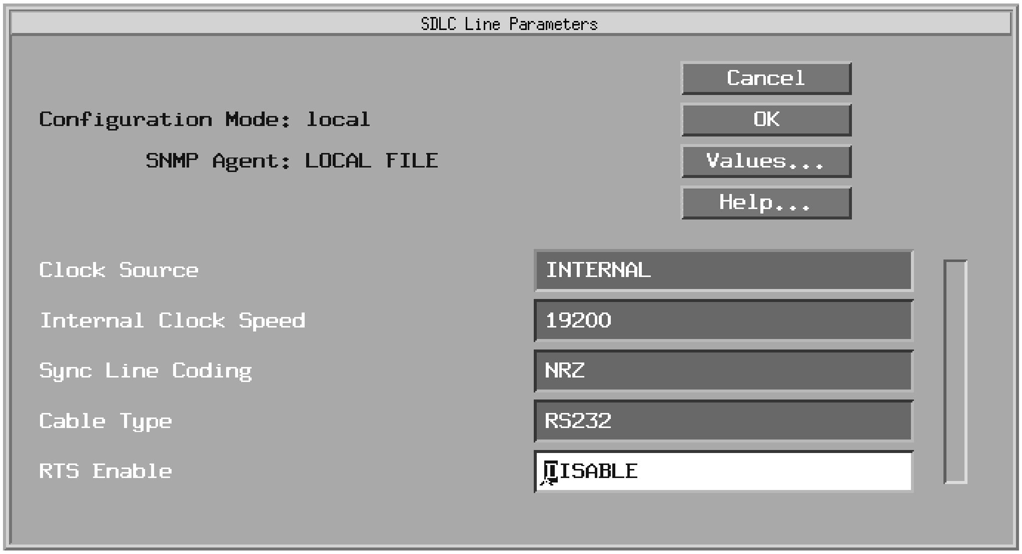
Parameter:	**Local MAC**
Default:	None
Options:	Standard MSB Token Ring MAC addresses
Function:	Provides the local MAC address, mapping incoming requests on this DLCI to that address. The Local MAC address must be unique, with only DLCI mapping for the specific MAC address.
Instructions:	Enter the MAC address of the recipient.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.6.9.1.4

Adding SDLC Line Parameters and Local Devices

To configure DLSw on synchronous interfaces (COM1, COM2, and so on) using the SDLC protocol:

1. **Select SDLC from the WAN protocols window.**

   The Configuration Manager displays the SDLC Line Parameters window (Figure 4-8).



SDLC Line Parameters

Configuration Mode: local

SNMP Agent: LOCAL FILE

Clock Source INTERNAL

Internal Clock Speed 19200

Sync Line Coding NRZ

Cable Type RS232

RTS Enable DISABLE

Figure 4-8. SDLC Line Parameters Window

2. **Edit the Clock Source, Internal Clock Speed, Sync Line Coding, Cable Type, and RTS Enable parameters, described next:**

Parameter:	**Clock Source**
Default:	Internal
Options:	External | Internal
Function:	Identifies whether the router provides clocking to (Internal) or receives clocking from (External) the other device. The parameter specifies the origin of the synchronous timing signals. If you set this parameter to Internal, this router supplies the required timing signals. If you set this parameter to External, an external network device supplies the required timing signals.
Instructions:	For direct connection to a control unit, such as an IBM 3174, set to Internal. For connection to a modem, set to External. For direct connection to an IBM 3745, either the router or the IBM 3745 can provide the clock source. If the IBM 3745 does not provide clocking, set to Internal.
MIB Object ID:	1.3.6.1.4.1.18.3.4.5.1.13

➡ **Note:** When connecting the router directly to an SNA endstation, the cables connecting these devices must connect the “transmit” pins of one device to the “receive” pins of the other. Typically, a DCE cable for the SNA equipment has a male interface and is connected to a Bay Networks synchronous pass-through cable with a female interface. Refer to Appendix C for more information about cables.

Parameter: **Internal Clock Speed**

Default: 19200 KB

Options: 1200 B | 2400 B | 4800 B | 7200 B | 9600 B |
19200 B | 32000 B | 38400 B | 56 KB | 64 KB |
125 KB | 230 KB | 420 KB | 625 KB | 833 KB |
1.25 MB | 2.5 MB | 5 MB

Function: Sets the clock speed of an internally supplied clock when Clock Source is set to Internal. Attached devices must be capable of operating at the specified speed. Some of the more common allowed speeds for IBM products are as follows:

- An IBM 3274 with an V.24/RS-232 interface supports up to 9600 b/s. Some support speeds up to 19200 b/s.
- An IBM 3274 with a V.35 interface supports up to 64 Kb/s.
- An IBM 3174 with a V.24/RS-232 interface supports up to 19200 b/s.
- An IBM 3174 with a V.35 interface and running Licensed Internal Code-C supports up to 256 Kb/s.

Instructions: Click on Values and set the clock speed for the internal clock to the desired data transmission rate across the synchronous line.

This parameter is unavailable when Clock Source is set to External.

MIB Object ID: 1.3.6.1.4.1.18.3.4.5.1.14

Parameter: **Sync Line Coding**

Default: NRZ

Options: NRZ | NRZI | NRZI Mark

Function: Sets the same line coding value for all devices attached to the same SDLC link. You can change the value of this parameter to match the line coding of a device at the other end of the line:

- NRZ -- Indicates nonreturn to zero encoding
- NRZI -- Indicates nonreturn to zero inverted encoding
- NRZI Mark -- Indicates nonreturn to zero inverted mark encoding

This parameter is relevant only for the AN® and ASN™ routers, and the Octal Sync module. Other Bay Networks router platforms use NRZ encoding.

Instructions: Select NRZ or NRZI. NRZI Mark is not generally used for SDLC.

MIB Object ID: 1.3.6.1.4.1.18.3.4.5.1.88

Note: NRZI line coding operates only with the following Bay Networks routers: AN, ASN, Octal Sync, and MCT1 with DS0A.

Parameter: **Cable Type**

Default: RS232

Options: Null | RS232 | RS422 | V35 | X21

Function: Specifies the cable interface to the network.

Instructions: Click on Values and select the installed cable interface type.

MIB Object ID: 1.3.6.1.4.1.18.3.4.5.1.83

Parameter: **RTS Enable**

Default: Disable

Options: Enable | Disable

Function: Controls the toggling of the Request to Send (RTS) signal on the interface.

Instructions: Click on Values and select Enable or Disable. For manual dial modems (2-wire), set this parameter to Enable. For leased modems (4-wire), set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.4.5.1.16

3. **Click on OK.**

   The Select Protocols window appears (Figure 4-9).

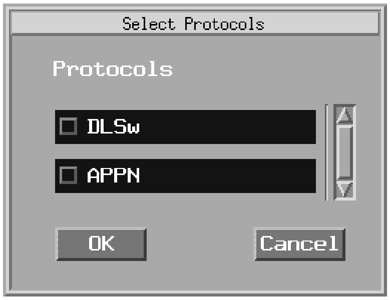


Figure 4-9. Select Protocols Window

4. **Select DLSw and click on OK.**
5. **Edit the DLSw basic global and basic interface parameters, as described earlier.**

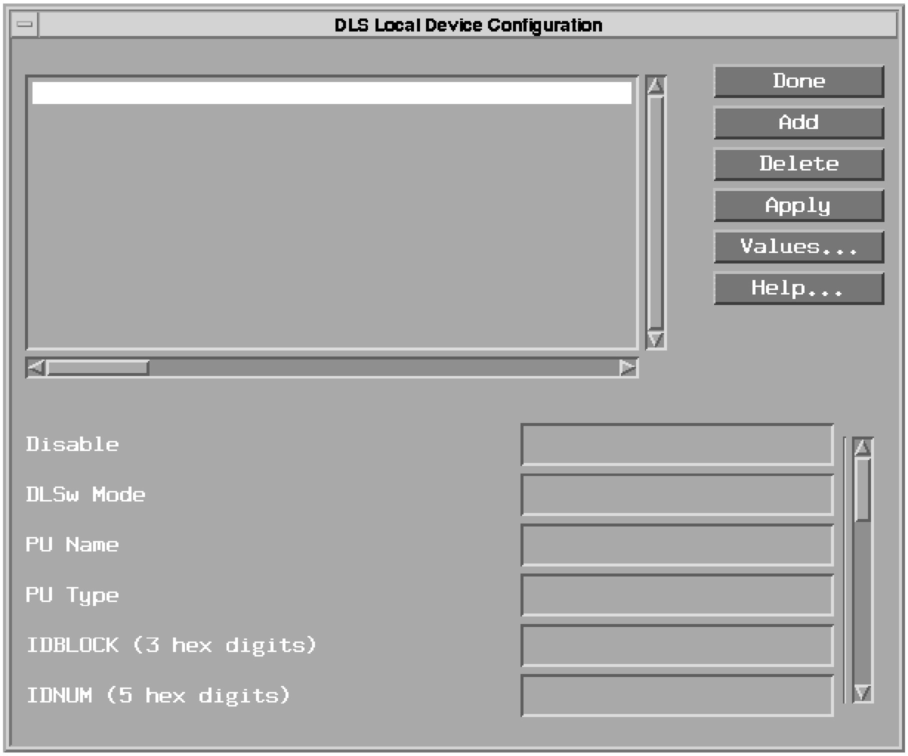
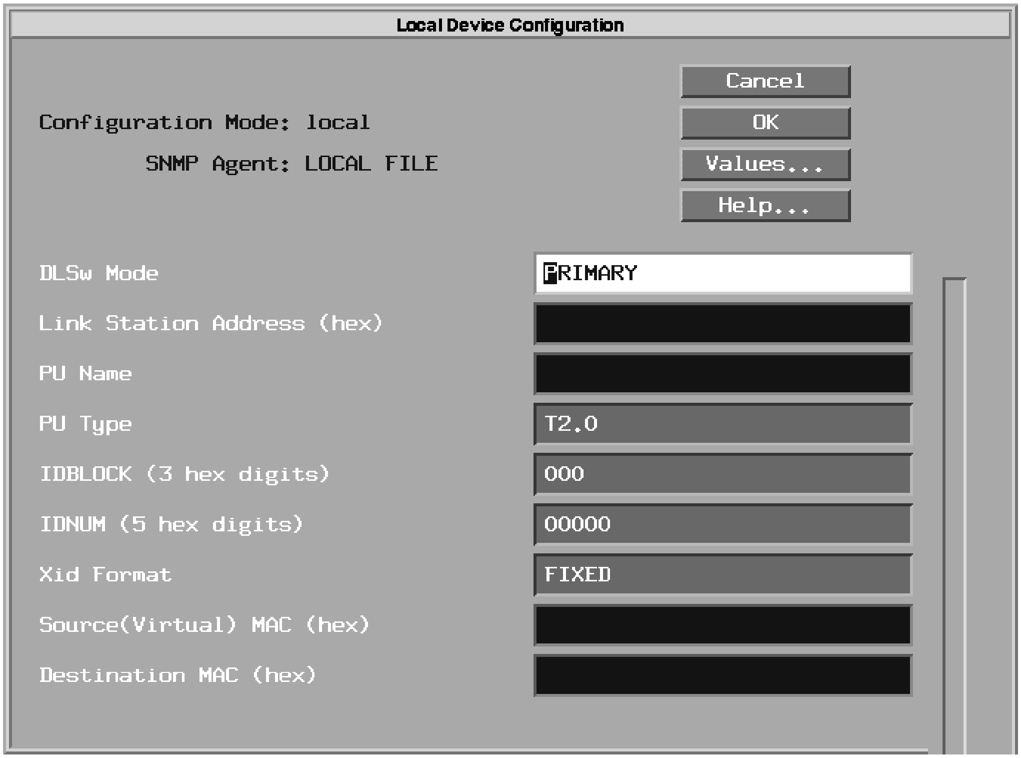


Figure 4-10. DLS Local Device Configuration Window

6. **From the DLS Local Device Configuration window (Figure 4-10), click on Add.**

   The Local Device Configuration window appears (Figure 4-11). To take advantage of integrated SDLC services in DLSw, you must define the SDLC devices that you want to appear as natively attached to the LAN. When you define such devices, you map the devices to LAN MAC and SAP addresses.



Local Device Configuration

Configuration Mode: local

SNMP Agent: LOCAL FILE

DLSw Mode	PRIMARY
Link Station Address (hex)	
PU Name	
PU Type	T2.0
IDBLOCK (3 hex digits)	000
IDNUM (5 hex digits)	00000
Xid Format	FIXED
Source(Virtual) MAC (hex)	
Destination MAC (hex)	

Figure 4-11. Local Device Configuration Window

Following are descriptions of the local device configuration parameters.

Parameter: DLSw Mode

Default: Primary

Options: Primary | Secondary PP | Secondary MP

Function: Specifies the type of link station you are configuring on this node. A primary link station controls a data link, issues commands, polls secondary stations, and initiates error recovery procedures. Only one link station on an SDLC line can be the primary station; all other stations on the line must be secondary. When configured as a primary SDLC link station, the router communicates with downstream PU 2.0 and PU 2.1 nodes.

A secondary link station receives commands and responds to primary link station polls. When configured as a secondary SDLC link station, the router emulates a PU 2.0 device.

Instructions: Click on Values and select Primary, Secondary PP, or Secondary MP.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.2.1.8

Parameter: Link Station Address (hex)

Default: None

Range: Any valid hexadecimal link station address from 0x01 to 0xFE

Function: Specifies the address of the link station. This parameter must match the polling address defined in the SDLC-attached device.

Instructions: Type 0x followed by the link station address.

MIB Object ID: N/A

Parameter: Disable

Default: Enable

Options: Enable | Disable

Function: Enables or disables the DLSw local device.

Instructions: Set to Disable if you want to temporarily disable the local device, rather than delete it. Set to Enable if you want to reinitialize the local device.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.2

Parameter: **PU Name**

Default: None

Options: Any valid, 8-byte ASCII name

Function: Specifies the name of the adjacent link station. This name uniquely identifies the station for statistics and Alert messages.

Instructions: Enter the 8-byte ASCII link station name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.7.5.1.32

Parameter: **PU Type**

Default: None

Options: T1.0 | T2.0 | T2.1

Function: Specifies the type of the XID-sending node. This parameter is used with the IDBLOCK, IDNUM, and XID Format parameters to determine the station exchange identification (XID) value. The value must match the PU type of the SDLC-attached device. For some devices, this is a fixed value. For example:

- IBM 5394 -- PU 1.0
- IBM 3274 -- PU2.0
- IBM 5494 -- PU 2.1.

For other devices, the PU Type is explicitly defined. For example, the IBM 3174 can be configured as PU 2.0 or PU 2.1.

Instructions: Choose T1.0, T2.0 or T2.1.

MIB Object ID: N/A

Parameter: **IDBLOCK**

Default: None

Options: Any 3-digit hexadecimal value

Function: Specifies the block number, which must match the host’s IDBLOCK parameter value that identifies incoming connection requests. This parameter is used with the PU Type, IDNUM, and XID Format parameters to determine the station exchange identification (XID) value. Table 4-2 lists the IDBLOCK numbers.

Instructions: Obtain the configured value at the host (from VTAM or other host operating system) for this device.

MIB Object ID: N/A

Table 4-2. IDBLOCK Numbers for Switched PUs

Device	IDBLOCK Number
NPSI	003
3770	004
3650/3680	005
6100/3790	006
NTO, 3767	007
S/34	00E
3774	011
3x74	017
3276	018
8775	019
S/1	021
S/38	022
5520	031
5280	032
PC/SRJE	03D
S/36	03E
4680	04D
APPC/PC	050
AS/400	056
6150	05C
OS/2 EE	05D
WSP	05E
PC/3270	061
RS/6000	071
Subarea	FFF

Parameter: **IDNUM**

Default: None

Options: Any 5-digit hexadecimal value from 00000 to FFFFF (for T1.0 or T2.0 nodes)

Function: Specifies the ID number, which must match the host’s IDNUM parameter value that identifies incoming connection requests. This parameter is used with the PU Type, IDBLOCK, and XID Format parameters to determine the station XID value.

Instructions: Obtain the configured value at the host (from VTAM or other host operating system) for this device. Type a 5-digit hexadecimal value from 00000 to FFFFF for T1.0 or T2.0 nodes.

MIB Object ID: N/A

➡ **Note:** IDBLOCK and IDNUM (required for PU 1.0 or 2.0 devices only) must match the same values on the host. The 3-digit IDBLOCK and the 5-digit IDNUM may be defined on the host as a single 8-digit XID.

Parameter: **XID Format**

Default: None

Options: FIXED | VARIABLE1 | VARIABLE2

Function: Specifies the format of the XID I-field. This parameter is typically set to FIXED for PU 2.0 devices, VARIABLE 1 for PU 1.0 devices, and set to VARIABLE2 for PU 2.1 devices.

Instructions: Enter one of the following options:

- FIXED -- Fixed format; most often used for PU 2.0 devices
- VARIABLE1 -- Variable format (for T1.0/T2.0/T2.1 to T4/T5 node exchanges), mostly used for PU 1.0 devices
- VARIABLE2 -- Variable format; most often used for PU 2.1 devices (for T2.1 to T2.1/T4/T5 node exchanges)

MIB Object ID: N/A

Parameter: **Source (Virtual) MAC (hex)**

Default: None

Options: Any standard MSB Token Ring MAC address

Function: Specifies the source MAC address of an emulated Token Ring endstation for this device. This parameter must be defined in the LAN gateway when using an IBM 3174 or compatible gateway. Other gateways typically do not define this value.

Instructions: Enter the 12-digit hexadecimal source MAC address that you want to assign to the SDLC device. The address should be in most significant bit (MSB) format, and it should be unique in the network (even among other source addresses on the router).

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.6

Parameter: **Source (Virtual) SAP (hex)**

Default: 0x4

Range: 0x01 to 0xFE

Function: Specifies the source service access point (SAP) of an emulated Token Ring or Ethernet endstation for this device. This parameter must be entered into the SAP Table of the source and destination routers. The default (04) is included in the default SAP Table.

Instructions: Begin the address with 0x and enter a 1-digit or 2-digit hexadecimal source SAP address associated with this device. Typical values are multiples of 4.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.7

Parameter: Destination (Host) MAC (hex)

Default: None

Options: Any standard MSB Token Ring MAC address

Function: Identifies (with the Destination SAP) the Token Ring or Ethernet host that the local device will reach via SDLC services. This parameter must match the MAC address of the LAN gateway, using MSB (Token Ring) format.

Instructions: Consult your host system manager for the host MAC address; then enter the 12-digit hexadecimal address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.8

Parameter: Destination (Host) SAP (hex)

Default: 0x4

Range: 0x01 to 0xFE

Function: Identifies (with the Destination MAC) the Token Ring or Ethernet host that the local device will reach via SDLC services. This parameter must be entered into the SAP Table of the source and destination routers. The default (04) is included in the default SAP Table.

Instructions: Consult your host system manager for the host SAP address. Enter the 0x prefix followed by a 1-digit or 2-digit hexadecimal address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.9

Parameter: MAXOUT

Default: 7

Range: 1 to 127

Function: Controls the maximum number of consecutive frames that an SDLC link station can send without acknowledgment.

Instructions: Enter a value from 1 to 127.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.7.5.1.10

Parameter: **MAXDATA**

Default: 2057

Options: 265 | 521 | 1033 | 2057

Function: Specifies the maximum frame size that SDLC supports. This value includes the transmission header (TH), request header (RH), and request unit (RU).

Instructions: Enter a maximum frame size equal to or larger than the largest frame size that will be received.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.7.5.1.7

Parameter: **Canureach Timer**

Default: 30

Range: 0 to 3600

Function: Specifies the time interval (in seconds) after which the router sends a CANUREACH message to the remote DLSw peer to establish a session.

Instructions: Enter the number of seconds you want for the time interval. For example, enter 1 to transmit a CANUREACH message once per second, or enter 3600 to transmit the message once per hour. Enter 0 if you do not want to transmit a CANUREACH message.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.11

Parameter: **Canureach Retries**

Default: 4294967295

Range: 0 to 4294967295

Function: Specifies the number of times a CANUREACH message is initially sent to the remote DLSw peer to establish a session.

Instructions: Enter the number of retries you want. Enter 0 if you do not want to transmit CANUREACH messages. Leave the default value 4294967295 to send an infinite number of CANUREACH messages for this connection.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.12

Parameter:	**Canureach Timer2**
Default:	30
Range:	0 to 3600
Function:	Specifies the time interval (in seconds) after which the router sends a canureach message to the remote DLSw peer to establish a session. This parameter setting becomes active when the Canureach Timer and Canureach Retries settings expire. Set the Canureach Timer2 and the Canureach Retries2 parameters in configurations where you want to switch to a longer interval, if the initial connection does not occur within the Canureach Timer and Canureach Retries settings. The slow poll timer would then use the Canureach Timer2 and Canureach Retries2 settings.
Instructions:	Enter the number of seconds that you want for the time interval. For example, enter 1 to transmit a CANUREACH message once per second, or enter 3600 to transmit the command once per hour. Enter 0 if you do not want to transmit a CANUREACH message.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.17

Parameter:	**Canureach Retries2**
Default:	0
Range:	0 to 4294967295
Function:	Specifies the number of times a CANUREACH message is sent to the remote DLSw peer to establish a session. This parameter setting becomes active when the standard Canureach Retries parameter setting expires. Set the Canureach Timer2 and the Canureach Retries2 parameters in configurations where you want to switch to a longer interval, if the initial connection does not occur within the standard Canureach Timer and Canureach Retries settings.
Instructions:	Type the number of retries that you want. Enter 0 if you do not want to transmit CANUREACH messages. Type 4294967295 to send an infinite number of CANUREACH messages for this connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.18

Parameter:	**Link Station Timer**
Default:	30
Range:	0 to 3600
Function:	Sets the time interval (in seconds) after which the router sends a connect request to the local SDLC device to establish a session.
Instructions:	Enter the number of seconds you want for the time interval. For example, enter 1 to send a connect request once a second, or enter 3600 to send a connect request once an hour. Enter 0 if you do not want to send connect requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.13

Parameter:	**Link Station Retries**
Default:	4294967295
Range:	0 to 4294967295
Function:	Specifies the maximum number of times that a connect request is sent to the local SDLC device to establish a session.
Instructions:	Enter the number of retries you want. Enter 0 if you do not want to send connect requests. Leave the default value 4294967295 to send an infinite number of connect requests for this connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.14

Parameter:	**SDLC Receive Credit**
Default:	10
Range:	0 to 200
Function:	Specifies the maximum number of frames that SDLC can send to DLSw. This is a flow control parameter.
Instructions:	Enter the maximum number of frames you want SDLC to send to DLSw. For example, enter 1 if you want DLSw to accept 1 frame from SDLC before it updates the SDLC credit. Enter 0 if you want DLSw to receive an infinite number of frames from SDLC without updating the SDLC credit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.15

Parameter:	**SDLC Transmit Credit**
Default:	10
Range:	0 to 200
Function:	Specifies the maximum number of frames that DLSw can send to SDLC.
Instructions:	Enter the maximum number of frames you want DLSw to send to SDLC. For example, enter 1 if you want DLSw to send only one frame to SDLC until it receives a credit update from SDLC. Enter 0 if you want DLSw to send an infinite number of frames to SDLC without updating the SDLC credit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.16

Parameter:	**Enable XID PassThru**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether XID is to be passed through to SDLC when the host is connected to Token Ring and the remote is SDLC. This parameter is used for PU2.1 circuits.
Instructions:	Accept the default, Disable, or change to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.19

Parameter:	**Device Activation Seq**
Default:	Local Device First
Options:	Local Device First | Peer First
Function:	Specifies the sequence of activation for SDLC PU2.0 fixed format primary devices. LocalDeviceFirst specifies that DLS establishes a connection with the SDLC End Station first. Once the local device responds successfully, DLS then starts up the SSP connection to the peer. PeerFirst specifies that DLS starts the SSP connection first, and contacts the SDLC End Station only after receiving a CONTACT message from the peer.
Instructions:	Accept the default, Local Device First, or change to Peer First.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.12

Configuring the DLSw/APPN Boundary Function

Configuring the DLSw boundary function involves the following tasks:

1. **Configuring DLSw and APPN on the router**
2. **Creating a virtual circuit and adding a DLSw interface**
3. **Obtaining an APPN interface to an existing virtual circuit**
4. **Adding an APPN interface to an existing virtual circuit**

This section also describes how to disable and reenable the Boundary function.

Configuring DLSw and APPN

Before you can configure the DLSw boundary function, DLSw and APPN must be running on the same slot on the router. Using Site Manager:

1. **Configure DLSw on a slot.**

   See “Starting DLSw on an Interface,” earlier in this chapter, for instructions.

2. **Configure APPN on the same slot as DLSw.**

   You must supply information for the following APPN advanced global parameters:

   - Default DLUS Name
   - Default Backup DLUS Name

   Set the Max Send BTU Size and Max Receive BTU Size APPN advanced port parameters. Set these parameters according to the size supported by the end device. If you enable HPR support, set these parameters to 768 or greater.

   The DLSw/APPN boundary function requires a setting of Enable for the Implicit DLUR parameter. When you configure the DLSw/APPN boundary function, Site Manager automatically sets the Implicit DLUR parameter to Enable. Make sure that this parameter is properly set.

   For information about configuring APPN, see *Configuring APPN Services*.

Creating a Virtual Circuit and Adding a DLSw Interface

Begin at the Configuration Manager window:

1. **Click on Protocols.**

   The Protocols menu opens.

2. **Click on DLSw.**

   The DLSw window opens.

3. **Click on Boundary Function.**

   The Boundary Function window opens.

4. **Click on Add VCCT.**

   Site Manager asks: “Do you want to create a new Virtual Circuit or use an existing one?”

5. **Click on OK to create a new virtual circuit and add a DLSw interface to the virtual circuit.**

   The VCCT Slot Configuration window opens.

6. **Specify a slot for the virtual circuit you are creating.**

   The slot you choose for the virtual circuit must be the same slot on which DLSw and APPN are running.

7. **Click on OK.**

   You return to the Configuration Manager window.

You have now created a virtual circuit and added a DLSw interface to the circuit.

To configure the DLSw/APPN boundary function, you must now add an APPN interface to the same virtual circuit as described in “Adding an APPN Interface to an Existing Virtual Circuit,” later in this chapter.

Obtaining the Virtual Circuit Number

Site Manager assigns a circuit number to each virtual circuit you create. When you add an APPN interface to the virtual circuit you are using to support the boundary function, you must specify the circuit number assigned to the VCCT. To obtain this information:

1. **Click on Protocols.**

   The Protocols menu opens.

2. **Click on Global Protocols.**

The Global Protocols window opens.

3. **Click on VCCT.**

   The VCCT menu opens.

4. **Click on Interfaces.**

   The VCCT Circuits window opens, listing all the virtual circuits on the router. Each entry specifies the slot and circuit number of the virtual circuit.

5. **Make a note of the circuit number of the VCCT you created and click on Done.**

   You return to the Configuration Manager window.

Adding an APPN Interface to an Existing Virtual Circuit

Begin at the Configuration Manager window:

1. **Click on Protocols.**

   The Protocols menu opens.

2. **Click on APPN.**

   The APPN window opens.

3. **Click on Boundary Function.**

   The Boundary Function window opens.

4. **Click on Add VCCT.**

   Site Manager asks: “Do you want to create a new Virtual Circuit or use an existing one?”

5. **Click on Cancel to use an existing virtual circuit.**

   The VCCT CCT Configuration window opens.

6. **Supply the slot and circuit number of the virtual circuit to which you want to add an APPN interface.**

7. **Click on Done.**

   The APPN Configuration window opens.

8. **Supply a MAC address and an SAP for the interface, as described in *Configuring APPN Services*.**

9. **Click on Done.**

Site Manager asks: “Would you like to configure Adjacent Link Stations on this port?”

10. **Click on Cancel.**

    You return to the Configuration Manager window.

Disabling and Reenabling the Boundary Function

By default, the DLSw/APPN boundary is enabled on the router. You can use the following Site Manager procedure to disable and reenable it.

Begin at the Configuration Manager window:

1. **Click on Protocols.**

   The Protocols menu opens.

2. **Click on DLSw.**

   The DLSw window opens.

3. **Click on Boundary Function.**

   The Boundary Function window opens.

4. **Click on Global.**

   The Edit VCCT Global Parameters window opens.

5. **Set the Enable parameter.**

6. **Click on OK.**

   You return to the Configuration Manager window.

Configuring DLSw for IP Multicasting

To configure DLSw for IP multicasting, you must:

- Configure DLSw to run in RFC 2166 multicast mode. To do this, set the DLSw RFC Version parameter from the DLSw Basic Global Parameters window (Figure 4-1) to RFC 2166.
- Enable IGMP. See *Configuring IP Multicasting and Multimedia Services* for instructions.
- Supply an IP multicast group address and assign the address to a DLSw slot.

The following procedure shows you how to add DLSw IP multicast support to a router that is already running DLSw:

Begin at the Configuration Manager window:

1. **Click on Protocols.**

   The Protocols menu opens.

2. **Click on DLSw.**

   The DLSw window opens.

3. **Click on Basic Global.**

   The DLSw Basic Global Parameter window opens.

4. **Click on the DLSw RFC Version parameter. Click on the Values button.**

   The Values window opens.

5. **Click on RFC 2166 (Multicast). Then click on OK.**

   The Initial IGMP Global Configuration window opens (if IGMP is not configured).

6. **Set IGMP global parameters (or accept the defaults) and click Save.**

   The DLSw Multicast Configuration window opens.

7. **Click on Add.**

   A second DLSw Multicast Configuration window opens.

8. **Supply an IP multicast group address and associate the address with a slot or slots. Click on OK.**

   The first DLSw Multicast Configuration window reopens.

9. **Edit the parameters, using the descriptions below. If you want to enable the backup feature, select Yes for the Backup Config parameter.**

10. **Click on Done.**

    The Configuration Manager window opens.

Following are descriptions of the DLSw multicast configuration parameters.

Parameter: **Multicast IP Address**

Default: 224.0.10.0

Options: Any valid IP address specified in dotted-decimal notation. The valid range is 224.0.1.0 through 239.255.255.255.

Function: Specifies the multicast IP address of this entry.

Instructions: Enter the appropriate IP address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.3

Parameter: **Slot**

Default: Depends on the number of slots in the router. For a BLN, the default is 00000.

Options: Depends on the number of slots in the router

Function: Specifies the slots that you want to receive and transmit multicast data.

Instructions: Click on the Values button. Select the slots that you want to receive and transmit multicast data. For example, if you select Slots 2 and 3 in a BLN, then the value in the Slot field appears as 01100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.4

Parameter: **Multicast IP Slots**

Default: The value or values you selected for the Slot parameter

Options: Depends on the number of slots in the router

Function: Specifies the slots that you want to receive and transmit multicast data.

Instructions: Accept the value you entered at the Slot parameter on the second DLSw Multicast Configuration window, or click on the Values button and select different slots.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.4

Parameter: Backup Config

Default: No

Options: Yes | No

Function: Enables the parameters that allow you to configure a backup peer.

Instructions: Accept the default, No, or click on the Values button and select Yes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.5

Parameter: Backup IP Address

Default: 0.0.0.0

Options: Any valid, 32-bit IP address of the form *network.host* (using dotted-decimal notation)

Function: Specifies the IP address of a backup DLSw peer and adds the peer to the DLSw Backup Peer IP Table. A backup peer receives all DLSw-related broadcast frames for a given router or network processor if the primary peer router is unavailable or cannot be reached over a TCP connection.

Instructions: Enter the IP address of the backup peer.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.6

Parameter: Backup Peer Type

Default: V20 (Unicast-Unknown)

Options: RFC 1795 | V20 (Unicast-TCP) | V20 (Unicast-Unknown) |
V20 (Unicast-UDP) | RFC 2166 (Multicast)

Function: Specifies the type of this DLSw backup peer.

Instructions: Accept the default, V20 (Unicast-Unknown) or click on the Values button and specify a different type.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.11

Parameter: Backup Max Up Time

Default: 0

Options: 0 to 999999

Function: Specifies the maximum time (in seconds) that the backup peer can remain connected to the local DLSw peer. When the maximum time is reached, the software terminates the TCP connection if there are no active TCP sessions between the routers. The software overrides the Backup Max Up Time parameter setting only if there is an active (non-idle) TCP connection with data transferring between the routers.

Instructions: Type a value in the range 0 to 999999. Specify 0 to disable the Backup Max Up Time parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.7

Parameter: Backup Hold Down Time (sec)

Default: 120

Options: 0 to 2147483647

Function: Specifies the time to wait (in seconds) after the primary peer is declared unreachable before the local router initiates a TCP connection to the backup peer. The hold down time ensures that the primary peer has enough time to respond to a TCP connection request before the local router initiates a TCP connection to the backup peer.

Instructions: Accept the default, 120, or click on the Values button and specify a different value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.8

Parameter: **Backup Start Time (hhmm)**

Default: 1

Options: 0 to 2400

Function: Specifies the start time when a configured backup peer is available. During this time period, the local router can establish a TCP connection with this backup peer if the primary peer is unreachable.

Instructions: Type the start time in *hhmm* format, where *hh* is hours and *mm* is minutes. For example, typing 0820 specifies 8:20 a.m., and 2400 specifies 12:00 midnight. Type 0 to disable the Backup Start Time parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.9

Parameter: **Backup End Time (hhmm)**

Default: 2400

Options: 1 to 2400

Function: Specifies the end time when a configured backup peer is available. During this time period, the local router can establish a TCP connection with this backup peer if the primary peer is unreachable.

Instructions: Type the end time in *hhmm* format, where *hh* is hours and *mm* is minutes. For example, typing 0820 specifies 8:20 a.m., and 2400 specifies 12:00 midnight. The Backup End Time parameter is disabled if the Backup Start Time is set to 0.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.10

Chapter 5
Editing DLSw Parameters

This chapter describes how to edit DLSw basic and advanced global and interface parameters, as well as how to add, edit, and delete the following configuration objects:

- Configured peers
- Slots
- SAPs
- Default NetBIOS peers
- Default MAC peers
- Local devices

This chapter also describes how to delete DLSw services from all circuits simultaneously.

The Site Manager sequence for adding the first DLSw interface to your router configuration requires you to define an initial set of DLSw configured peers, slots, and SAPs.

Using the Parameter Descriptions

Each DLSw parameter description provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (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, see *Using Technician Interface Software*.

⛔ **Caution:** The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

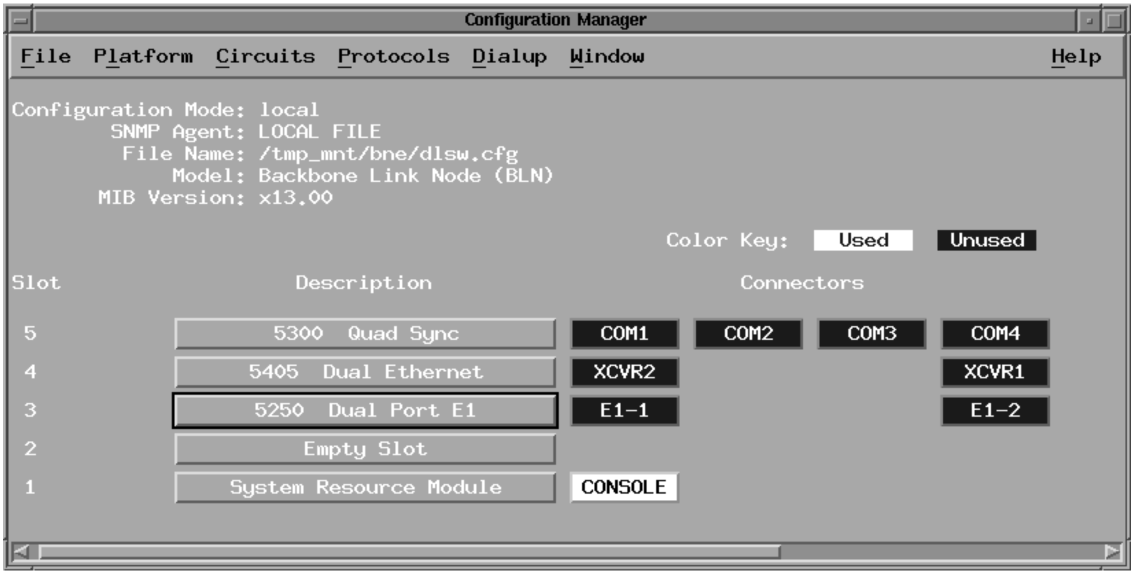
You may be required to customize the LLC2, TCP/IP, SDLC, or SRB parameters as well, since these support DLSw services on the router. If so, refer to one of the guides listed in Table 5-1. Otherwise, you can access parameters of the DLSw support protocols from the Protocols menu of the Configuration Manager window or the Circuit Definition window.

Table 5-1. Customizing the DLSw Support Protocols

Protocol	Refer To
TCP	*Configuring IP Utilities*
IP	*Configuring IP Services*
SRB	*Configuring Bridging Services*
LLC2	*Configuring LLC Services*
SDLC	*Configuring SDLC Services*
Multicast DVMRP	*Configuring IP Multicasting and Multimedia Services*
MOSPF	*Configuring IP Multicasting and Multimedia Services*

Accessing DLSw Parameters

To access and edit DLSw parameters, begin at the Configuration Manager window (Figure 5-1) and select Protocols > DLSw.



```
Configuration Mode: local
        SNMP Agent: LOCAL FILE
         File Name: /tmp_mnt/bne/dlsw.cfg
             Model: Backbone Link Node (BLN)
       MIB Version: x13.00

                                    Color Key:  Used   Unused

Slot          Description                       Connectors

 5      5300  Quad Sync           COM1    COM2    COM3    COM4
 4      5405  Dual Ethernet       XCVR2                   XCVR1
 3      5250  Dual Port E1        E1-1                    E1-2
 2      Empty Slot
 1      System Resource Module    CONSOLE
```

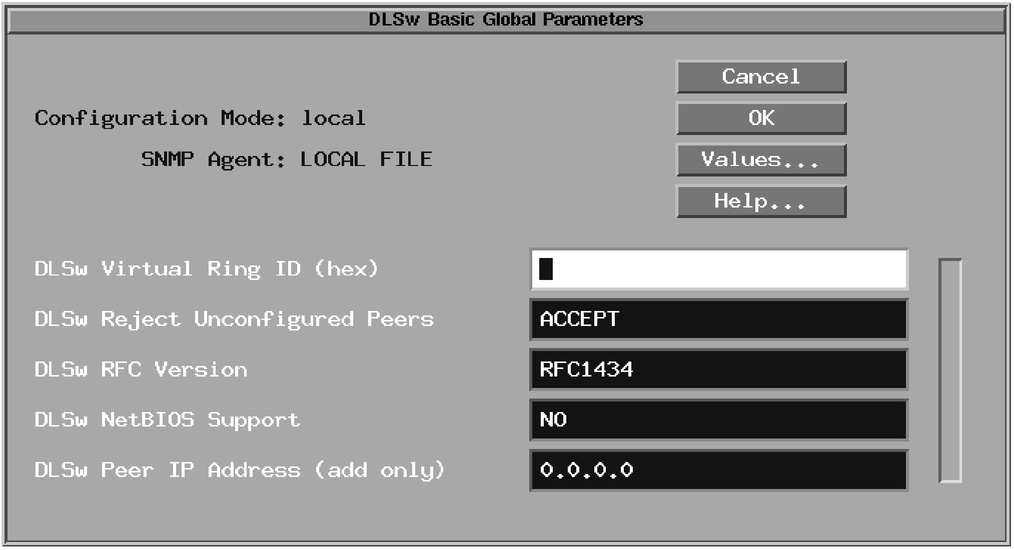
Figure 5-1. Configuration Manager Window

Editing DLSw Basic Global Parameters

To edit DLSw basic global parameters, begin at the Configuration Manager window (Figure 5-1) and then

1. **Select Protocols > DLSw > Basic Global.**

   The DLSw Basic Global Parameters window appears (Figure 5-2).



DLSw Basic Global Parameters

Configuration Mode: local

SNMP Agent: LOCAL FILE

DLSw Virtual Ring ID (hex)

DLSw Reject Unconfigured Peers ACCEPT

DLSw RFC Version RFC1434

DLSw NetBIOS Support NO

DLSw Peer IP Address (add only) 0.0.0.0

Figure 5-2. DLSw Basic Global Parameters Window

2. **Edit the parameters that you want to change.**
3. **Click on OK.**

   This saves your changes and returns you to the Configuration Manager window.

DLSw Basic Global Parameter Descriptions

This section describes the DLSw global parameters that you can customize from the DLSw Basic Global Parameters window.

Parameter: DLSw Virtual Ring ID

Default: None

Options: Any valid, unassigned ring number from 1 to 4095 (0x001 to 0xFFF) in hexadecimal format

Function: Specifies a standard ring number that SRB uses to identify traffic that is placed on the SRB LAN by DLSw. This ring number is the first entry in the packet’s routing information field (RIF).

Instructions: The ring number must be unique within the network. However, all Bay Networks routers on the network can use the same value. The number must be

- Unique among any other ring IDs, group LAN IDs, or internal LAN IDs assigned in the network
- The same as the virtual ring number used by all other DLSw peers on the same TCP/IP network

Entering a hexadecimal value for this mandatory parameter prepares the router for DLSw services on Token Ring/802.5 circuits. Enter a value even if you are presently configuring DLSw services on Ethernet/802.3 circuits only. Bay Networks recommends the value 0xFFD if this value is available.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.5

Parameter: DLSw Reject Unconfigured Peers

Default: Accept

Options: Accept | Reject

Function: Specifies whether DLSw peers in this router should allow (Accept) or disallow (Reject) TCP sessions with other DLSw peers not defined in the DLSw Peer Table.

Instructions: Select Accept if you want to allow TCP sessions with Bay Networks or other DLSw peers not defined in the Peer Table.

Select Reject if you want to disallow TCP sessions with Bay Networks or other DLSw peers not defined in the Peer Table. Disallowing TCP sessions prevents the router from learning the IP addresses of other peers in the network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.13

Parameter: DLSw RFC Version

Default: RFC1434

Options: RFC1434 | RFC1795 | V2.0 (Unicast) | RFC2166 (Multicast)

Function: Selects the RFC implementation to run on the router: RFC 1434, RFC 1795, DLSw Version 2.0, or RFC 2166.

Instructions: Click on Values and select RFC 1434, RFC 1795, V2.0, or RFC 2166. Refer to Chapter 1 for detailed information on these RFCs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.28

Parameter: DLSw NetBIOS Support

Default: No

Options: Yes | No

Function: Specifies whether this router supports NetBIOS traffic and adds the NetBIOS SAP entry 0xF0 to the SAP Table.

Instructions: Click on Values and select Yes or No. If you specify Yes, the software automatically adds the SAP 0xF0 to the SAP Table.

MIB Object ID: N/A

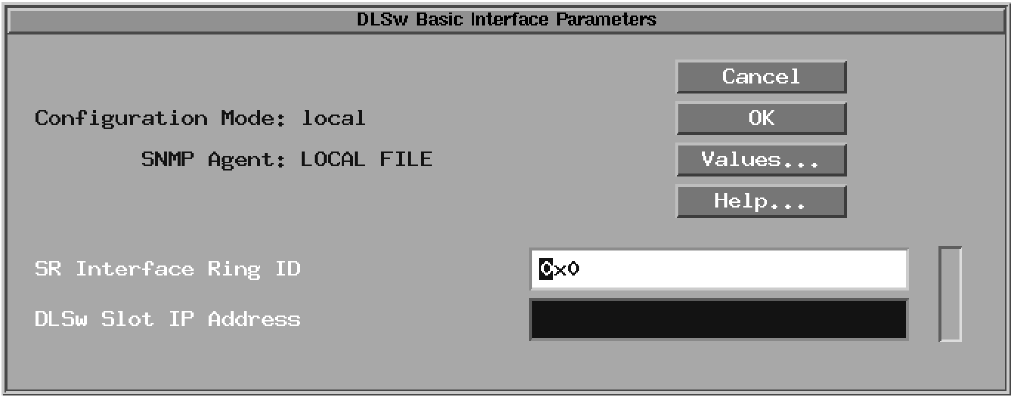
Parameter:	**DLSw Peer IP Address (add only)**
Default:	0.0.0.0
Options:	Any valid, 32-bit IP unicast address of the form *network.host* (using dotted-decimal notation). The valid ranges are 0.0.0.0 through 223.255.255.255 and 240.0.0.0 through 255.255.255.255.
Function:	Specifies the IP address of a remote DLSw peer. Once added to the DLSw peer table, this address defines a “configured peer” on the local router. Configured peers receive all DLSw-related broadcast frames for a given router or network processor.
Instructions:	Enter the IP address at which the configured peer will receive all DLSw-related broadcast frames.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.3

Editing DLSw Basic Interface Parameters

To edit DLSw basic interface parameters, begin at the Configuration Manager window (refer to Figure 5-1) and then

1. **Select Protocols > DLSw > Basic Interface.**

   The DLSw Basic Interface Parameters window appears (Figure 5-3).



Configuration Mode: local

SNMP Agent: LOCAL FILE

SR Interface Ring ID: 0x0

DLSw Slot IP Address:

Figure 5-3. DLSw Basic Interface Parameters

If you are configuring a DLSw slot for a Token Ring or Frame Relay BAN network, edit the SR Interface Ring ID parameter. See *Configuring Bridging Services* for detailed information on the SR Interface Ring ID parameter.

To edit an IP address on a DLSw slot:

1. **Enter the appropriate slot value and its IP address.**
2. **Click on OK.**

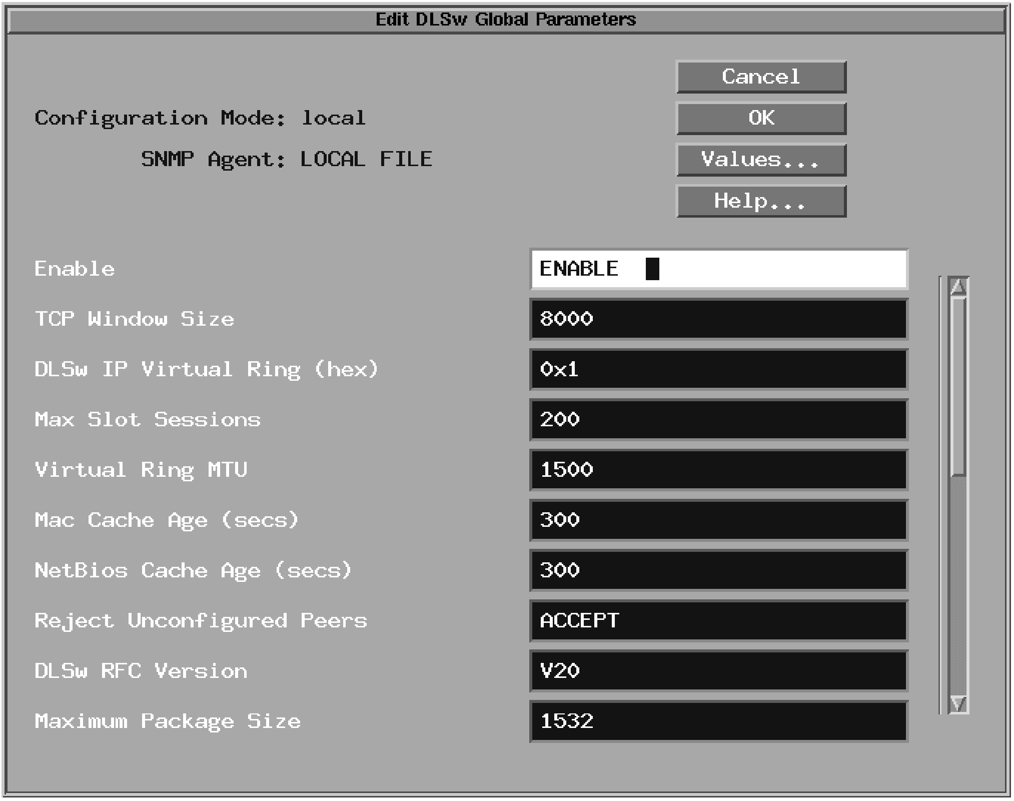
Note: The SR Interface Ring ID only appears if you are configuring Token Ring or Frame Relay BAN.

Parameter:	**DLSw Slot IP Address**
Default:	0.0.0.0
Options:	Any IP address specified in dotted-decimal notation
Function:	Specifies a unique IP address for each slot running DLSw on the router. The address cannot be reused on another slot. The IP address specifies where the TCP connection for DLSw terminates.
Instructions:	Enter the appropriate IP address. If a circuitless IP address is configured, use that address for this parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.3.1.3

Editing the DLSw Advanced Global Parameters

To edit DLSw advanced global parameters, begin at the Configuration Manager window (refer to Figure 5-1) and then select Protocols > DLSw > Advanced > Global.

The Edit DLSw Global Parameters window appears (Figure 5-4). The advanced global parameters include the basic global parameters that you used when you first configured DLSw on the interface. You can edit the basic global parameters if you need to make changes to you DLSw network.



Edit DLSw Global Parameters

Configuration Mode: local

SNMP Agent: LOCAL FILE

Enable	ENABLE
TCP Window Size	8000
DLSw IP Virtual Ring (hex)	0x1
Max Slot Sessions	200
Virtual Ring MTU	1500
Mac Cache Age (secs)	300
NetBios Cache Age (secs)	300
Reject Unconfigured Peers	ACCEPT
DLSw RFC Version	V20
Maximum Package Size	1532

Figure 5-4. Edit DLSw Global Parameters Window

Descriptions of the DLSw advanced global parameters follow.

Parameter: Enable

Default: Enable

Options: Enable | Disable

Function: Globally enables or disables the system software mechanisms that allow you to add DLSw interfaces to the node configuration:

- Disable -- Switches every DLSw interface enabled on the router to the disabled (inactive) state
- Enable -- Reinitializes every DLSw interface on the router, based on:
  - -- The current setting of the associated Enable parameter
  - -- The current state of the associated circuit

Instructions: Select Disable to switch every DLSw interface existing on the node to the inactive state.

Select Enable to globally reinitialize all DLSw interfaces configured on the node.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.2

Parameter:	**TCP Window Size**
Default:	8000
Range:	5000 to 64000 (octets)
Function:	Specifies (in octets) the maximum amount of DLSw data that the local and remote TCP entities can send before requiring an acknowledgment, or can receive before acknowledging. The TCP Window Size parameter informs DLSw about how much data can be outstanding on a TCP connection. The size of the window affects performance, latency, flow control, and memory usage. A larger window causes less flow control to occur with a possible increase in latency. Editing the TCP Window Size parameter affects new TCP session establishment only. Existing sessions are unaffected.
Instructions:	Type any valid number of octets. Generally, networks with slower line speeds require smaller window sizes, while networks with faster line speeds benefit from larger windows. The default value is acceptable for most networks. A TCP Window Size setting of 5000 octets may be appropriate for low-speed lines (or networks running over low speed lines). For high-speed lines, you may want to increase this value, or use the default value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.4

➡ **Note:** The default value is based on both NetBIOS and SNA traffic. SNA and NetBIOS can have frame sizes up to 4 KB, but the default virtual ring MTU limits the frame size on the network to 1500 bytes (unless changed). Keep the window as small as possible. This allows the most consistent response time when packets are not excessively queued in TCP. Selection of this parameter depends on the WAN speed and frame size distribution.

Parameter:	**DLSw IP Virtual Ring**
Default:	None
Options:	Any valid, unassigned ring number from 1 to 4095 (0x001 to 0xFFF) in hexadecimal format
Function:	Specifies a standard ring number that SRB uses to identify traffic that is placed on the SRB LAN by DLSw. This ring number is the first entry in the packet’s RIF.
Instructions:	The ring number must be unique within the network. However, all Bay Networks routers on the network can use the same value. The number must be: • Unique among any other ring IDs, group LAN IDs, or internal LAN IDs assigned in the network • The same as the virtual ring number used by all other DLSw peers on the same TCP/IP network Entering a hexadecimal value for this mandatory parameter prepares the router for DLSw services on Token Ring/802.5 circuits. Enter a value even if you are presently configuring DLSw services on Ethernet/802.3 circuits only. Bay Networks recommends the value 0xFFD if this value is available.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.5

➡ **Note:** The DLSw IP Virtual Ring and Virtual Ring MTU parameters that appear in the Edit DLSw Global Parameters window are primarily for compatibility with SRB networks locally attached to the router. However, Site Manager requires you to enter a value for the IP Virtual Ring, even if you are configuring DLSw services on non-SRB segments locally attached to the same router.

Parameter: Max Slot Sessions

Default: 200

Range: 1 to 10000

Function: Specifies the maximum number of LLC2 sessions that a given slot in the router can support for DLSw requirements. Specifying more sessions per slot has the effect of dedicating more memory and processing resources to DLSw interfaces running on the router.

Instructions: If possible, estimate the maximum number of LLC2 sessions that each DLSw peer slot may need to support concurrently. Type a number that:

- Meets session support requirements for DLSw services provided on any slot of the router
- Allows a balance between the number of sessions supported for DLSw services on a slot, and the amount of resources remaining for other protocols configured on the same slot

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.8

Parameter: Virtual Ring MTU

Default: 1500

Options: Any number of bytes equal to or greater than 1

Function: Specifies an MTU size for frames sent from local, LAN-attached systems to systems on remote LANs. The smallest MTU size supported among all remote LANs in your configuration determines the maximum value of the Virtual Ring MTU parameter for the local router.

The Virtual Ring MTU allows network administrators to limit the size of packets traversing the network. Based on the value that you specify, the router enters the appropriate maximum MTU into any SRB explorer packet that uses DLSw services.

Instructions: Type any number of bytes equal to or greater than 1.

Entering a new value or accepting the default value for this mandatory parameter helps to prepare endstations for the MTUs of remote LANs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.10

Note: Ethernet networks support an MTU size of 1500 bytes, while Token Ring networks support much larger MTUs. When configuring DLSw for local Token Ring-to-Ethernet translation bridge topologies, the Virtual Ring MTU parameter should not exceed 1500. This sets the Token Ring MTU size so that Ethernet endstations can accept the Token Ring traffic.

Parameter: **MAC Cache Age**

Default: 300

Options: Any number of seconds greater than 20

Function: Specifies the maximum number of seconds that inactive MAC addresses can exist in the MAC-to-DLSw mapping cache.

Instructions: Enter an interval to limit the amount of memory that inactive MAC cache entries consume for DLSw services on the router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.11

Parameter: **NetBIOS Cache Age**

Default: 300

Options: Any number of seconds greater than 20

Function: Specifies the maximum number of seconds that inactive NetBIOS names can exist in the NetBIOS-to-DLSw Peer mapping cache.

Instructions: Enter an interval to limit the amount of memory that inactive NetBIOS cache entries consume for DLSw services on the router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.12

Parameter: **Reject Unconfigured Peers**

Default: Accept

Options: Accept | Reject

Function: Specifies whether DLSw peers in this router should allow (Accept) or disallow (Reject) TCP sessions with other DLSw peers not defined in the DLSw Peer Table.

Instructions: Select Accept if you want to allow TCP sessions with Bay Networks or other DLSw peers not defined in the Peer Table.

Select Reject if you want to disallow TCP sessions with Bay Networks or other DLSw peers not defined in the Peer Table. Disallowing TCP sessions prevents the router from learning the IP addresses of other peers in the network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.13

Parameter: **DLSw RFC Version**

Default: RFC1434

Options: RFC1434 | RFC1795 | V2.0 (Unicast) | RFC2166 (Multicast)

Function: Selects the RFC implementation to run on the router: RFC 1434, RFC 1795, or DLSw Version 2.0.

Instructions: Click on Values and select RFC 1434, RFC 1795, or V2.0. Refer to Chapter 1 for detailed information on these RFCs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.28

Parameter:	**Maximum Package Size**
Default:	1532
Range:	0 to 2147483647
Function:	Specifies the maximum amount of information (in bytes) that can reside in one package when sending multiple DLSw frames in a single TCP frame for transmission over a wide area network. DLSw does not split switch-to-switch protocol (SSP) frames (SSP header and user data) among multiple packages.
Instructions:	Specify a value smaller than the TCP Window Size parameter and less than or equal to the Virtual Ring MTU size for the network, minus the size of the TCP/IP and MAC headers. Specify 0 to disable packaging.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.23

Parameter:	**Packaging Timeout (msec)**
Default:	10
Range:	0 to 2147483647
Function:	Specifies the time interval (in milliseconds) to delay a package before sending it to TCP. This value is based on the Packaging Threshold parameter. The value should not be greater than the time it takes to send the number of outstanding bytes before packaging begins.
Instructions:	Type any positive integer in the range 0 to 2147483647.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.24

Parameter: Packaging Threshold

Default: 20

Range: 0 to 100

Function: Specifies the percentage of the DLSw TCP window that must be in use if DLSw is to delay sending a package (one that is currently being built). The default value (20 percent) allows DLSw to send a package to TCP only if the TCP Window is currently using less than 3200 bytes (20 percent of the default TCP Window Size of 16,000 bytes). This mechanism ensures that small packages, such as acknowledgments, are not delayed.

Instructions: Type a value in the range 0 to 100 percent. A value of 50 percent indicates that if 50 percent of the TCP window size is being used, DLSw issues the delay, as specified by the Packaging Timeout parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.25

Parameter: Multislot Broadcasts

Default: Enable

Options: Enable | Disable

Function: Broadcasts received CANUREACH frames over all DLSw slots, or to the specific DLSw slots on which the frames are received.

By default, when the router receives CANUREACH frames over a DLSw port, the software first converts the frames to SNA format before broadcasting the frames across all configured DLSw slots. If you disable this feature, the router will broadcast the frames only over the DLSw slots on which the frames are received.

Instructions: Click on Values and select Enable or Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.26

Note: Because a DLSw slot can have multiple ports (or interfaces), the Multislot Broadcasts parameter setting affects all DLSw ports on the slot on which CANUREACH frames are received.

Parameter: **Initial Pacing Window**

Default: 5

Range: 5 to 100

Function: Specifies the initial number of received data frames that the local DLSw router permits during an established connection with another DLSw router running RFC 1795 or DLSw Version 2. The two DLSw routers advertise their initial pacing value to each other over capabilities exchange messages.

Instructions: Enter a value in the range 5 to 100. Depending on the amount of network traffic during the session, the router may increase or decrease the pacing window size. An increase in the window size means that the router is granting permission to receive more data frames from the sending DLSw router. A decrease in the window size means that the router is reducing the number of data frames that it will accept from the sending DLSw router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.27

Parameter: **NetBIOS Session Alive Filter**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the NetBIOS session alive frame transmissions. Continuously sending session alive frames can cause lines to remain active unnecessarily, possibly increasing the usage cost of the line.

Instructions: Click on Values and select Enable or Disable. Select Enable to start the NetBIOS session alive filter, stopping session alive frame transmissions. Select Disable to cancel the filter and continue session alive frame transmissions every 30 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.29

Parameter:	**KeepAlive Time (sec)**
Default:	60
Range:	0 to 2147483647
Function:	The TCP KeepAlive Time parameter specifies how often the router sends a signal to the peer router to check that the peer router is working correctly and can receive messages. You enable the parameter by specifying a nonzero value. When a keepalive packet goes unacknowledged by the remote peer, retransmission begins at the local peer router. You should tune the keepalive interval based on the total time it takes to send and receive acknowledgment from the remote peer. Since keepalive packets are sent only on idle lines, increasing the keepalive interval may decrease the cost of an idle network. In busy networks, the keepalive interval is not necessary. Frequent traffic for TCP transmission performs the same function as a keepalive setting.
Instructions:	Enter a value appropriate for the network in the range 0 to 2147483647 seconds. We recommend that you set this parameter to the same value on the peer router to maintain synchronization. The default is 60 seconds.
Instructions:	Type the number of seconds that you want for the keepalive time interval, or type 0 to disable the keepalive feature.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.16

Parameter:	**KeepAlive Retry Timer**
Default:	60
Options:	0 to 600
Function:	The Keepalive Retry Timer parameter specifies the maximum time (in seconds) between successive retransmissions of keepalive packets. If an acknowledgment is not received by the local peer router within the TCP keepalive retry timeout, the local peer router retransmits the keepalive packet. The router continues to retransmit keepalive packets at every TCP keepalive retry timeout until it receives an acknowledgment from the remote peer, or until TCP reaches the keepalive retries setting.
Instructions:	Enter a value in the range 0 to 600 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.30

Parameter: **KeepAlive Retries (sec)**

Default: 4

Options: 0 to 99

Function: TCP determines a lost connection (either a failed link with no rerouting possible, or the remote router is unavailable) when TCP attempts to deliver data. If TCP does not receive an acknowledgment to transmitted keepalive packets after a series of retries, it declares the connection inoperable and informs DLSw. The TCP KeepAlive Retries is the number of times TCP attempts to establish or maintain a connection.

Instructions: Enter a value in the range 0 to 99.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.31

Parameter: **SNA Fallback Attempts**

Default: 5

Options: 0 to 2147483647

Function: Specifies the maximum number of attempts the local router should make when establishing a connection with a remote DLSw peer before reverting to earlier DLSw RFCs. The SNA Fallback Attempts parameter operates with DLSw Version 2 peers that you configured with the Transport Type parameter set to Unknown.

An “unknown” peer operates in DLSw Version 2.0 mode. Unless a TCP connection already exists, the local peer will use UDP explorer frames to locate the remote peer MAC address prior to establishing the connection. The remote UDP peer can revert to RFC1795 protocols only if it receives a TCP connection from the local peer along with a Capabilities Exchange message.

Instructions: Enter the number of attempts in the range 0 to 2147483647. Enter 0 to specify that only one connection attempt should be made before reverting to an earlier RFC.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.32

Parameter: **NetBIOS Fallback Time (sec)**

Default: 180

Options: 0 to 2147483647

Function: Specifies the period of time before a peer router (with a Transport Type of Unknown) reverts to RFC 1795 protocols when a NetBIOS name query from the router goes unacknowledged. The TCP Inact Time parameter operates with DLSw Version 2 and with configured DLSw backup peers.

Instructions: Enter a time in the range 0 to 2147483647 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.33

Parameter: **TCP Inact Time (sec)**

Default: 300

Options: 0 to 2147483647

Function: Specifies the period of inactivity to elapse before terminating a TCP connection. Inactivity may result after a prior session has terminated, or if no data has been transferred. The TCP Inact Time parameter functions with DLSw Version 2 and with configured DLSw backup peers.

This parameter operates with the TCP Inact Method parameter.

Instructions: Enter a time in the range 0 to 2147483647 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.34

Parameter: **TCP Inact Method**

Default: Circuits

Options: Never | Circuits | Data

Function: Specifies the type of connection that will cause a TCP connection to terminate when the TCP inactivity time expires. Inactivity results when there is no active DLSw circuit between the local router and a remote peer, or if no data has been transferred between the peers. The TCP Inact Method parameter functions with DLSw Version 2 and with configured DLSw backup peers.

This parameter operates with the TCP Inact Time parameter.

Instructions: Click on Values and select Never, Circuits, or Data:

- Select Never to keep the TCP connection active when the inactivity time expires.
- Select Circuits to disable the TCP connection when a session does not exist between the peers when the inactivity timer expires.
- Select Data to disable the TCP connection if no data has been transferred between the peers when the inactivity timer expires.

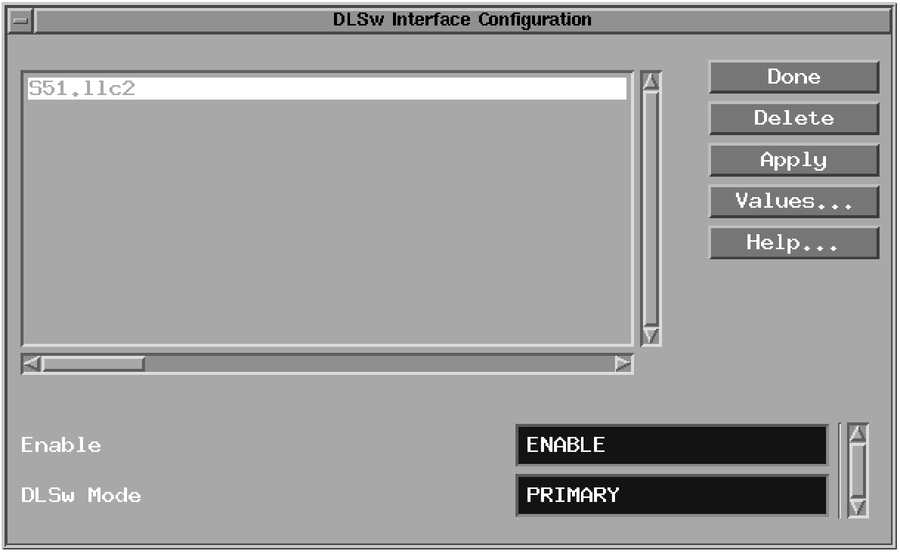
MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.35

Enabling a DLSw Interface

You can use the Configuration Manager to enable or disable a DLSw interface on a specific circuit. To access the DLSw interface parameters from the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols > DLSw > Advanced > Interfaces.**

   The DLSw Interface Configuration window appears (Figure 5-5).



DLSw Interface Configuration

S51.llc2

Enable ENABLE

DLSw Mode PRIMARY

Figure 5-5. DLSw Interface Configuration Window

2. **Select an interface from the list.**

   The interfaces appear in the form *<circuit_name>.llc2.*

3. **Change the setting of the Enable parameter, if necessary.**

   Refer to the parameter description that follows this procedure.

4. **Edit the DLSw Mode parameter if this is an SDLC interface.**

5. **Click on Apply to save your changes.**

6. **Click on Done.**

   The Configuration Manager window reappears.

Following is a description of the parameters in the DLSw Interface Configuration window.

Parameter: **Enable**

Default: Enable

Options: Enable | Disable

Function: Enables or disables Data Link Switching over this interface.

- Enable -- Initializes the DLSw interface that you added to a physical circuit. Also use the Enable setting to reinitialize an existing DLSw interface disabled earlier. The state of the interface depends on the up/down state of the associated circuit and slot.
- Disable -- Switches a DLSw interface from the enabled (up) state to the disabled (down) state.

Instructions: Select Enable if you previously set this parameter to Disable and now want to reenable data link switching over this interface.

Select Disable only if you want to disable data link switching over this interface. This cancels all active LLC2 sessions currently supported by the interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.2.1.2

Parameter: **DLSw Mode**

Default: Primary

Options: Primary | Secondary PP | Secondary MP

Function: Specifies the type of link station that you are configuring on this node. A primary link station controls a data link, issues commands, polls secondary stations, and initiates error recovery procedures. Only one link station on an SDLC line can be the primary station; all other stations on the line must be secondary. When configured as a primary SDLC link station, the router communicates with downstream PU 2.0 and PU 2.1 nodes.

A secondary link station receives commands and responds to primary link station polls. When configured as a secondary SDLC link station, the router emulates a PU 2.0 device.

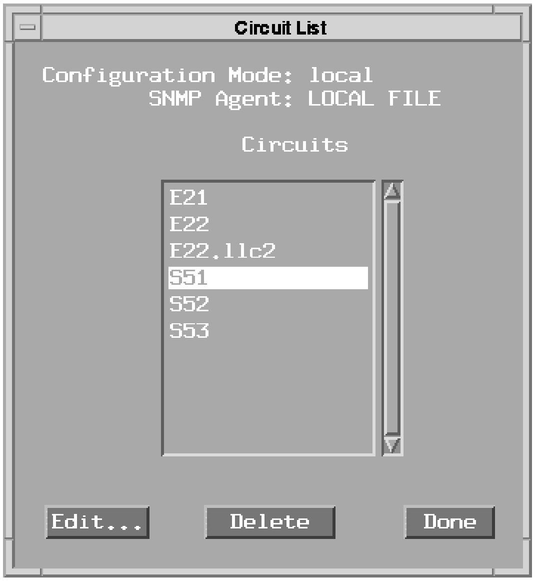
Instructions: Click on Values and select Primary, Secondary PP, or Secondary MP.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.2.1.8

Enabling a DLSw Interface Using the Edit Circuits Function

You can also access the Enable parameter of a DLSw interface through the Edit Circuits function. To do so, begin at the Configuration Manager window (refer to Figure 5-1), and do either of the following:

- Select Circuits > Edit Circuits to open the Circuit List window (Figure 5-6); then select a circuit and click on Edit.
- Select a connector in the Configuration Manager window to open the Edit Connector window (Figure 5-7); then click on Edit Circuit.



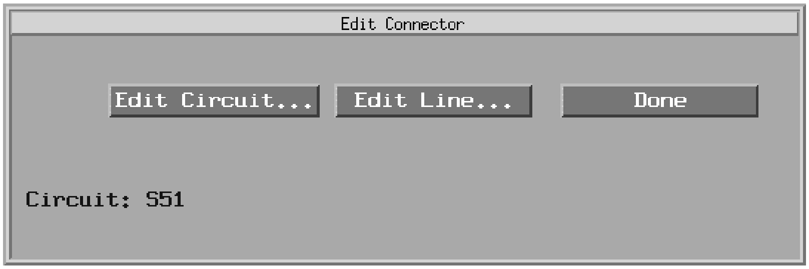
Circuit List

Configuration Mode: local
SNMP Agent: LOCAL FILE

Circuits

E21
E22
E22.llc2
S51
S52
S53

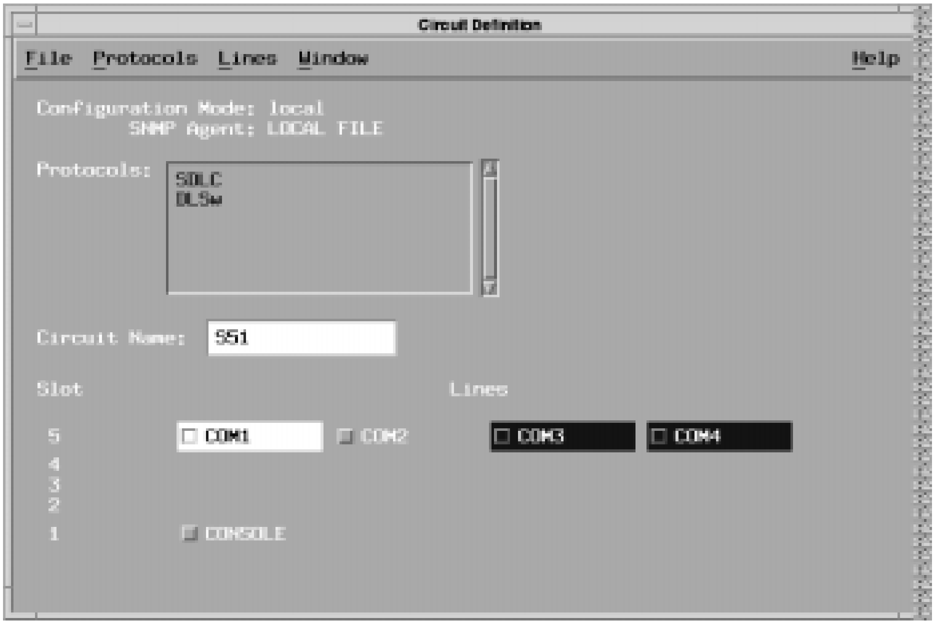
Figure 5-6. Circuit List Window



Circuit: S51

Figure 5-7. Edit Connector Window

In either case, the Circuit Definition window appears (Figure 5-8).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Protocols:
SDLC
DLSw

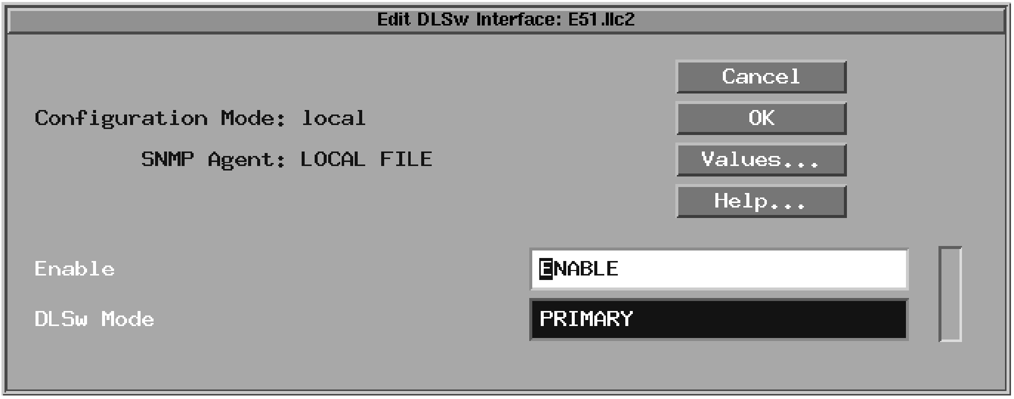
Circuit Name: S51

Figure 5-8. Circuit Definition Window

Follow these steps to enable or disable a DLSw interface:

1. **Select Protocols > DLSw > Interfaces.**

   The Edit DLSw Interface window appears (Figure 5-9).



Edit DLSw Interface: E51.llc2

Configuration Mode: local

SNMP Agent: LOCAL FILE

Enable ENABLE

DLSw Mode PRIMARY

Figure 5-9. Edit DLSw Interface Window

2. **Click on Values and select Enable or Disable.**
3. **If you are editing an SDLC circuit, edit the DLSw Mode parameter by clicking on Values and selecting Primary, Secondary PP, or Secondary MP for the type of SDLC link station in this configuration.**
4. **Click on OK.**

   This closes the Edit DLSw Interface window, and the Circuit Definition window reappears (refer to Figure 5-8).

5. **Select File > Exit.**

The result of Step 5 depends on how you originally accessed the DLSw Interface Enable parameter:

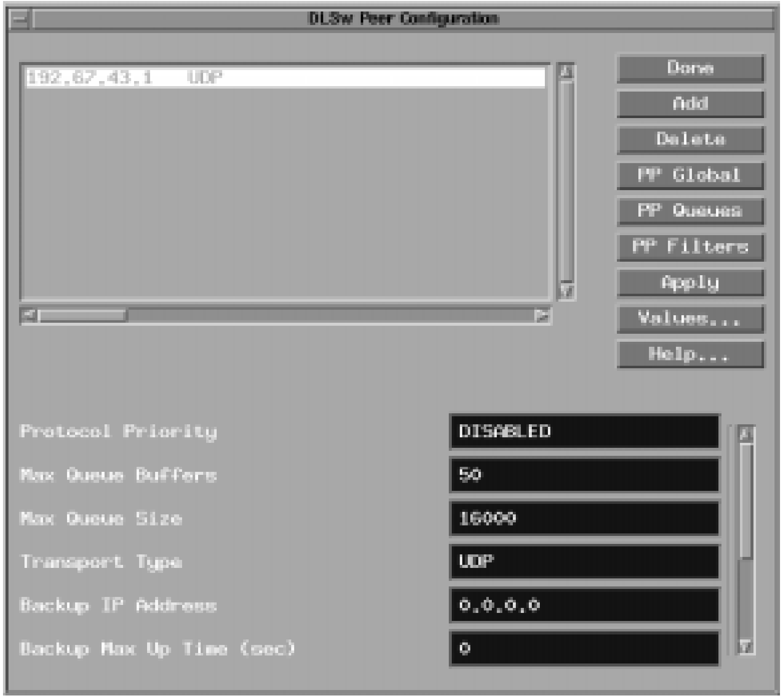
- If you selected Circuits > Edit Circuits from the Configuration Manager window, the Circuit List window appears (refer to Figure 5-6). Clicking on Done in the Circuit List window completes the procedure and returns you to the Configuration Manager window.

- If you selected a connector to invoke the Edit Connector window (refer to Figure 5-7), the Configuration Manager window appears, indicating that you completed the procedure.

Editing DLSw Peer IP Table Parameters

The DLSw Peer IP Table contains the list of all configured remote peers known to the local router. This section describes how to add, edit, and delete configured peers. (Refer to Chapter 3 for more information on configured and unconfigured peers.)

To access the DLSw Peer IP Table, begin at the Configuration Manager window (refer to Figure 5-1) and select Protocols > DLSw > Peer IP Table. The DLSw Peer Configuration window appears, listing all DLSw configured peers known to the local router (Figure 5-10).



192.67.43.1 UDP

Protocol Priority DISABLED
Max Queue Buffers 50
Max Queue Size 16000
Transport Type UDP
Backup IP Address 0.0.0.0
Backup Max Up Time (sec) 0

Figure 5-10. DLSw Peer Configuration Window

Descriptions of the Peer IP Table parameters follow.

Note: The DLSw protocol prioritization and traffic filtering functions are described in Chapter 6. Refer to this chapter for information on the Protocol Priority, Max Queue Buffers, and Max Queue Size parameters, as well as information on the protocol priority buttons in the DLSw Peer Configuration window.

Parameter: **Transport Type**

Default: Unknown

Options: TCP | UDP | Unknown

Function: Specifies the transport capabilities at the remote peer: TCP, UDP, or Unknown. The local router attempts to use this configured transport option when establishing a TCP connection with the remote peer. The Transport Type parameter is available only when the DLSw RFC Version parameter is set to V2.0.

A remote peer configured with the transport type TCP operates in RFC 1795 mode. A remote peer configured with the transport type UDP operates in DLSw Version 2.0 mode only. When set to UDP, the router does not make any attempts to revert to RFC 1795.

An “unknown” peer operates in DLSw Version 2.0 mode. Unless a TCP connection already exists, the local peer uses UDP explorer frames to locate the remote peer MAC address prior to establishing the connection.

The “unknown” peer can revert to RFC 1795 if there is no response to the UDP explorer frames.

Instructions: Click on Values and select TCP, UDP, or Unknown. If you select Unknown, use the SNA Fallback Attempts parameter to set the number of connection attempts using UDP explorer frames before reverting to earlier RFCs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.5.1.10

Parameter: **Backup Config**

Default: No

Options: Yes | No

Function: Enables the parameters that allow you to configure a backup peer.

Instructions: Click on Values and select Yes or No.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.5.1.11

Parameter: **Backup IP Address**

Default: 0.0.0.0

Options: Any valid, 32-bit IP address of the form *network.host* (using dotted-decimal notation)

Function: Specifies the IP address of a backup DLSw peer and adds the peer to the DLSw Backup Peer IP Table. A backup peer receives all DLSw-related broadcast frames for a given router or network processor if the primary peer router is unavailable or cannot be reached over a TCP connection.

Instructions: Enter the IP address of the backup peer.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.5.1.12

Parameter: **Backup Peer Type**

Default: V20 (Unicast - Unknown)

Options: RFC1795 | V20 (Unicast - TCP) | V20 (Unicast - Unknown) | V20 (Unicast - UDP) | RFC2166 (Multicast)

Function: Specifies the type of DLSw backup peer.

Instructions: Accept the default, V20 (Unicast - Unknown), or select a different option.

MIB Object ID: 1.2.6.1.4.1.18.3.5.1.5.5.1.18

Parameter: Backup Max Up Time

Default: 0

Options: 0 to 999999

Function: Specifies the maximum time (in seconds) that the backup peer can remain connected to the local DLSw peer. When the maximum time is reached, the software terminates the TCP connection if there are no active TCP sessions between the routers. The software overrides the Backup Max Up Time parameter setting only if there is an active (non-idle) TCP connection with data transferring between the routers.

Instructions: Type a value in the range 0 to 999999. Specify 0 to disable the Backup Max Up Time parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.5.1.13

Parameter: Backup Hold Down Time (sec)

Default: 120

Options: 0 to 2147483647

Function: Specifies the time to wait (in seconds) after the primary peer is declared unreachable before the local router initiates a TCP connection to the backup peer. The hold down time ensures that the primary peer has enough time to respond to a TCP connection request before the local router initiates a TCP connection to the backup peer.

Instructions: Type a value in the range 0 to 2147483647.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.5.1.14

Parameter: **Backup Start Time (hhmm)**

Default: 1

Options: 0 to 2400

Function: Specifies the start time when a configured backup peer is available. During this time period, the local router can establish a TCP connection with this backup peer if the primary peer is unreachable.

Instructions: Type the start time in *hhmm* format, where *hh* is hours and *mm* is minutes. For example, typing 0820 specifies 8:20 a.m., and 2400 specifies 12:00 midnight. Type 0 to disable the Backup Start Time parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.5.1.15

Parameter: **Backup End Time (hhmm)**

Default: 1

Options: 1 to 2400

Function: Specifies the end time when a configured backup peer is available. During this time period, the local router can establish a TCP connection with this backup peer if the primary peer is unreachable.

Instructions: Type the end time in *hhmm* format, where *hh* is hours and *mm* is minutes. For example, typing 0820 specifies 8:20 a.m., and 2400 specifies 12:00 midnight. The Backup End Time parameter is disabled if the Backup Start Time is set to 0.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.5.1.16

Adding a DLSw Peer IP Table Entry

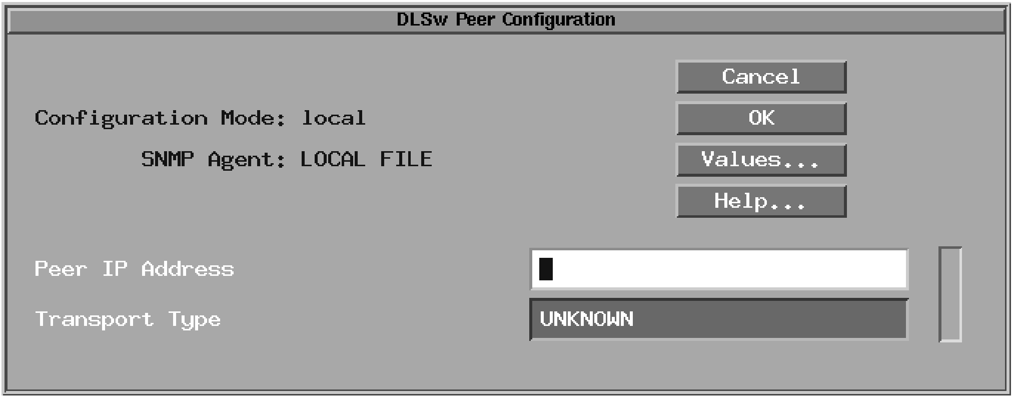
To add a new DLSw Peer IP Table entry, begin at the DLSw Peer Configuration window (refer to Figure 5-10) and then

1. **Click on Add.**

   The second DLSw Peer Configuration window appears (Figure 5-11).

2. **Enter a valid IP address for the Peer IP Address parameter.**

➡ **Note:** Do not enter the IP address of any DLSw peer (slot) that resides in the local router. Enter one IP address for each remote peer router.


DLSw Peer Configuration

Configuration Mode: local

SNMP Agent: LOCAL FILE

Peer IP Address

Transport Type UNKNOWN

Figure 5-11. Add DLSw Peer Configuration Window

3. **Specify the Transport Type.**
4. **Click on OK.**

   This saves the new entry. The DLSw Peer Configuration window reappears (refer to Figure 5-10) with the new entry in the list of existing peers.

5. **Click on Done.**

   The Configuration Manager window reappears.

   Descriptions of the Peer IP Table parameters follow.

Parameter:	**Peer IP Address**
Default:	None
Options:	Any valid, 32-bit IP unicast address in the form *network.host* (using dotted- decimal notation). The valid ranges are 0.0.0.0 through 223.255.255.255 and 240.0.0.0 through 255.255.255.255.
Function:	Specifies the IP address of a remote DLSw peer. Adding this address to the DLSw IP Peer Table defines a configured peer to the local router. Configured peers receive all DLSw-related broadcast frames from the local router.
Instructions:	Type the IP address at which the configured peer should receive all DLSw-related broadcast frames.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.3

Parameter:	**Transport Type**
Default:	Unknown
Options:	TCP | UDP | Unknown
Function:	Specifies the transport capabilities at the remote peer: TCP, UDP, or Unknown. The local router attempts to use this configured transport option when establishing a TCP connection with the remote peer. The Transport Type parameter is available only when the DLSw RFC Version parameter is set to V2.0. A remote peer configured with the transport type TCP operates in RFC 1795 mode. A remote peer configured with the transport type UDP operates in DLSw Version 2.0 mode only. When set to UDP, the router does not make any attempts to revert to RFC 1495. An “unknown” peer operates in DLSw Version 2.0 mode. Unless a TCP connection already exists, the local peer uses UDP explorer frames to locate the remote peer MAC address prior to establishing the connection. The “unknown” peer can revert to RFC 1795 if there is no response to the UDP explorer frames.
Instructions:	Click on Values and select TCP, UDP, or Unknown. If you select Unknown, use the SNA Fallback Attempts parameter to set the number of connection attempts using UDP explorer frames before reverting to earlier RFCs.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.10

Deleting a DLSw Peer IP Table Entry

You cannot edit the Peer IP Address parameter associated with an existing DLSw Peer IP Table entry. To change the IP address of an entry:

1. **Delete the existing entry from the DLSw Peer IP Table.**
2. **Using the appropriate IP address, add a new configured peer entry to the DLSw Peer IP Table.**

   See the preceding section, “Adding a DLSw Peer IP Table Entry.”

To delete a DLSw Peer IP Table entry, start at the DLSw Peer Configuration window (refer to Figure 5-10):

1. **Select the entry to delete.**
2. **Click on Delete.**

   The system software deletes the entry, and the removes entry from the list of configured peers.

3. **Click on Done.**

   The Configuration Manager window reappears.

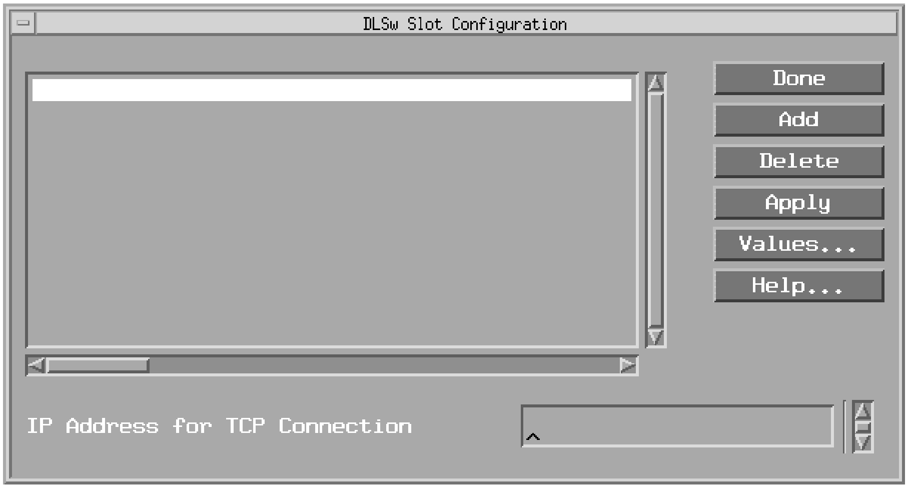
Editing the DLSw Slot IP Table

The DLSw Slot Configuration Table contains a list of all DLSw-capable slots in your router. Each table entry establishes a slot in the router as a DLSw peer on your TCP/IP network.

You identify a slot by its number in the router chassis, and a DLSw peer by its IP interface address on the TCP/IP network. DLSw Slot IP Table entries associate the number of a DLSw-capable slot with the IP network address of that peer slot. This section describes how to add, edit, and delete DLSw Slot IP Table entries.

➡ **Note:** Before you add any entries to the slot table, you must add or allocate one IP interface for each DLSw-capable slot in the router configuration. You need not configure the associated IP and DLSw interfaces on the same slot. You can also use the circuitless IP interface address for a DLSw-capable slot. Using the circuitless IP interface allows TCP connections for DLSw services on that slot to be less dependent on the availability of specific physical circuits or datalinks. For more information about the nature and use of the circuitless IP interface, see *Configuring IP Services*.

To access the DLSw Slot IP Table, begin at the Configuration Manager window (refer to Figure 5-1) and select Protocols > DLSw > Slot IP Table. The DLSw Slot Configuration window appears, showing a list of all slots serving as DLSw peers on your TCP/IP network (Figure 5-12).



IP Address for TCP Connection

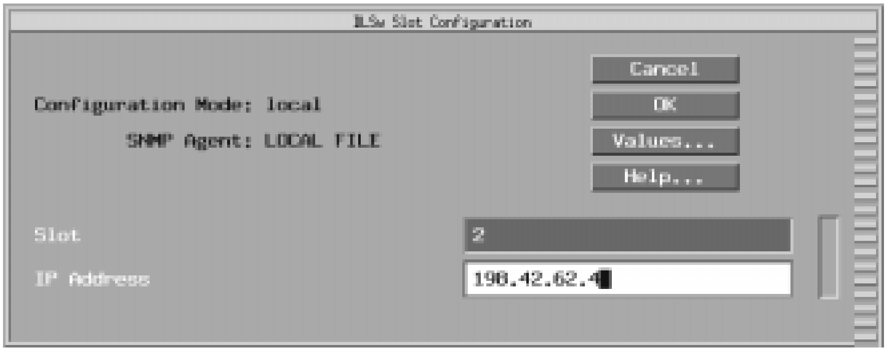
Figure 5-12. DLSw Slot Configuration Window

Adding a DLSw Slot IP Table Entry

To add a new DLSw Slot IP Table entry, begin at the DLSw Slot Configuration window (Figure 5-12) and:

1. **Click on Add.**

   The DLSw Slot Configuration window appears (Figure 5-13).



Configuration Mode: local

SNMP Agent: LOCAL FILE

Slot 2

IP Address 198.42.62.4

Figure 5-13. IP Address in DLSw Slot Configuration Window

2. **Type a value for the Slot parameter.**
3. **Type the IP address of an interface configured earlier on the router.**

   Each DLSw-capable slot requires its own IP interface in the router configuration. Do not specify the same IP interface address for two or more different DLSw-capable slots in the same router configuration.
4. **Click on OK to save your entry to the configuration file.**

   The DLSw Slot Configuration window reappears (refer to Figure 5-12) with the new entry added to the list of existing DLSw-capable slots.

Following are descriptions of the DLSw Slot IP Table parameters.

Parameter: **Slot**

Default: None

Range: 1 to 14

Function: Specifies the slot number that you want to associate with the IP interface address that you reserved for that slot.

Instructions: Type a slot number from 1 to 14, depending on the:

- Type of node/chassis
- Slots that link modules can occupy

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.3.1.2

Parameter: **IP Address**

Default: None

Options: Any valid, 32-bit IP address in the form *network.host* in dotted-decimal notation

Function: Specifies an IP address associated with a specific DLSw peer slot in the router. TCP uses this IP address for connections associated with that slot.

Instructions: Type a valid IP address for the slot. The IP interface need not reside on the DLSw-capable slot. Do *not* enter a value for every active slot in the router; enter one IP address associated with one DLSw slot.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.3.1.3

Editing a DLSw Slot IP Table Entry

You can edit only the IP Address for TCP Connection parameter in an existing DLSw Slot IP Table entry.

To edit the IP address associated with a particular slot, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols > DLSw > Slot IP Table.**

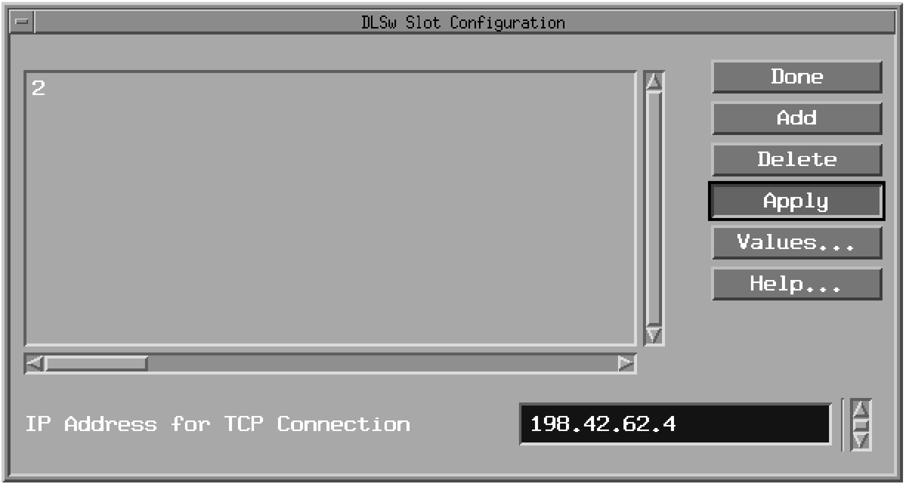
   The DLSw Slot Configuration window appears (Figure 5-14).

2. **Select the DLSw Slot IP Table entry.**

3. **Click on the IP Address for TCP Connection parameter box, and enter a new IP address.**

4. **Click on Apply.**

   This saves your changes to the router configuration file.



IP Address for TCP Connection 198.42.62.4

Figure 5-14. Saving an Edited DLSw Slot IP Address

5. **Click on Done.**

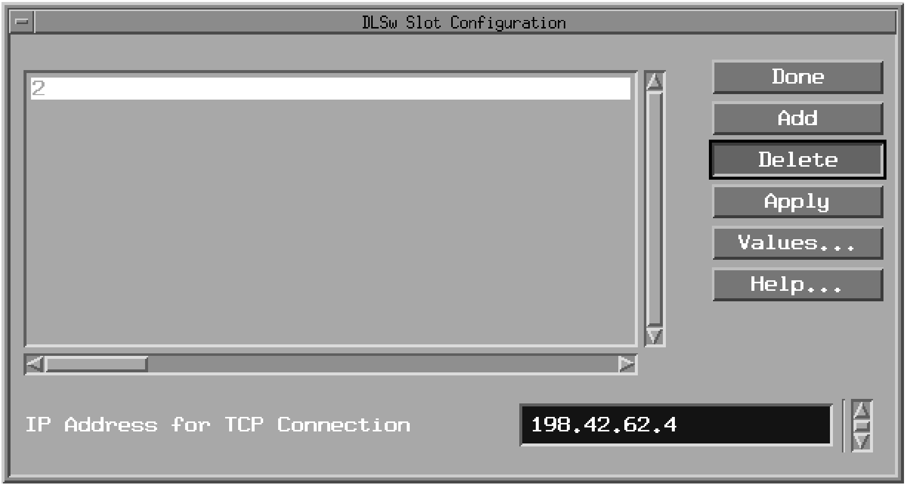
   The Configuration Manager window reappears.

Following is a description of the IP Address for TCP Connection parameter.

Parameter:	**IP Address for TCP Connection**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* in dotted-decimal notation
Function:	Specifies an IP address associated with a specific DLSw peer (slot) in the router. TCP uses this IP address for connections associated with that slot.
Instructions:	Type a valid IP address for each slot. Do *not* enter a value for every active slot in the router; enter only a single IP address associated with a single DLSw slot.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.3.1.3

Deleting a DLSw Slot IP Table Entry

To delete a DLSw Slot IP Table entry, start at the DLSw Slot Configuration window (Figure 5-15):



IP Address for TCP Connection 198.42.62.4

Figure 5-15. Deleting a DLSw Slot Table Entry

1. **Select the Slot IP Table entry.**
2. **Click on Delete.**

   The system software deletes the entry you selected, and the entry disappears from the list.

3. **Click on Done.**

   You return to the Configuration Manager window.

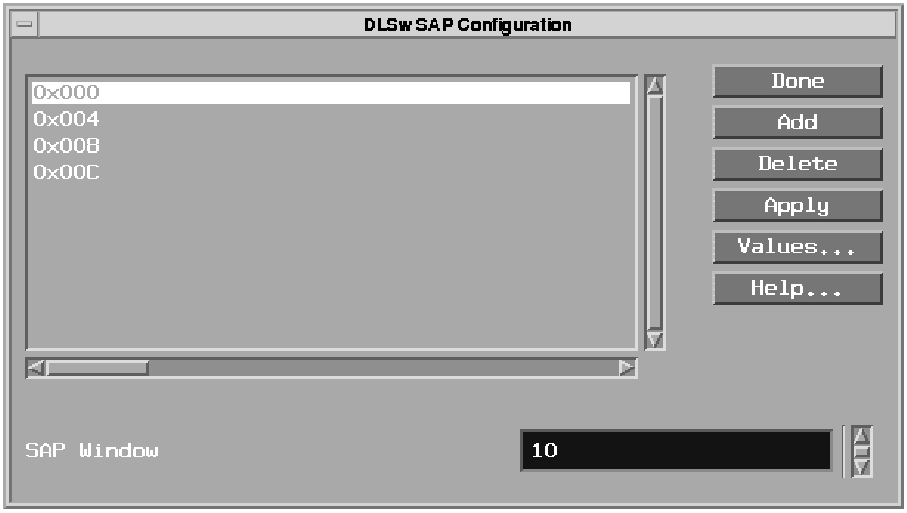
Editing DLSw SAP Table Parameters

The DLSw SAP Table contains a list of the SAP addresses associated with communication subsystems on PCs, hosts, FEPs, cluster controllers, and other systems in your network. This section describes how to add, edit, and delete DLSw SAPs.

Each SAP Table entry establishes a DLSw SAP address and a SAP window (flow control parameter) value for that SAP. See Chapter 3 for more information about DLSw SAPs.

DLSw SAP Table entries appear in the DLSw SAP Configuration window. When you add DLSw to a router configuration, there are four predefined SAP entries: 00, 04, 08, and 0C (Figure 5-16). If you specified Yes to the DLSw NetBIOS Support parameter, then the SAP F0 also appears in the list.

To access the DLSw SAP Configuration window, begin at the Configuration Manager window (refer to Figure 5-1) and select Protocols > DLSw > SAP Table. The DLSw SAP Configuration window appears (Figure 5-16), listing all SAP addresses that are accessible through DLSw services on the router.



SAP Window 10

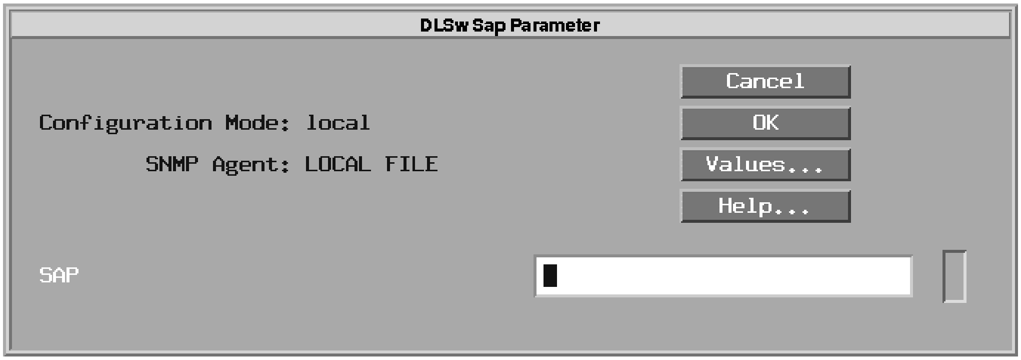
Figure 5-16. SAP Addresses in the DLSw SAP Configuration Window

Adding a DLSw SAP Table Entry

To add a new SAP Table entry, begin at the DLSw SAP Configuration window:

1. **Click on Add.**

   The DLSw SAP Parameter window appears (Figure 5-17).



Configuration Mode: local

SNMP Agent: LOCAL FILE

SAP

Figure 5-17. DLSw SAP Parameter Window

2. **Type the 0x prefix and then enter a hexadecimal value for the SAP parameter.**

   Valid SAP addresses include even values 00, 04 to EC, and F0.

3. **Click on OK.**

   This saves your entry to the router configuration file. The DLSw SAP Configuration window reappears (refer to Figure 5-16) with the new entry added to the list of existing DLSw SAPs.

4. **Repeat Steps 1 through 3 for each SAP that you want to add.**

5. **Click on Done.**

   The Configuration Manager window reappears.

Following is a description of the SAP parameter.

Parameter: **SAP**

Default: None

Options: A valid even SAP address (00 to F0) in hexadecimal format

Function: Specifies the destination SAP address associated with a communication subsystem on a remote device (for example, on a PC or host).

Instructions: Begin the address with 0x and type the SAP address associated with a specific communication subsystem. For example, the SAP associated with NetBIOS is 0xF0.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.4.1.2

Editing a DLSw SAP Table Entry

You can edit only the SAP Window (flow control) parameter associated with an existing DLSw SAP Table entry.

> **Note:** After you add an entry to the DLSw SAP Table, Site Manager disallows any attempt to edit the SAP address associated with that entry. To change the address of an existing DLSw SAP, you must delete the entry in the DLSw SAP Configuration window, and then add a new SAP with the new address. Refer to the preceding section, “Adding a DLSw SAP Table Entry,” for information about how to add a new DLSw SAP.

To edit the SAP Window parameter associated with a particular DLSw SAP, begin at the Configuration Manager window (refer to Figure 5-1):

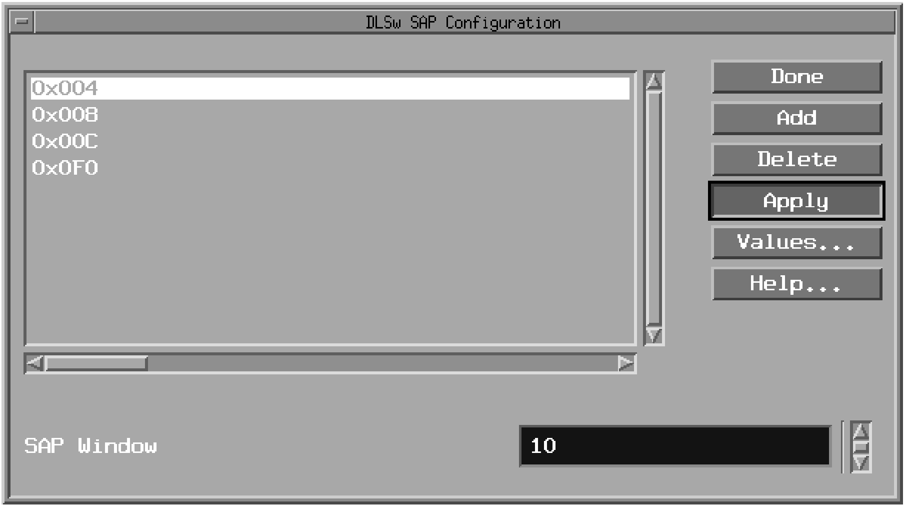
1. **Select Protocols > DLSw > SAP Table.**

   The DLSw SAP Configuration window appears (Figure 5-18).

2. **Select the DLSw SAP Table entry to edit.**

3. **Click on the SAP Window parameter box and enter a new value.**

4. **Click on Apply to save.**



0x004
0x008
0x00C
0x0F0

SAP Window 10

Figure 5-18. Saving the Edited SAP Window Setting

5. **Click on Done.**

   You return to the Configuration Manager window.

Following is a description of the SAP Window parameter.

Parameter: **SAP Window**

Default: 10

Range: 6 to 200

Function: Specifies the maximum number of unacknowledged LLC2 frames that the local endstation DLSw switch accepts for forwarding to the remote endstation. See the section “Flow Control” in Chapter 2 for more information.

Instructions: Enter a SAP window size that is appropriate for your network configuration and requirements. Specifying a larger size dedicates more buffer space to a particular SAP, thereby improving performance on that SAP. Specifying a smaller window size reduces buffer size and decreases performance on that SAP.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.4.1.3

Note: The default value of 10 frames is based on the commonly used value of 7 plus additional frames to accommodate possible differences in timing between the router and the endstations.

Deleting a DLSw SAP Table Entry

To delete a SAP table entry, begin at the Configuration Manager window (refer to Figure 5-1):

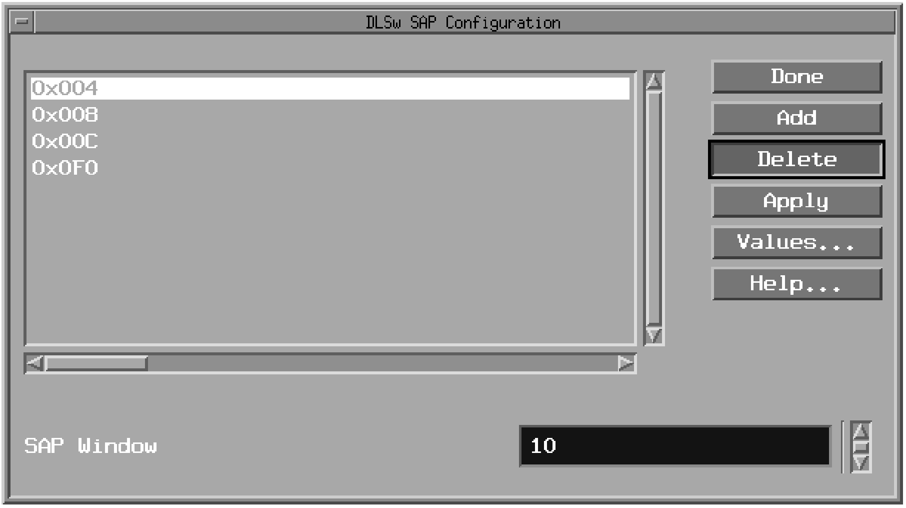
1. **Select Protocols > DLSw > SAP Table.**

   The DLSw SAP Configuration window opens (Figure 5-19).

2. **Select the SAP Table entry to delete.**

3. **Click on Delete.**

   The system software deletes the entry you selected, and removes the entry from the DLSw SAP Configuration window.



DLSw SAP Configuration

0x004
0x008
0x00C
0x0F0

SAP Window: 10

Figure 5-19. Deleting a SAP Table Entry

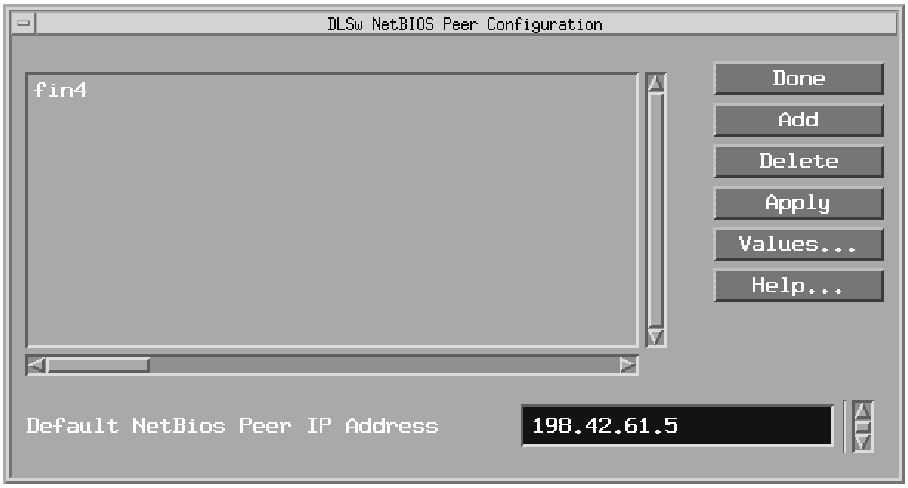
4. **Click on Done.**

   This completes the deletion procedure and returns you to the Configuration Manager window.

Editing DLSw Default NetBIOS Peer IP Table Parameters

The Default NetBIOS Peer IP Table contains the list of all remote NetBIOS systems and applications that you can access via DLSw connection services on the local router. Each entry that you define in the Default NetBIOS Peer IP Table associates the name of a NetBIOS client or server with the IP address of the remote DLSw peer that can reach that client or server. You add, edit, and delete Default NetBIOS Peer IP Table entries in the DLSw NetBIOS Peer Configuration window.

To access the DLSw NetBIOS Peer Configuration window, begin at the Configuration Manager window and select Protocols > DLSw > Default NetBIOS. The DLSw NetBIOS Peer Configuration window appears (Figure 5-20), showing a list of NetBIOS client and server names.



fin4

Default NetBios Peer IP Address 198.42.61.5

Figure 5-20. DLSw NetBIOS Peer Configuration Window

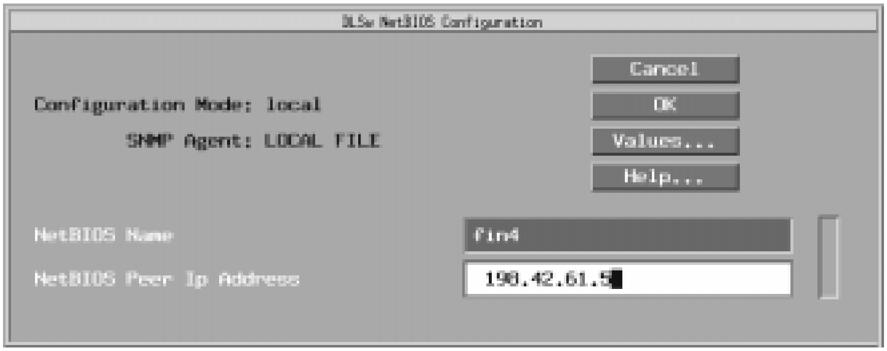
Clicking on a name in the list window causes the DLSw Peer IP address associated with that name to appear in the Default NetBIOS Peer IP Address parameter field (Figure 5-20).

Adding a DLSw Default NetBIOS Peer IP Table Entry

To add a DLSw Default NetBIOS Peer IP Table entry, from the DLSw NetBIOS Peer Configuration window (refer to Figure 5-20):

1. **Click on Add.**

   The DLSw NetBIOS Configuration window appears (Figure 5-21).



DLSw NetBIOS Configuration

Configuration Mode: local

SNMP Agent: LOCAL FILE

NetBIOS Name: fin4

NetBIOS Peer Ip Address: 198.42.61.5

Figure 5-21. DLSw NetBIOS Configuration Window

2. **Type the name of the remote NetBIOS client or server.**

   This is the client or server that you want to reach via DLSw services.

3. **Type the IP address of the remote DLSw peer.**

   This is the IP address of the DLSw peer that can reach the NetBIOS client or server you identified with the NetBIOS Name parameter.

4. **Click on OK.**

   This saves your entry to the router configuration file.

   The DLSw NetBIOS Peer Configuration window reappears with the new entry in the list of existing NetBIOS peers (refer to Figure 5-20).

Following are descriptions of the NetBIOS Name and NetBIOS Peer IP Address parameters.

Parameter: **NetBIOS Name**

Default: None

Options: Any valid NetBIOS name

Function: Specifies the name of the remote NetBIOS client/server or application that you want to reach via DLSw services.

Instructions: Enter the name of the remote NetBIOS client or server station or application that you want to reach via DLSw services.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.11.1.2

Parameter: **NetBIOS Peer IP Address**

Default: None

Options: Any valid, 32-bit IP address in the form *network.host* (using dotted-decimal notation)

Function: Specifies the IP address of the DLSw peer that can reach the remote NetBIOS client/server or application named in the same DLSw Default NetBIOS Peer IP Table entry.

Instructions: Enter the IP address of the DLSw peer that can reach the remote client or server station or application named in the same DLSw Default NetBIOS Peer IP Table entry. The router adds this IP address to the list of configured peers in the local DLSw Peer IP Table.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.11.1.3

Editing a DLSw Default NetBIOS Peer IP Table Entry

You can edit only the Default NetBIOS Peer IP Address parameter in a Default NetBIOS Peer IP Table entry. To edit the parameter, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols > DLSw > Default NetBIOS.**

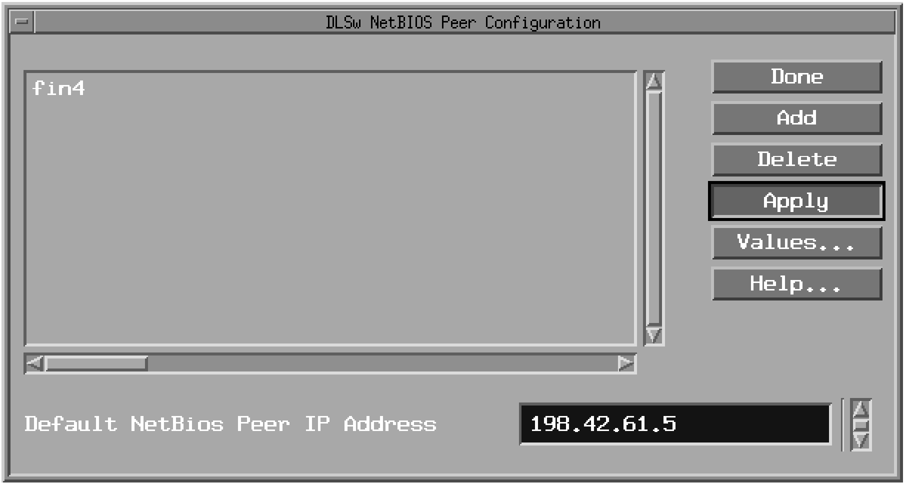
   The DLSw NetBIOS Peer Configuration window appears (Figure 5-22).

2. **Select the DLSw Default NetBIOS Peer IP Table entry to edit.**

3. **Click on the Default NetBIOS Peer IP Address parameter and enter a new address.**

4. **Click on Apply.**

   This saves your change to the router configuration file.



Default NetBios Peer IP Address 198.42.61.5

Figure 5-22. Saving a DLSw Default NetBIOS Peer IP Table Entry

5. **Click on Done.**

   You return to the Configuration Manager window.

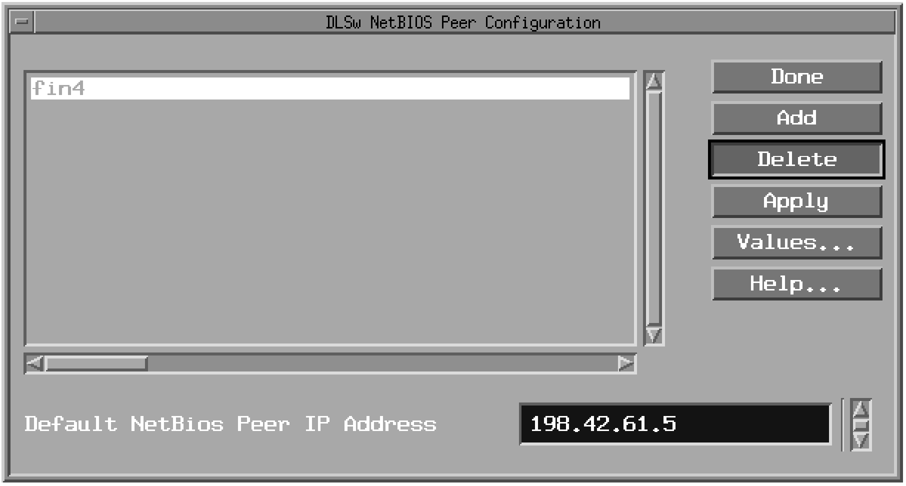
Following is a description of the Default NetBIOS Peer IP Address parameter.

Parameter:	**Default NetBIOS Peer IP Address**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* (using dotted-decimal notation)
Function:	Specifies the IP address of the remote DLSw peer that can reach the NetBIOS client/server system or application currently selected in the DLSw NetBIOS Peer Configuration window.
Instructions:	Type the IP address of the DLSw peer that can reach the remote client/server or application currently selected in the DLSw NetBIOS Peer Configuration window. The router adds this IP address to the list of configured peers in the local DLSw Peer IP Table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.11.1.3

Deleting a DLSw Default NetBIOS Peer IP Table Entry

To delete a DLSw Default NetBIOS Peer IP Table entry from the router configuration, start at the DLSw NetBIOS Peer Configuration window (Figure 5-23):

1. **Select the table entry to delete.**


DLSw NetBIOS Peer Configuration

fin4

Default NetBios Peer IP Address 198.42.61.5

Figure 5-23. Deleting a DLSw Default NetBIOS Peer IP Table Entry

2. **Click on Delete.**

   The system deletes the entry you selected, and removes the entry from the list.

3. **Click on Done.**

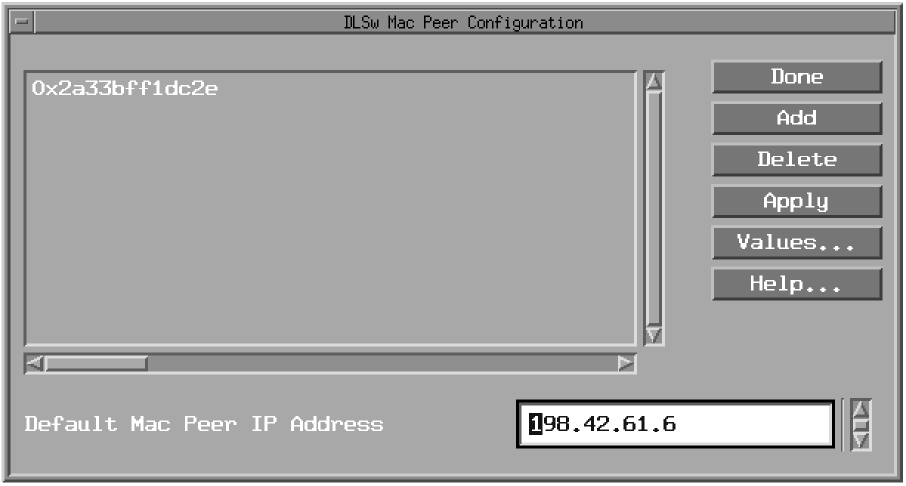
   You return to the Configuration Manager window.

Editing DLSw Default MAC Peer IP Table Parameters

The DLSw Default MAC Peer IP Table contains the list of all remote SNA systems and applications that you can access via DLSw connection services on the local router. Each entry you define in the DLSw Default MAC Peer IP Table contains the IP address of a remote DLSw peer that can reach a target SNA system or application. The target system or application has an associated Token Ring/ 802.5 MAC address, which you also specify in the DLSw Default MAC Peer IP Table entry. You add, edit, and delete DLSw Default MAC Peer IP Table entries in the DLSw MAC Peer Configuration window.

To access the DLSw MAC Peer Configuration window, begin at the Configuration Manager window (refer to Figure 5-1) and select Protocols > DLSw > Default MAC.

The DLSw MAC Peer Configuration window appears (Figure 5-24), showing a list of Token Ring/802.5 MAC addresses associated with frequently accessed, remote SNA systems and applications.



0x2a33bff1dc2e

Default Mac Peer IP Address 198.42.61.6

Figure 5-24. DLSw MAC Peer Configuration Window

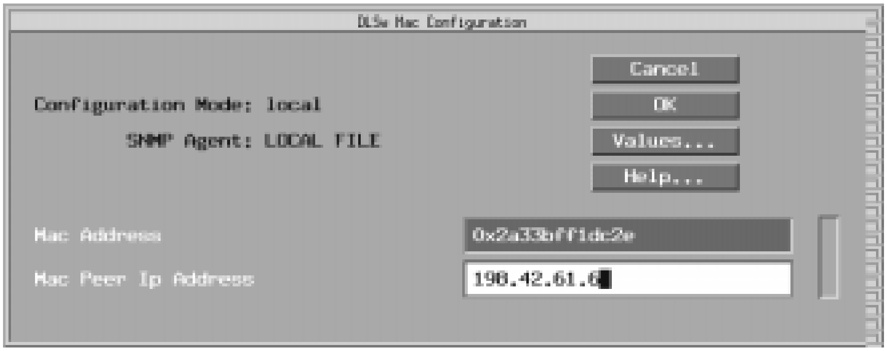
Each entry in the list is associated with the IP address of the remote DLSw peer that can reach the target SNA system or application. The IP address of the currently selected table entry appears in the Default MAC Peer IP Address parameter box.

Adding a DLSw Default MAC Peer IP Table Entry

To add a new DLSw Default MAC Peer IP Table entry, begin at the DLSw MAC Peer Configuration window and:

1. **Click on Add.**

   The DLSw MAC Configuration window appears (Figure 5-25).



DLSw Mac Configuration

Configuration Mode: local

SNMP Agent: LOCAL FILE

Mac Address 0x2a33bff1dc2e

Mac Peer Ip Address 198.42.61.6

Figure 5-25. MAC Addresses in the DLSw MAC Configuration Window

2. **Type the Token Ring/802.5 MAC address.**

   This is the address associated with the SNA system or application that you want to reach via DLSw services.

3. **Type the IP address of the DLSw peer.**

   This is the IP address of the DLSw peer that can reach the SNA system or application that you identified in the MAC Address parameter box.

4. **Click on OK.**

   This saves your entry to the configuration file.

   The DLSw MAC Peer Configuration window reappears with the new entry in the list of existing DLSw MAC peers (refer to Figure 5-24).

Following are descriptions of the MAC Address and MAC Peer IP Address parameters.

Parameter: **MAC Address**

Default: None

Options: Any valid, 48-bit MAC address expressed in hexadecimal notation

Function: Specifies the MAC address associated with the SNA system or application that you want to reach via DLSw services.

Instructions: Type in hexadecimal format the MAC address associated with the remote SNA system or application that you want to reach via DLSw services.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.10.1.2

Parameter: **MAC Peer IP Address**

Default: None

Options: Any valid, 32-bit IP address in the form *network.host* (using dotted-decimal notation)

Function: Specifies the IP address of a remote DLSw peer that can reach the remote SNA system or application identified by the MAC address in the same Default MAC Peer IP Table entry. The router adds this IP address to the list of configured peers in the DLSw Peer IP Table.

Instructions: Type the IP address of the remote DLSw peer that can reach the remote SNA system or application identified by the MAC address in the same Default MAC Peer IP table entry.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.10.1.3

Editing a DLSw Default MAC Peer IP Table Entry

You can edit only the Default MAC Peer IP Address parameter in the Default MAC Peer IP Table. To edit the DLSw MAC Peer IP Address, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols > DLSw > Default MAC.**

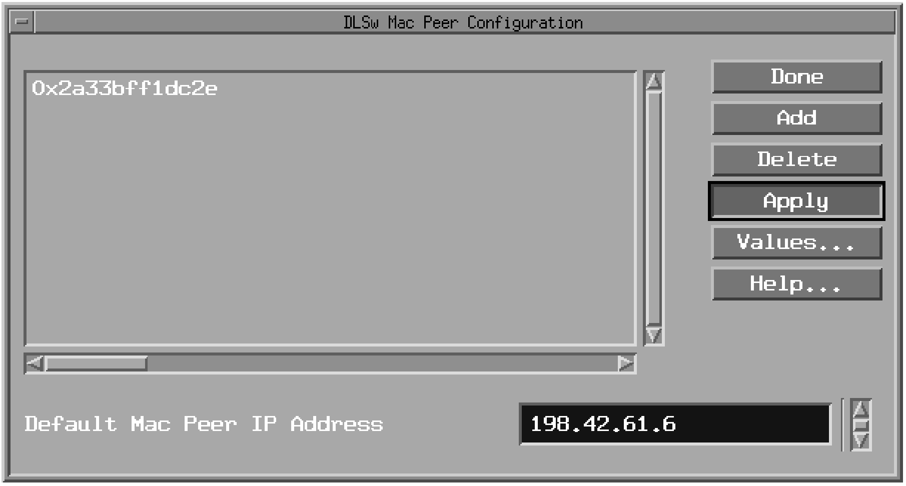
   The DLSw MAC Peer Configuration window appears (Figure 5-26).

2. **Select the entry to edit.**

3. **Click on the Default MAC Peer IP Address parameter field and enter a new address.**

4. **Click on Apply.**

   This saves your change to the router configuration file.



DLSw Mac Peer Configuration

0x2a33bff1dc2e

Default Mac Peer IP Address 198.42.61.6

Figure 5-26. Saving a DLSw Default MAC Peer IP Table Entry

5. **Click on Done.**

   The Configuration Manager window reappears.

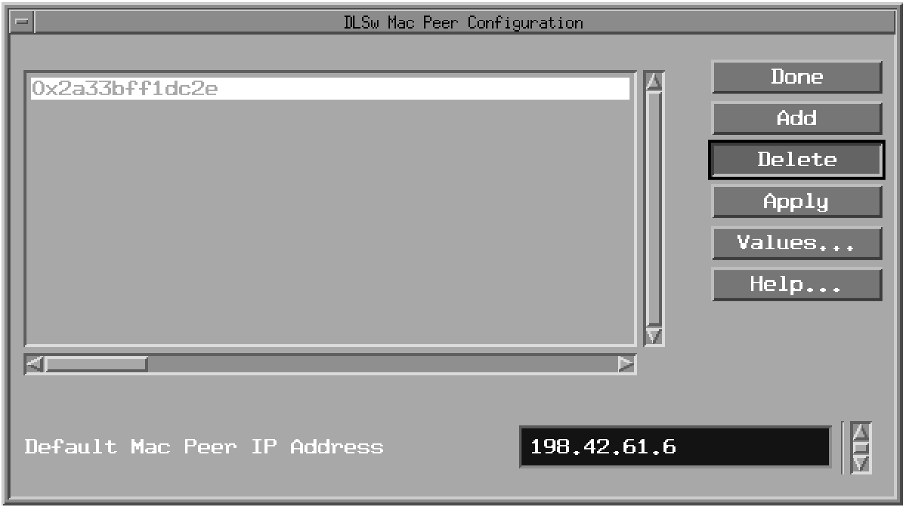
Following is a description of the Default MAC Peer IP Address parameter.

Parameter:	**Default MAC Peer IP Address**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* (using dotted-decimal notation)
Function:	Specifies the IP address of a remote DLSw peer that can reach the SNA system or application identified by the MAC address and currently selected in the DLSw MAC Peer Configuration window. The router adds this IP address to the list of configured peers in the DLSw Peer IP Table.
Instructions:	Type the IP address of the remote DLSw peer that can reach the remote SNA system or application identified by the MAC address and currently selected in the DLSw MAC Peer Configuration window.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.10.1.3

Deleting a DLSw Default MAC Peer IP Table Entry

To delete a DLSw Default MAC Peer IP Table entry from the router configuration, start at the DLSw MAC Peer Configuration window (Figure 5-27):

1. **Select the entry to delete.**
2. **Click on Delete.**



0x2a33bff1dc2e

Default Mac Peer IP Address 198.42.61.6

Figure 5-27. Deleting a DLSw Default MAC Peer IP Table Entry

The system software deletes the entry you select, and removes the entry from the list.

3. **Click on Done.**

   The Configuration Manager window reappears.

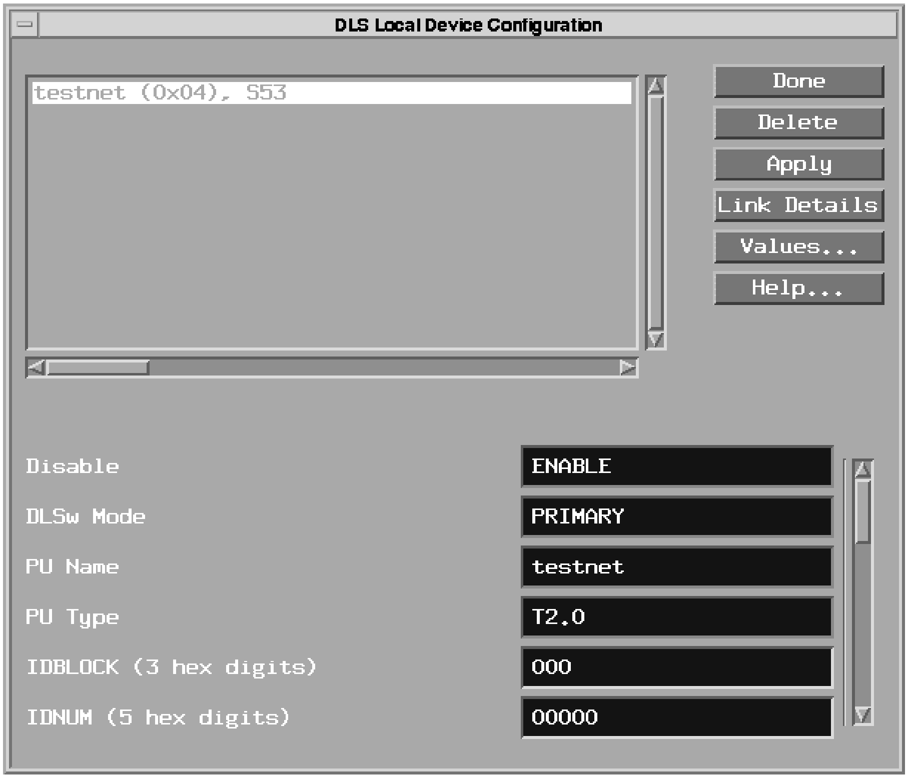
Editing DLSw Local Devices Parameters

DLSw Local Devices parameters let you map SDLC devices to LAN MAC and SAP addresses. This section assumes that you have already added local devices. (Chapter 3 describes the different ways that you can add local devices.) Read this section if you want to edit the local device configurations.

To access DLSw Local Devices parameters, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols > DLSw > Local Devices.**

   The DLS Local Device Configuration window appears (Figure 5-28).



testnet (0x04), S53

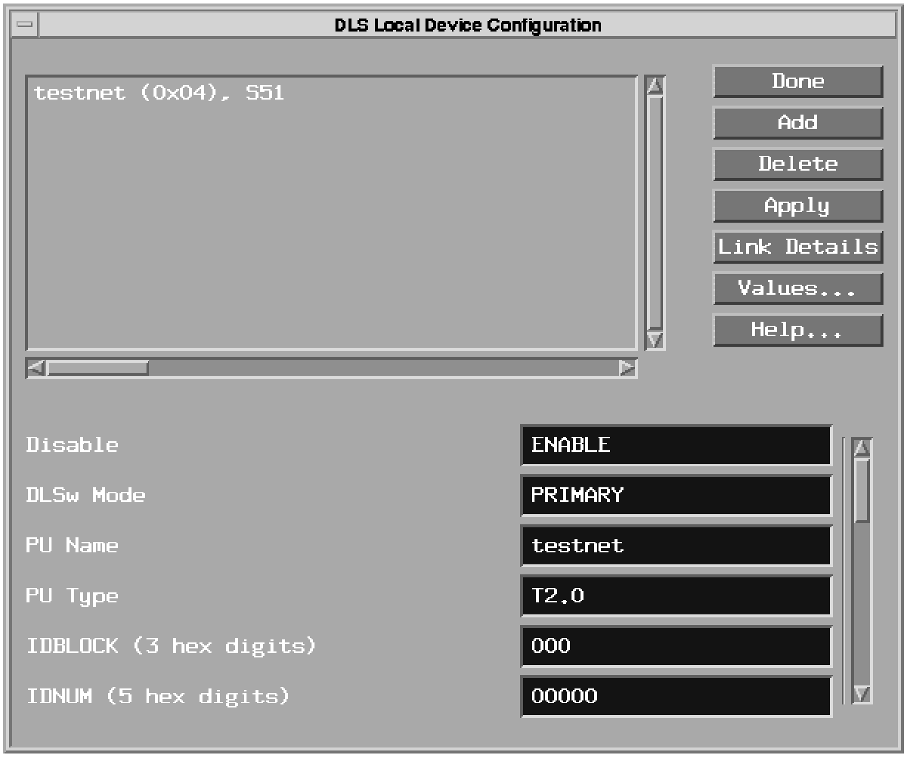
Disable ENABLE
DLSw Mode PRIMARY
PU Name testnet
PU Type T2.0
IDBLOCK (3 hex digits) 000
IDNUM (5 hex digits) 00000

Figure 5-28. DLS Local Device Configuration Window

2. **Click on the local device whose parameters you want to change.**
3. **Edit the appropriate parameters.**

   For information, see the next section, “DLSw Local Devices Parameter Descriptions.”
4. **Click on Apply to save your changes.**
5. **Proceed as follows:**
   - To edit the parameters of another local device, select that device and repeat Steps 2 and 3.
   - Select Link Details to display the SDLC Link Station Configuration window. Refer to *Configuring SDLC Services* for information about the parameters in this window.

- To add a local device, start at the Configuration Manager window and select the connector to which you are adding a local device. Select Edit Circuit, and then select Protocols > DLSw > Local Devices. The DLS Local Device Configuration window (Figure 5-29) appears with the Add button.



DLS Local Device Configuration

testnet (0x04), S51

Disable ENABLE

DLSw Mode PRIMARY

PU Name testnet

PU Type T2.0

IDBLOCK (3 hex digits) 000

IDNUM (5 hex digits) 00000

Figure 5-29. DLS Local Device Configuration Add Window

- If you are finished working with the local device parameters, click on Done to return to the Configuration Manager window.

DLSw Local Devices Parameter Descriptions

This section describes the DLSw Local Devices parameters that you can customize from the DLS Local Device Configuration window.

Parameter: **Link Station Address (hex)**

Default: None

Range: Any valid hexadecimal link station address from 0x01 to 0xFE

Function: Specifies the address of the link station. This parameter must match the polling address defined in the SDLC-attached device.

Instructions: Type 0x followed by the link station address.

MIB Object ID: N/A

Parameter: **Disable**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the DLSw local device.

Instructions: Set to Disable if you want to temporarily disable the local device, rather than delete it. Set to Enable if you want to reinitialize the local device.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.2

Parameter: **DLSw Mode**

Default: Primary

Options: Primary | Secondary PP | Secondary MP

Function: Specifies the type of link station that you are configuring on this node. A primary link station controls a data link, issues commands, polls secondary stations, and initiates error recovery procedures. Only one link station on an SDLC line can be the primary station; all other stations on the line must be secondary. When configured as a primary SDLC link station, the router communicates with downstream PU 2.0 and PU 2.1 nodes

A secondary link station receives commands and responds to primary link station polls. When configured as a secondary SDLC link station, the router emulates a PU 2.0 device.

Instructions: Click on Values and select Primary, Secondary PP, or Secondary MP.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.2.1.8

Parameter: **PU Name**

Default: None

Options: Any valid, 8-byte ASCII name

Function: Specifies the name of the adjacent link station. This name uniquely identifies the station for statistics and Alert messages.

Instructions: Type the 8-byte ASCII link station name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.7.5.1.32

Parameter: **PU Type**

Default: None

Options: T1.0 | T2.0 | T2.1

Function: Specifies the type of the XID-sending node. This parameter is used with the IDBLOCK, IDNUM, and XID Format parameters to determine the station XID value.

Instructions: Choose T1.0, T2.0, or T2.1.

MIB Object ID: N/A

Parameter: **IDBLOCK**

Default: None

Options: Any 3-digit hexadecimal value

Function: Specifies the block number, which must match the host's IDBLOCK parameter value that identifies incoming connection requests. This parameter is used with the PU Type, IDNUM, and XID Format parameters to determine the station XID value. Table 5-2 lists the IDBLOCK numbers.

Instructions: Obtain the configured value at the host (from VTAM or other host operating system) for this device.

MIB Object ID: N/A

Table 5-2. IDBLOCK Numbers for Switched PUs

Device	IDBLOCK Number
NPSI	003
3770	004
3650/3680	005
6100/3790	006
NTO, 3767	007
S/34	00E
3774	011
3x74	017
3276	018
8775	019
S/1	021
S/38	022
5520	031
5280	032
PC/SRJE	03D
S/36	03E
4680	04D

(continued)

Table 5-2. IDBLOCK Numbers for Switched PUs *(continued)*

Device	IDBLOCK Number
APPC/PC	050
AS/400	056
6150	05C
OS/2 EE	05D
WSP	05E
PC/3270	061
RS/6000	071
Subarea	FFF

Parameter: IDNUM

Default: None

Options: Any 5-digit hexadecimal value from 00000 to FFFFF (for T1.0 or T2.0 nodes)

Function: Specifies the ID number, which must match the host's IDNUM parameter value that identifies incoming connection requests. This parameter is used with the PU Type, IDBLOCK, and XID Format parameters to determine the station XID value.

Instructions: Obtain the configured value at the host (from VTAM or other host operating system) for this device. Type a 5-digit hexadecimal value from 00000 to FFFFF for T1.0 or T2.0 nodes.

MIB Object ID: N/A

Parameter: **XID Format**

Default: None

Options: FIXED | VARIABLE1 | VARIABLE2

Function: Specifies the format of the XID I-field. This parameter is typically set to FIXED for PU 2.0 devices, VARIABLE 1 for PU 1.0 devices, and set to VARIABLE2 for PU 2.1 devices.

Instructions: Click on Values and select one of the following options:

- FIXED -- Fixed format; most often used for PU 2.0 devices
- VARIABLE1 -- Variable format (for T1.0/T2.0/T2.1 to T4/T5 node exchanges), mostly used for PU 1.0 devices
- VARIABLE2 -- Variable format; most often used for PU 2.1 devices (for T2.1 to T2.1/T4/T5 node exchanges)

MIB Object ID: N/A

Parameter: **Source (Virtual) MAC (hex)**

Default: None

Options: Any standard MSB Token Ring MAC address

Function: Specifies the source MAC address of an emulated Token Ring endstation for this device.

Instructions: Type the 12-digit hexadecimal source MAC address that you want to assign to the SDLC device. The address should be in MSB format, and it should be unique in the network, even among other source addresses on the router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.6

Parameter: **Source (Virtual) SAP (hex)**

Default: 0x4

Range: 0x01 to 0xFE

Function: Specifies the source SAP of an emulated Token Ring or Ethernet endstation for this device.

Instructions: Begin the address with 0x and type a 1-digit or 2-digit hexadecimal source SAP address associated with this device. Typical values are multiples of 4.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.7

Parameter: **Destination MAC (hex)**

Default: None

Options: Any standard MSB Token Ring MAC address

Function: Identifies (with the Destination SAP) the Token Ring or Ethernet host that the local device will reach via SDLC services.

Instructions: Consult your host system manager for the host MAC address; then type the 12-digit hexadecimal address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.8

Parameter: **Destination SAP (hex)**

Default: 0x4

Range: 0x01 to 0xFE

Function: Identifies (with the Destination MAC) the Token Ring or Ethernet host that the local device will reach via SDLC services.

Instructions: Consult your host system manager for the host SAP address. Type 0x followed by a 1-digit or 2-digit hexadecimal address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.9

Parameter:	**MAXOUT**
Default:	7
Range:	1 to 127
Function:	Controls the maximum number of consecutive frames that an SDLC link station can send without acknowledgment.
Instructions:	Type a value from 1 to 127.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.7.5.1.10

Parameter:	**MAXDATA**
Default:	2057
Options:	265 | 521 | 1033 | 2057
Function:	Specifies the maximum frame size that SDLC supports. This value includes the transmission header (TH) and request header (RH).
Instructions:	Enter a maximum frame size that is equal to or larger than the largest frame size that will be received.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.7.5.1.7

Parameter:	**Canureach Timer (sec)**
Default:	30
Range:	0 to 3600
Function:	Specifies the time interval (in seconds) after which the router sends a CANUREACH message to the remote DLSw peer to establish a session.
Instructions:	Enter the number of seconds you want for the time interval. For example, type 1 to transmit a CANUREACH message once per second, or type 3600 to transmit the message once per hour. Type 0 if you do not want to transmit a CANUREACH message.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.11

Parameter:	**Canureach Retries**
Default:	4294967295
Range:	0 to 4294967295
Function:	Specifies the number of times a CANUREACH message is initially sent to the remote DLSw peer to establish a session.
Instructions:	Type the number of retries that you want. Type 0 if you do not want to transmit CANUREACH messages. Leave the default value 4294967295 to send an infinite number of CANUREACH messages for this connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.12

Parameter:	**Canureach Timer2 (sec)**
Default:	30
Range:	0 to 3600
Function:	Specifies the time interval (in seconds) after which the router sends a canureach message to the remote DLSw peer to establish a session. This parameter setting becomes active when the Canureach Timer and Canureach Retries settings expire. Set the Canureach Timer2 and the Canureach Retries2 parameters in configurations where you want to switch to a longer interval, if the initial connection does not occur within the Canureach Timer and Canureach Retries settings. The slow poll timer would then use the Canureach Timer2 and Canureach Retries2 settings.
Instructions:	Enter the number of seconds that you want for the time interval. For example, enter 1 to transmit a CANUREACH message once per second, or enter 3600 to transmit the command once per hour. Enter 0 if you do not want to transmit a CANUREACH message.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.17

Parameter: **Canureach Retries2**

Default: 0

Range: 0 to 4294967295

Function: Specifies the number of times a CANUREACH message is sent to the remote DLSw peer to establish a session. This parameter setting becomes active when the Canureach Retries setting expires.

Set the Canureach Timer2 and the Canureach Retries2 parameters in configurations where you want to switch to a longer interval if the initial connection does not occur within the Canureach Timer and Canureach Retries settings.

Instructions: Type the number of retries that you want. Enter 0 if you do not want to transmit CANUREACH messages. Type 4294967295 to send an infinite number of CANUREACH messages for this connection.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.18

Parameter: **Link Station Timer (sec)**

Default: 30

Range: 0 to 3600

Function: Sets the time interval (in seconds) after which the router sends a connect request to the local SDLC device to establish a session.

Instructions: Enter the number of seconds that you want for the time interval. For example, type 1 to send a connect request once a second, or type 3600 to send a connect request once an hour. Type 0 if you do not want to send connect requests.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.13

Parameter: **Link Station Retries**

Default: 4294967295

Range: 0 to 4294967295

Function: Specifies the maximum number of times that a connect request is sent to the local SDLC device to establish a session.

Instructions: Enter the number of retries that you want. Type 0 if you do not want to send connect requests. Leave the default value 4294967295 to send an infinite number of connect requests for this connection.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.14

Parameter: **SDLC Receive Credit**

Default: 10

Range: 0 to 200

Function: Specifies the maximum number of frames that SDLC can send to DLSw. This is a flow control parameter.

Instructions: Enter the maximum number of frames that you want SDLC to send to DLSw. For example, type 1 if you want DLSw to accept one frame from SDLC before it updates the SDLC credit. Type 0 if you want DLSw to receive an infinite number of frames from SDLC without updating the SDLC credit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.15

Parameter: **SDLC Transmit Credit**

Default: 10

Range: 0 to 200

Function: Specifies the maximum number of frames that DLSw can send to SDLC.

Instructions: Enter the maximum number of frames that you want DLSw to send to SDLC. For example, type 1 if you want DLSw to send only one frame to SDLC until it receives credit update from SDLC. Type 0 if you want DLSw to send an infinite number of frames to SDLC without updating the SDLC credit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.16

Parameter: **Enable XID PassThru**

Default: Disable

Options: Enable | Disable

Function: Specifies whether XID is to be passed through to SDLC when the host is connected to Token Ring and the remote is SDLC. This parameter is used for PU2.1 circuits.

Instructions: Accept the default, Disable, or change to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.19

Parameter: **Device Activation Seq**

Default: Local Device First

Options: Local Device First | Peer First

Function: Specifies the sequence of activation for SDLC PU2.0 fixed format primary devices. LocalDeviceFirst specifies that DLS establishes a connection with the SDLC End Station first. Once the local device responds successfully, DLS then starts up the SSP connection to the peer. PeerFirst specifies that DLS starts the SSP connection first, and contacts the SDLC End Station only after receiving a CONTACT message from the peer.

Instructions: Accept the default, Local Device First, or change to Peer First.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.12.1.12

Deleting a DLSw Local Device Entry

To delete a DLSw Local Device entry from the router configuration, start at the DLS Local Device Configuration window (refer to Figure 5-28):

1. **Select the DLSw local device to delete.**
2. **Click on Delete.**

Editing a DLSw IP Multicast Entry

To edit a DLSw IP multicast entry, begin at the Configuration Manager window:

1. **Select Protocols > DLSw > Multicast IP Table > Multicast IP Table.**

The DLSw Multicast Configuration window opens.

2. **Select the IP multicast entry you want to edit.**
3. **Edit the parameters for the selected entry, using the descriptions below. If you want to enable the backup feature, select Yes for the Backup Config parameter.**
4. **Click on Done.**

   The first DLSw Multicast Configuration window reopens.

To add more multicast entries, from the DLSw Multicast Configuration window:

5. **Click on Add.**

   A second DLSw Multicast Configuration window opens.

6. **Supply an IP multicast group address and associate the address with a slot or slots. Click on OK.**

   The first DLSw Multicast Configuration window reopens.

7. **Edit the parameters, using the descriptions below. If you want to enable the backup feature, select Yes for the Backup Config parameter.**
8. **Click on Done.**

   The Configuration Manager window opens.

Following are descriptions of the DLSw multicast configuration parameters.

Parameter:	**Multicast IP Address**
Default:	224.0.10.0
Options:	Any valid IP address specified in dotted-decimal notation. The valid range is 224.0.1.0 through 239.255.255.255.
Function:	Specifies the multicast IP address of this entry.
Instructions:	Enter the appropriate IP address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.15.1.3

Parameter: **Slot**

Default: Depends on the number of slots in the router. For a BLN, the default is 00000.

Options: Depends on the number of slots in the router

Function: Specifies the slots that you want to receive and transmit multicast data.

Instructions: Click on the Values button. Select the slots that you want to receive and transmit multicast data. For example, if you select Slots 2 and 3 in a BLN, then the value in the Slot field appears as 01100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.4

Parameter: **Multicast IP Slots**

Default: The value or values you selected for the Slot parameter

Options: Depends on the number of slots in the router

Function: Specifies the slots that you want to receive and transmit multicast data.

Instructions: Accept the value you entered at the Slot parameter on the second DLSw Multicast Configuration window, or click on the Values button and select different slots.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.4

Parameter: **Backup Config**

Default: No

Options: Yes | No

Function: Enables the parameters that allow you to configure a backup peer.

Instructions: Accept the default, No, or click on the Values button and select Yes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.5

Parameter: **Backup IP Address**

Default: 0.0.0.0

Options: Any valid, 32-bit IP address of the form *network.host* (using dotted-decimal notation)

Function: Specifies the IP address of a backup DLSw peer and adds the peer to the DLSw Backup Peer IP Table. A backup peer receives all DLSw-related broadcast frames for a given router or network processor if the primary peer router is unavailable or cannot be reached over a TCP connection.

Instructions: Enter the IP address of the backup peer.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.6

Parameter: **Backup Peer Type**

Default: V20 (Unicast-Unknown)

Options: RFC 1795 | V20 (Unicast-TCP) | V20 (Unicast-Unknown) |
V20 (Unicast-UDP) | RFC 2166 (Multicast)

Function: Specifies the type of this DLSw backup peer.

Instructions: Accept the default, V20 (Unicast-Unknown) or click on the Values button and specify a different type.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.11

Parameter: **Backup Max Up Time**

Default: 0

Options: 0 to 999999

Function: Specifies the maximum time (in seconds) that the backup peer can remain connected to the local DLSw peer. When the maximum time is reached, the software terminates the TCP connection if there are no active TCP sessions between the routers. The software overrides the Backup Max Up Time parameter setting only if there is an active (non-idle) TCP connection with data transferring between the routers.

Instructions: Type a value in the range 0 to 999999. Specify 0 to disable the Backup Max Up Time parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.7

Parameter: **Backup Hold Down Time (sec)**

Default: 120

Options: 0 to 2147483647

Function: Specifies the time to wait (in seconds) after the primary peer is declared unreachable before the local router initiates a TCP connection to the backup peer. The hold down time ensures that the primary peer has enough time to respond to a TCP connection request before the local router initiates a TCP connection to the backup peer.

Instructions: Accept the default, 120, or click on the Values button and specify a different value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.8

Parameter: **Backup Start Time (hhmm)**

Default: 1

Options: 0 to 2400

Function: Specifies the start time when a configured backup peer is available. During this time period, the local router can establish a TCP connection with this backup peer if the primary peer is unreachable.

Instructions: Type the start time in *hhmm* format, where *hh* is hours and *mm* is minutes. For example, typing 0820 specifies 8:20 a.m., and 2400 specifies 12:00 midnight. Type 0 to disable the Backup Start Time parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.15.1.9

Parameter:	**Backup End Time (hhmm)**
Default:	2400
Options:	1 to 2400
Function:	Specifies the end time when a configured backup peer is available. During this time period, the local router can establish a TCP connection with this backup peer if the primary peer is unreachable.
Instructions:	Type the end time in *hhmm* format, where *hh* is hours and *mm* is minutes. For example, typing 0820 specifies 8:20 a.m., and 2400 specifies 12:00 midnight. The Backup End Time parameter is disabled if the Backup Start Time is set to 0.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.15.1.10

Editing DLSw Traffic Filters and Protocol Prioritization

For information about how to access and configure traffic filters and protocol prioritization for DLSw services, refer to Chapter 6.

Deleting DLSw from a Node

You can delete DLSw from a node entirely.

To delete DLSw, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols > DLSw > Delete DLS.**

   A confirmation window appears.

2. **Click on OK.**

   The Configuration Manager window appears.

DLSw is no longer configured on the router.

Chapter 6
Using DLSw Prioritization

This chapter provides guidelines for implementing DLSw TCP-level prioritization. Following an overview of DLSw protocol prioritization, later sections describe how to use Configuration Manager when:

- Configuring Default Priority Queues
- Configuring Peer-Specific Priority Queues
- Creating DLSw Priority Filters

Note: This chapter assumes that DLSw is already configured on an interface and that the Peer Table is complete. For information about configuring a circuit with DLSw and setting the slot, peer, and SAP parameters, refer to the earlier chapters in this manual.

Protocol Prioritization Overview

Outbound traffic filters act on packets that the router sends on a synchronous interface to a wide area network. Outbound traffic filter actions let you direct traffic into delivery queues of varying precedence. Applying a priority queue action to an outbound filter is called *protocol prioritization*. These outbound filters are often called *priority filters*.

As a router operates, network traffic from a variety of sources converges at an interface. Without protocol prioritization, the router transmits packets in a first in first out (FIFO) order. Site Manager’s protocol prioritization features allow you to instruct the router to use a different transmit order for specified ranges of packets on an individual interface.

With protocol prioritization, the router sorts traffic into queues according to priority filters that you configure. For most traffic, you configure priority filters on an outbound interface. If a queue is full or you have configured an outbound drop filter, the router discards (*clips*) the traffic. For DLSw traffic you can also create priority queues for DLSw peers; the router cannot clip DLSw traffic.

The router holds the sorted packets in priority queues. It then uses a dequeuing allocation algorithm to drain the queues and transmit traffic.

Priority queues do not affect traffic as it is entering the router, but rather affect the sequence in which data leaves an interface. For this reason, protocol prioritization is considered an outbound filter mechanism.

Types of Protocol Prioritization

There are two separate implementations of protocol priority queuing. For all synchronous protocols that support outbound traffic filters, Bay Networks supports a high, normal, and low priority queue at the circuit interface level. For inbound and outbound DLSw traffic, Bay Networks also supports one to ten queues at the TCP level for DLSw peers.

Using existing protocol prioritization support, you can prioritize DLSw traffic before other protocols. DLSw protocol prioritization gives preference to specific types of DLSw traffic, such as:

- Ethernet
- Frame Relay
- SDLC
- Token Ring
- Other SRB traffic

➡ **Note:** You can apply both circuit-level and TCP-level prioritization to DLSw traffic. Note that TCP-level prioritization alone does not give DLSw traffic precedence over other routing protocols. For information about circuit-level prioritization, refer to *Configuring Traffic Filters and Protocol Prioritization*.

DLSw Priority Queues

This section describes how DLSw protocol prioritization works, and defines DLSw terms.

Although similar to the existing circuit-level protocol prioritization, DLSw prioritization is not limited to synchronous interfaces and does not operate at the driver level. DLSw prioritization occurs before TCP sequences packets, where the data link control (LLC2 or SDLC) and TCP function.

The router sorts packets into priority queues as described later in “The Enqueuing Process.” The router then drains (*dequeues*) the priority queues to transmit packets according to a weighted allocation algorithm, described later in “The Dequeuing Process.”

Based on the needs of your site, you can configure up to ten queues for each DLSw peer. You can create queues for traffic with specific MAC or SAP address ranges or, for SNA traffic, based on criteria in the SNA transmission header (FID2 and FID4). You determine whether a queue applies to all DLSw peers or to one or more specific configured peers.

Default and Peer-Specific DLSw Queues

To set the way the router handles priority queues for *all* DLSw traffic (including unconfigured peers), you use the default DLSw queue configuration. To customize the handling of queued traffic for a *particular* configured peer, you configure peer-specific priority queues that apply to that peer’s IP address only.

The default priority queue configuration applies to all configured DLSw peers *except* those individual peers for which you configure a custom priority queue. Peer-specific queues take precedence over the default queue.

The Enqueuing Process

The router enqueues packets that match a DLSw priority filter as follows:

1. Applies filter rules
2. Stamps packets with a queue number
3. Places packets in appropriate queues

The router holds packets in the assigned priority queue according to how you configure DLSw protocol prioritization.

Based on the needs of your site, you can configure up to ten queues (Q0 to Q9) for each DLSw peer. For example, you can assign a separate queue for each filter criterion, for specific address ranges, or for particular DLSw peers.

When you enable DLSw protocol prioritization, you distribute the available bandwidth for a configured DLSw peer among its priority queues. The combined bandwidth of each peer's queues totals 100 percent.

By default, there are two DLSw priority queues: Q0 receives 60 percent of the bandwidth and Q1 receives 40 percent.

Nonordered Queues

Although Site Manager numbers the DLSw priority queues, the queue number hierarchy does not determine priority. You configure both the number of queues for each DLSw peer and the percentage of bandwidth assigned to each queue. For example, you can assign 50 percent of available bandwidth to Q3 and 25 percent each to Q1 and Q0.

The Dequeuing Process

The algorithm for DLSw bandwidth allocation is called *weighted dequeuing*. With weighted dequeuing, packets at the front of the protocol prioritization queues enter a *dequeue list* and receive a weighted score. Packets with the lowest score are transmitted first.

By distributing the selection of packets from all queues, weighted dequeuing is more stable than the algorithms used for circuit-level WAN protocol prioritization.

One goal of weighted dequeuing is to send smaller packets ahead of large packets, without violating the bandwidth of each queue or depriving large packets. The algorithm accomplishes this by putting smaller packets ahead of larger packets by simultaneously considering how long the larger packets have been in the dequeue list. A large packet accumulates credit (lowering its weighted score) as each smaller packet gets ahead of it, and eventually the larger packet moves to the front of the dequeue list.

The Dequeue List

Three factors determine a packet's weighted score:

- Size of the packet
- Percent of bandwidth allocated to the packet's queue
- Time spent in the dequeue list

The dequeuing algorithm calculates a packet's dequeue weight using the following formula:

$$\textbf{Weight} = \frac{\textbf{Size of packet}}{\textbf{Bandwidth \%}} - \textbf{Time in dequeue list}$$

Weighted Dequeuing Algorithm

Weighted dequeuing works as follows:

1. Each priority queue enters its first (oldest) entry on a dequeue list.
2. The dequeue list orders the packets according to a weighted score.
3. TCP requests DLSw packets.
4. The router sends the requested number of packets or bytes to TCP from the top of the dequeue list, up to the configured queue limit.
5. TCP transmits the packets.
6. The sequence repeats at Step 1.

Figure 6-1 illustrates weighted dequeuing.

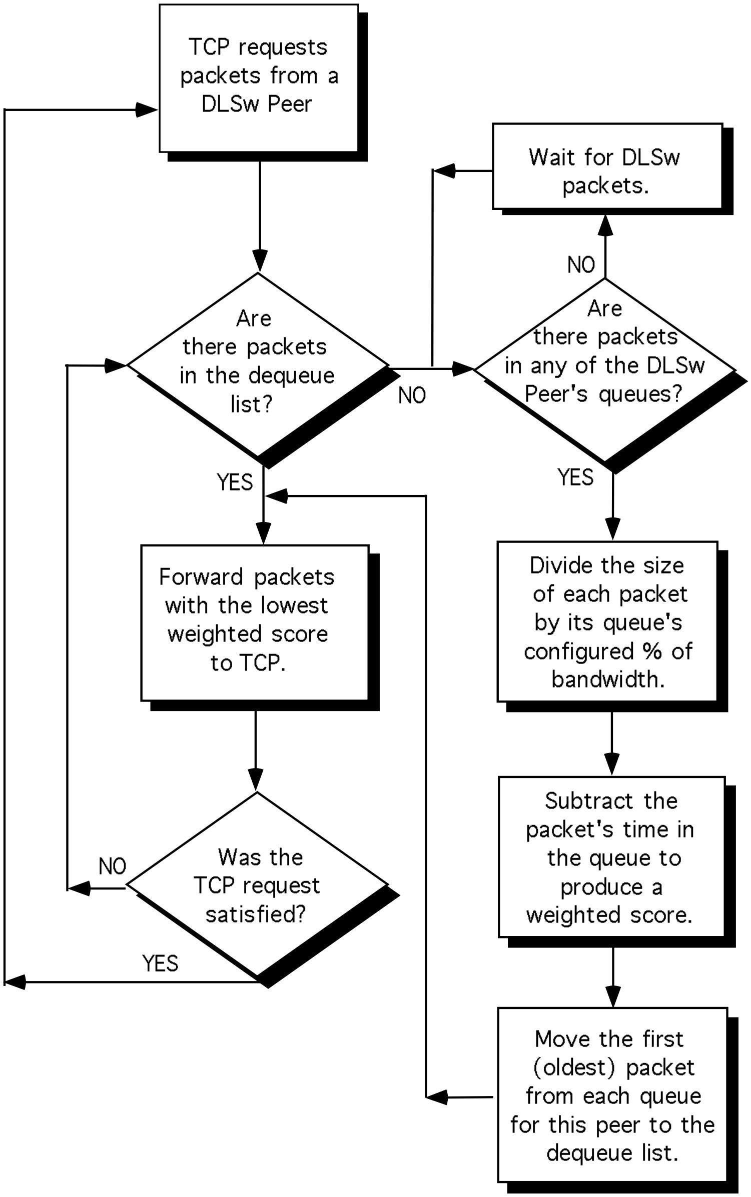

TCP requests packets from a DLSw Peer
Wait for DLSw packets.
NO
Are there packets in the dequeue list?
NO
Are there packets in any of the DLSw Peer's queues?
YES
YES
Forward packets with the lowest weighted score to TCP.
Divide the size of each packet by its queue's configured % of bandwidth.
Subtract the packet's time in the queue to produce a weighted score.
NO
Was the TCP request satisfied?
YES
Move the first (oldest) packet from each queue for this peer to the dequeue list.

Figure 6-1. Weighted Bandwidth Allocation

Tuning DLSw Protocol Prioritization

This section explains how congestion control and queue depth affect DLSw prioritization results for your network. The sections “Customizing the Default Queue Configuration” and “Customizing Specific DLSw Peer Queues,” later in this chapter, show how to use Configuration Manager to configure these values.

DLSw Priority Queues and Congestion Control

Because the router cannot clip DLSw traffic without breaking the DLSw session, DLSw protocol prioritization includes an internal congestion control feature to:

- Temporarily save overflow packets in memory until the appropriate priority queue can handle them
- Notify DLSw to stop and start the flow of packets

There must be sufficient memory available for congestion control to prevent clipping. The less the congestion, the better the queue performance.

Queue Depth

Using Site Manager parameters, you configure the maximum queue buffers and the percentage of bandwidth for each queue.

Queue depth is the configurable number of packets that each DLSw priority queue can hold. The default value is 50 packets, regardless of packet size.

When you set the queue depth, you assign buffers that hold the packets in the DLSw queues. To determine whether there are enough buffers for the DLSw traffic flow on your network, examine the following protocol prioritization statistics that the router keeps for each DLSw priority queue:

- DLSw HiWater Packets Mark -- The greatest number of packets that have been in each queue.
- DLSw Congestion Control Count -- The number of packets that the router has discarded from each queue. The router discards packets from full priority queues.

Generally, if a queue’s Congestion Control Count is high, and its HiWater Packets Mark is close to or equal to its queue depth, you have not assigned enough buffers to that queue.

Configuring Default Priority Queues

You configure the default behavior of DLSw protocol prioritization using the Global DLSw PP Parameters/Defaults window. Use this window to enable, disable, or change the default configuration of priority queues for configured and unconfigured DLSw peers.

This section shows how to:

- Enable the default priority queues for all configured DLSw Peers
- Enable the default priority queues for unconfigured peers
- Customize the default priority queue configuration

Note: This section assumes that DLSw is already configured on an interface and that the Peer Table is complete. For information about configuring a circuit with DLSw and setting the slot, peer, and SAP parameters, refer to earlier chapters.

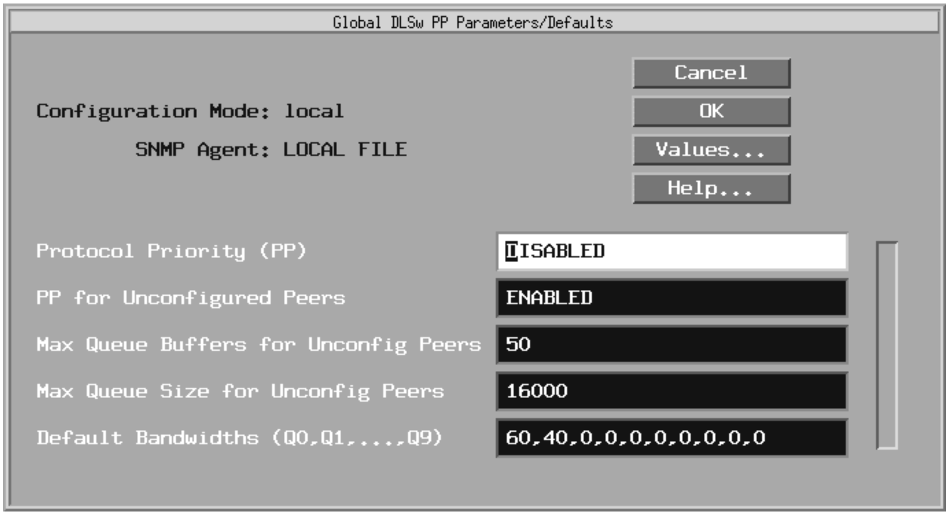
Enabling the Default Queues for Configured and Unconfigured Peers

Begin by displaying the DLSw Protocol Prioritization (PP) Global Parameters window:

1. **From the Configuration Manager window, select Protocols > DLSw > Prot Prioritization (Outbound) > Global).**

   The Global DLSw PP Parameters/Defaults window appears (Figure 6-2).

Note: See the section "Using the DLSw Peer Configuration Window," later in this chapter, for another way to access the Global DLSw PP Parameters/ Defaults window.



Global DLSw PP Parameters/Defaults

Configuration Mode: local

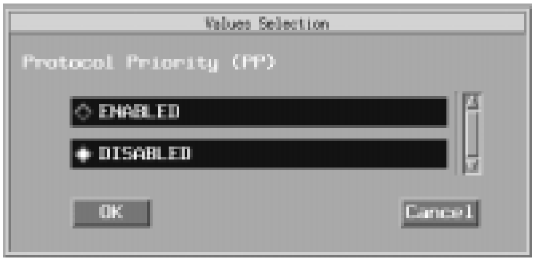
SNMP Agent: LOCAL FILE

Protocol Priority (PP)	DISABLED
PP for Unconfigured Peers	ENABLED
Max Queue Buffers for Unconfig Peers	50
Max Queue Size for Unconfig Peers	16000
Default Bandwidths (Q0,Q1,...,Q9)	60,40,0,0,0,0,0,0,0,0

Figure 6-2. Global DLSw PP Parameters/Defaults Window

2. **Select Protocol Priority (PP) and click on Values.**

   The Protocol Priority (PP) Values Selection window appears (Figure 6-3).



Values Selection

Protocol Priority (PP)

○ ENABLED

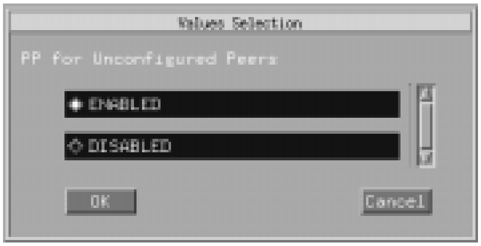
● DISABLED

Figure 6-3. Enabling Protocol Prioritization on DLSw Peers

3. **Select ENABLED.**
4. **Click on OK.**

   The Global DLSw PP Parameters/Defaults window reappears (Figure 6-2).

5. **To also use the default priority queue structure for all *un*configured peers, change the value of the PP for Unconfigured Peers box to Enabled (Figure 6-4).**



Values Selection

PP for Unconfigured Peers

● ENABLED

○ DISABLED

Figure 6-4. Enabling Protocol Prioritization for Unconfigured Peers

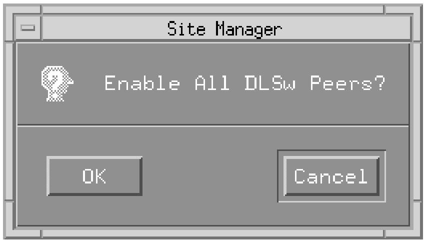
6. **Click on OK.**

   The Global DLSw PP Parameters/Defaults window reappears (refer to Figure 6-2).

7. **Decide whether to use the default queue configuration or customize the queue to suit your network:**

   - To use the default queue configuration, click on OK to exit.

     Site Manager asks you to confirm (Figure 6-5).



Site Manager

Enable All DLSw Peers?

Figure 6-5. Enabling Protocol Prioritization for All DLSw Peers

- To customize the default queue configuration, continue with the next section, “Customizing the Default Queue Configuration.”

Customizing the Default Queue Configuration

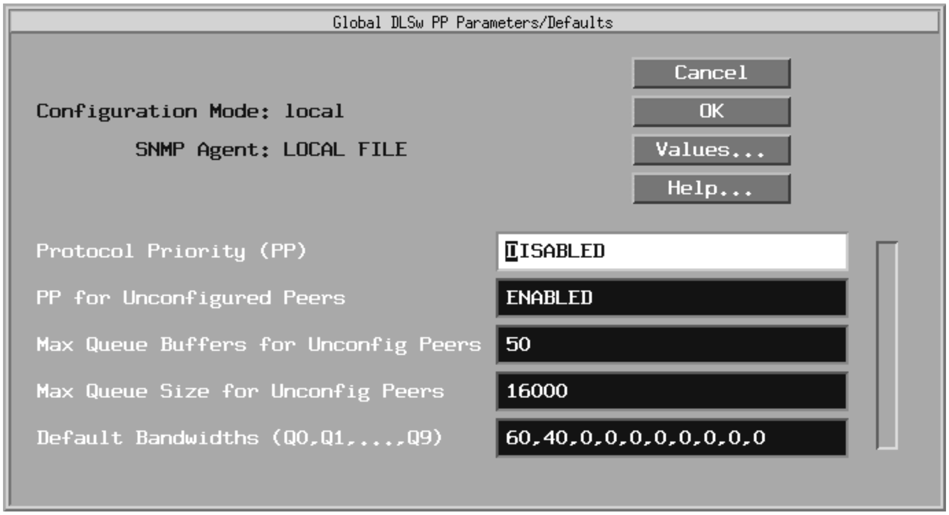
Once you enable DLSw protocol prioritization, any DLSw peer uses default values that control how priority queues work. You can change these values according to your network traffic needs.

➡ **Note:** The default priority queue configuration applies to all configured DLSw peers except those configured with a custom priority queue configuration. Peer-specific queue configurations take precedence over the default DLSw priority queue configuration.

Complete the following steps to edit the default DLSw protocol prioritization parameters:

1. **From the Configuration Manager window, select Protocols > DLSw > Prot Prioritization (Outbound) > Global.**

   The Global DLSw PP Parameters/Defaults window appears (Figure 6-6).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Protocol Priority (PP) DISABLED
PP for Unconfigured Peers ENABLED
Max Queue Buffers for Unconfig Peers 50
Max Queue Size for Unconfig Peers 16000
Default Bandwidths (Q0,Q1,...,Q9) 60,40,0,0,0,0,0,0,0,0

Figure 6-6. Global DLSw PP Parameters/Defaults Window

2. **Edit the parameters that you want to change, using the descriptions following this procedure as guidelines.**
3. **Click on OK when you are finished editing parameters.**

DLSw Protocol Prioritization Parameter Descriptions

Use the following descriptions as guidelines when you configure parameters in the Global DLSw PP Parameters/Defaults window.

Parameter: **Protocol Priority (PP)**

Default: Disabled

Options: Enabled | Disabled

Function: Toggles protocol prioritization on and off for configured DLSw peers. If you set this parameter to Disabled, all default priority queues will be disabled. Setting this parameter to Disabled is useful if you want to temporarily disable protocol prioritization for configured peers.

Instructions: Set to Disabled if you want to temporarily disable all protocol prioritization activity. Set to Enabled if you previously disabled protocol prioritization and now want to reenable it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.17

Note: Once you enable a peer-specific priority queue using the Peer Queues window, you must use that window to disable that peer's queues. You cannot disable queues that are already active from the Global DLSw PP Parameters/ Defaults window.

Parameter: **PP for Unconfigured Peers**

Default: Disabled

Options: Enabled | Disabled

Function: Toggles protocol prioritization for unconfigured DLSw peers on and off. Setting this parameter to Disabled disables all unconfigured priority queues. The Disabled setting is useful if you want to temporarily disable protocol prioritization for unconfigured peers.

Instructions: Set to Disabled if you want to temporarily disable all protocol prioritization activity. Set to Enabled if you previously disabled protocol prioritization and now want to reenable it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.20

Parameter:	**Max Queue Buffers for Unconfig Peers**
Default:	50
Range:	10 to 2147483647
Function:	Specifies the maximum number of packets in each default queue.
Instructions:	Enter a number of packets to increase or decrease the default buffer size of 50 packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.21

Parameter:	**Max Queue Size for Unconfig Peers**
Default:	16000
Range:	5000 to 2147483647
Function:	Specifies the maximum size (in bytes) of each default queue.
Instructions:	Enter a number of bytes to increase or decrease the default queue size of 16000 bytes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.22

Parameter:	**Default Bandwidths**
Default:	60, 40, 0, 0, 0, 0, 0, 0, 0, 0
Range:	Ten entries (one per queue) of a percentage between 0 and 100
Function:	Determines the number of default queues and allocates the bandwidth for each.
Instructions:	Either accept the default of 60 percent in Q0 and 40 percent in Q1, or enter up to ten values (one for each queue). Separate each bandwidth percent with a comma. The bandwidth percentages must total 100 percent. On low-speed lines running NetBIOS, you should allocate 20 percent of the total bandwidth due to endstation timing. For example, the following allots 10 percent of the bandwidth to each of ten queues: **10, 10, 10, 10, 10, 10, 10, 10, 10, 10**
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.19

Configuring Peer-Specific Priority Queues

You create the priority queue configuration for all configured and unconfigured DLSw peers using the Global DLSw PP Parameters/Default window (refer to Figure 6-6).

You customize priority queues for particular configured DLSw peers using the Peer Queue Configuration window.

➡ **Note:** Peer-specific queue configurations take precedence over the default DLSw priority queue configuration.

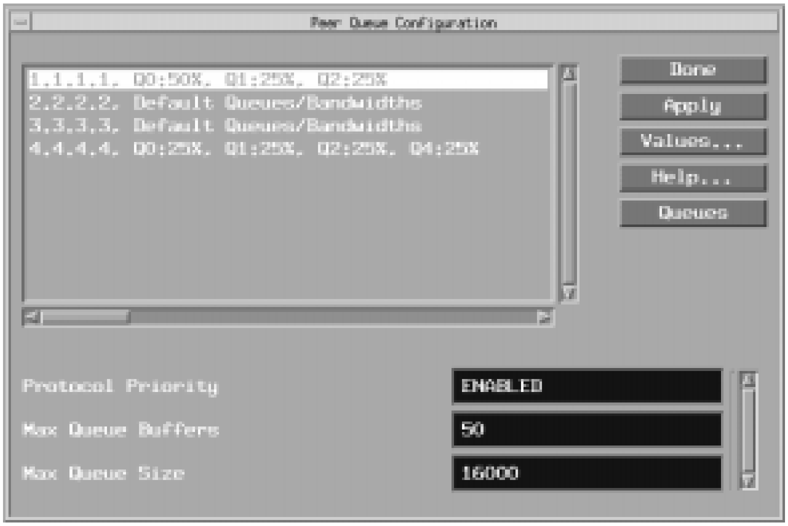
Priority Queues for a Specific DLSw Peer

Begin by displaying the Peer Queue Configuration window:

1. **From the Configuration Manager window, select Protocols > DLSw > Prot Prioritization (Outbound) > Peer Queue Entries.**

   The Peer Queue Configuration window appears (Figure 6-7).

➡ **Note:** See the later section, "Using the DLSw Peer Configuration Window," for another way to access the Peer Queue Configuration window.



```
1.1.1.1. Q0:50%. Q1:25%. Q2:25%
2.2.2.2. Default Queues/Bandwidths
3.3.3.3. Default Queues/Bandwidths
4.4.4.4. Q0:25%. Q1:25%. Q2:25%. Q4:25%
```

Protocol Priority ENABLED

Max Queue Buffers 50

Max Queue Size 16000

Figure 6-7. Peer Queue Configuration Window

The Peer Queue Configuration window summarizes the priority queue status for all DLSw peers. The scroll box lists each peer and indicates whether it uses the default or a specific queue configuration. (All of the DLSw peers in Figure 6-7 use the default queue configuration.)

The parameter boxes at the bottom of the screen show protocol prioritization as currently Disabled or Enabled for the selected peer, and list that peer’s queue configuration information (queue buffers and size).

2. **Select the individual peer address on which to configure priority queues.**

3. **Click on Queues in the Peer Queue Configuration window.**

   The Add/Edit/Delete Queues window appears (Figure 6-8).

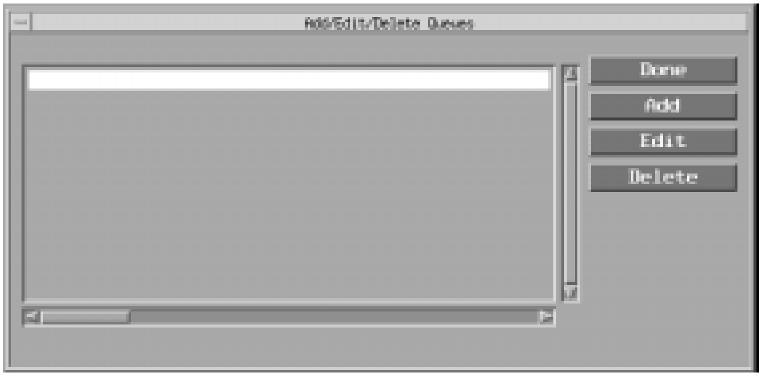
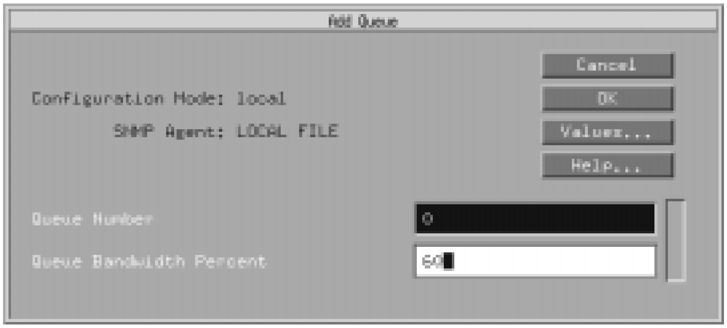


Figure 6-8. Add/Edit/Delete Queues Window

4. **Click on Add.**

   The Add Queue window appears (Figure 6-9).



Configuration Mode: local

SNMP Agent: LOCAL FILE

Queue Number 0

Queue Bandwidth Percent 60

Figure 6-9. Add Queue Window

5. **Enter a queue number.**

   The first queue must be Q0. You can number additional queues from 1 to 9. You do not need to number them in sequence, although doing so may help you keep track of the queues on a peer.

6. **Enter a bandwidth.**

   The bandwidth for Q0 must be greater than 0. You can assign any percentage between 0 and 99 to subsequent queues, as long as the combined bandwidth for all queues totals 100 percent.

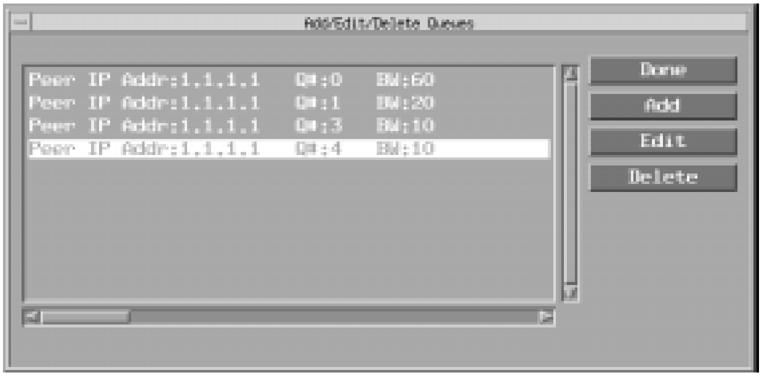
   On low-speed lines running NetBIOS, you should allocate 20 percent of the total bandwidth due to endstation timing.

7. **Click on OK.**

   The Add/Edit/Delete Queues window reappears.

8. **Repeat Steps 3 through 7 until the total bandwidth is 100 percent.**

   Figure 6-10 shows a sample screen after adding queues.

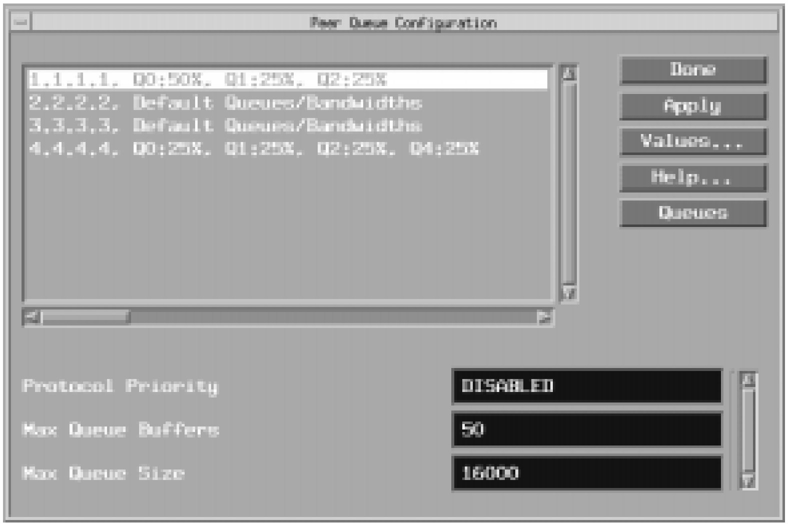


```
Peer IP Addr:1.1.1.1    Q#:0    BW:60
Peer IP Addr:1.1.1.1    Q#:1    BW:20
Peer IP Addr:1.1.1.1    Q#:3    BW:10
Peer IP Addr:1.1.1.1    Q#:4    BW:10
```

Figure 6-10. Configured Queues

9. **Click on Done.**

   The Peer Queue Configuration window reappears (Figure 6-11). Now two of the DLSw peers use peer-specific queues, and two use the default queue configuration.



```
1.1.1.1. Q0:50%. Q1:25%. Q2:25%
2.2.2.2. Default Queues/Bandwidths
3.3.3.3. Default Queues/Bandwidths
4.4.4.4. Q0:25%. Q1:25%. Q2:25%. Q4:25%
```

Protocol Priority: DISABLED

Max Queue Buffers: 50

Max Queue Size: 16000

Figure 6-11. Peer Queue Configuration Window with Both Default and Peer-Specific Configurations

Enabling or Disabling a Single Peer’s Priority Queues

You can enable or disable the queues that you configured for an individual DLSw peer using the Peer Queue window.

Note: Once you enable priority queues using the Peer Queue Configuration window, you must use that window to disable that peer’s queues. You cannot disable queues that are already active from the Global DLSw PP Parameters/Default window.

1. **From the Configuration Manager window, select Protocols > DLSw > Prot Prioritization (Outbound) > Peer Queue Entries.**

   The Peer Queue Configuration window appears (refer to Figure 6-11).

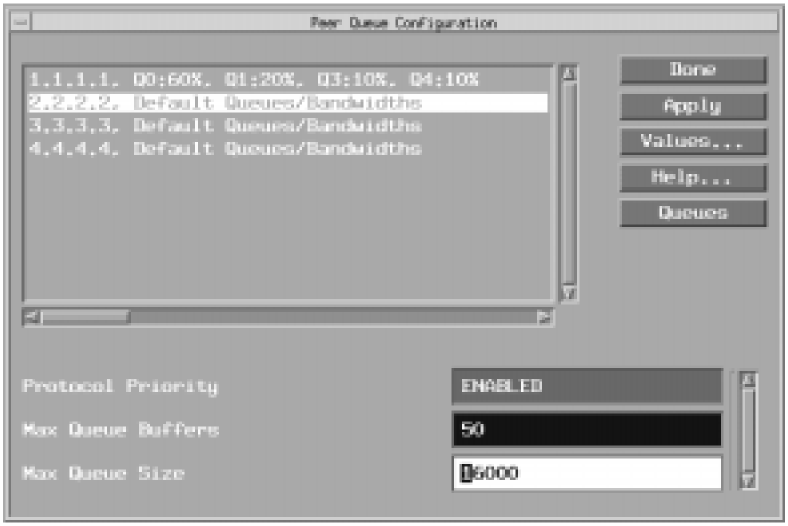
2. **Select the peer from the scroll box.**
3. **Change the value of Protocol Priority to Enabled or Disabled.**
4. **Click on Apply.**
5. **Click on Done.**

Customizing Specific DLSw Peer Queues

Once you create and enable peer-specific queues, the DLSw peer in question uses default values that dictate how the priority queues work. You can change these values according to your network traffic needs.

1. **From the Configuration Manager window, select Protocols > DLSw > Prot Prioritization (Outbound) > Peer Queue Entries.**

   The Peer Queue Configuration window appears (Figure 6-12).



1.1.1.1. Q0:60%. Q1:20%. Q3:10%. Q4:10%
2.2.2.2. Default Queues/Bandwidths
3.3.3.3. Default Queues/Bandwidths
4.4.4.4. Default Queues/Bandwidths

Protocol Priority ENABLED
Max Queue Buffers 50
Max Queue Size 16000

Figure 6-12. Peer Queue Configuration Window

2. **Edit the Peer Queue parameters that you want to change, using the following descriptions as guidelines.**
3. **Click on Apply.**
4. **Click on Done.**

Peer Queue Configuration Parameter Descriptions

Use the following descriptions as guidelines when you configure parameters on the Peer Queue Configuration window.

Parameter: **Protocol Priority**

Default: Disabled

Options: Enabled | Disabled

Function: Toggles protocol prioritization on and off for this peer. If you set this parameter to Disabled, priority filters will be disabled on this peer. Setting this parameter to Disabled is useful if you want to temporarily disable protocol priority but leave the outbound filters in place.

Instructions: Set to Disabled if you want to temporarily disable all protocol prioritization activity on this peer. Set to Enabled if you previously disabled protocol prioritization on this peer and now want to reenable it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.5.1.5

Parameter: **Max Queue Buffers**

Default: 50

Range: 10 to 2147483647

Function: Specifies the maximum number of packets in each of this peer’s queues.

Instructions: Enter a number of packets to increase or decrease the default buffer size of 50 packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.5.1.6

Parameter:	**Max Queue Size**
Default:	16000
Range:	5000 to 2147483647
Function:	Specifies the maximum size of each of this peer’s queues.
Instructions:	Enter a number of bytes to increase or decrease the default queue size of 16000 bytes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.7

Creating DLSw Priority Filters

Outbound traffic filters configured with the “queue” action (*priority filters*) determine which DLSw traffic is processed into priority queues.

To configure the DLSw priority filters, begin by displaying the DLS Priority/ Outbound Filters window.

1. **From the Configuration Manager window, select Protocols > DLSw > Prot Prioritization (Outbound) > PP Traffic Filters.**

   The DLS Priority/Outbound Filters window appears (Figure 6-13).

➡ **Note:** See the later section, “Using the DLSw Peer Configuration Window,” for another way to access the DLS Priority/Outbound Filters window.

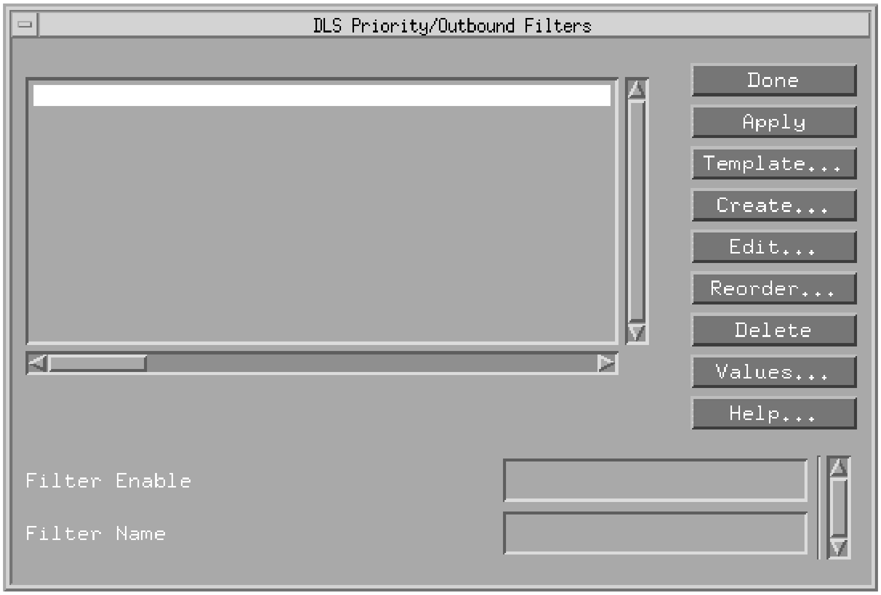


Figure 6-13. DLS Priority/Outbound Filters Window

This window shows any existing outbound traffic filters for DLSw peers, regardless of whether the filters are currently active on the peers.

2. **Click on Template.**

   The Filter Template Management window appears (Figure 6-14). You create templates in this window the same way you do in the Template Management window for WAN protocols.

   See *Configuring Traffic Filters and Protocol Prioritization* for details about using the Priority/Outbound Filters window for WAN protocols.

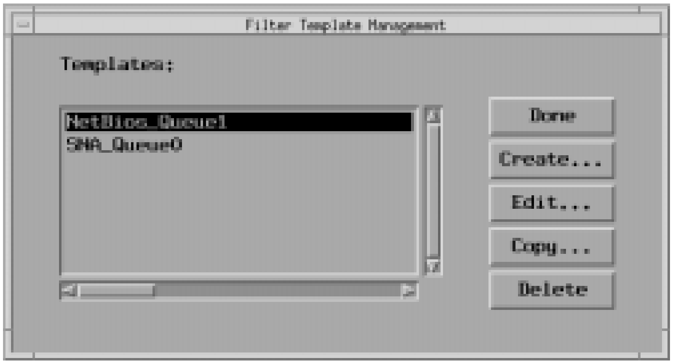


Figure 6-14. Filter Template Management Window

The software includes sample templates for filtering NetBIOS and SNA traffic (*NetBIOS_Queue1* and *SNA_Queue0*, shown in Figure 6-14).

The sample templates place SNA traffic in Q0 and NetBIOS traffic in Q1. Unless you have customized the default queue configuration, Q0 (SNA) receives 60 percent of the bandwidth and Q1 (NetBIOS) receives 40 percent. Using the remaining steps in this section, you can create filters from these, or similar, templates.

To use the sample templates, copy the file */usr/wf/template/template.flt* to the directory from which you start Site Manager (your Site Manager working directory). If that directory already contains a *template.flt* file, rename the existing file or copy the contents of the *template.flt* file into your existing *template.flt* file.

3. **Decide whether to create a new template or use an existing template:**
   - If no existing template matches your needs, create a new filter template.
   - To create a template similar to an existing one, copy the existing template (to preserve the original template) to a new template with the same criteria and actions. Then, edit the new template.
   - To modify an existing template without preserving the original template, edit the existing template. Note that changing a template does not affect interfaces to which the template has already been applied.

4. **Click on Create to make a new template, or select an existing template and click on Edit.**

   The Create DLS Template window or the Edit DLS Template window appears. Creating and editing templates involve the same steps; you use both windows exactly the same way.

5. **Name the template.**

6. **Select a DLSw criterion (Figure 6-15).**

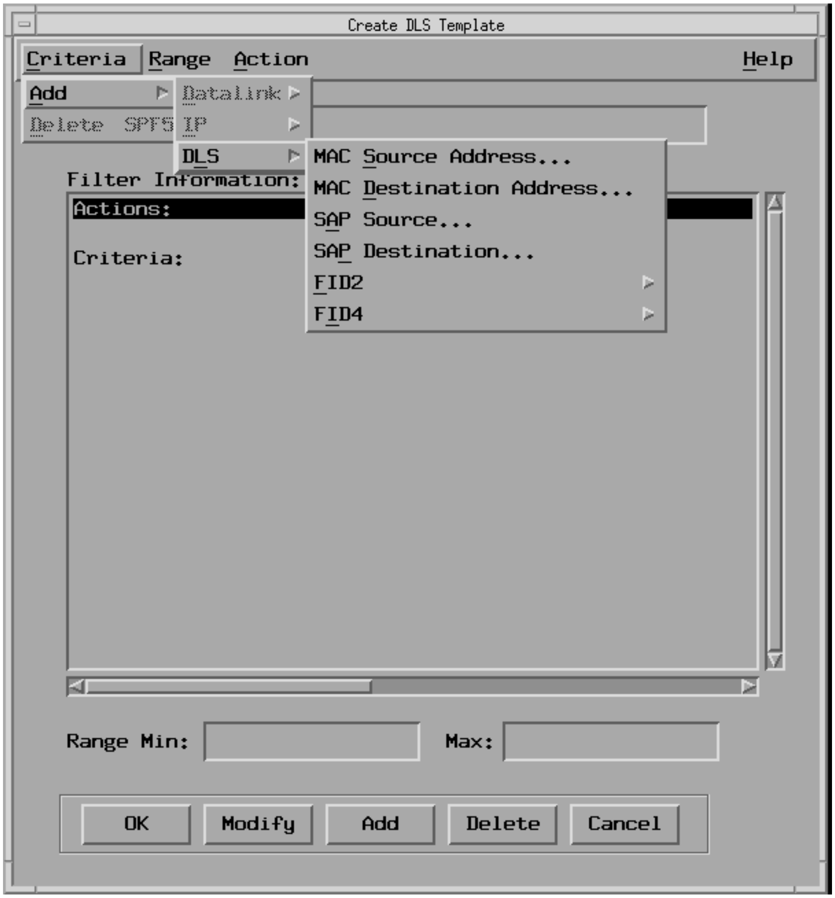


Figure 6-15. Selecting a Predefined DLSw Outbound Filter Criterion

Refer to Appendix B for information about the DLSw outbound traffic filter criteria.

7. **Select Action > Add > Queue (Figure 6-16).**

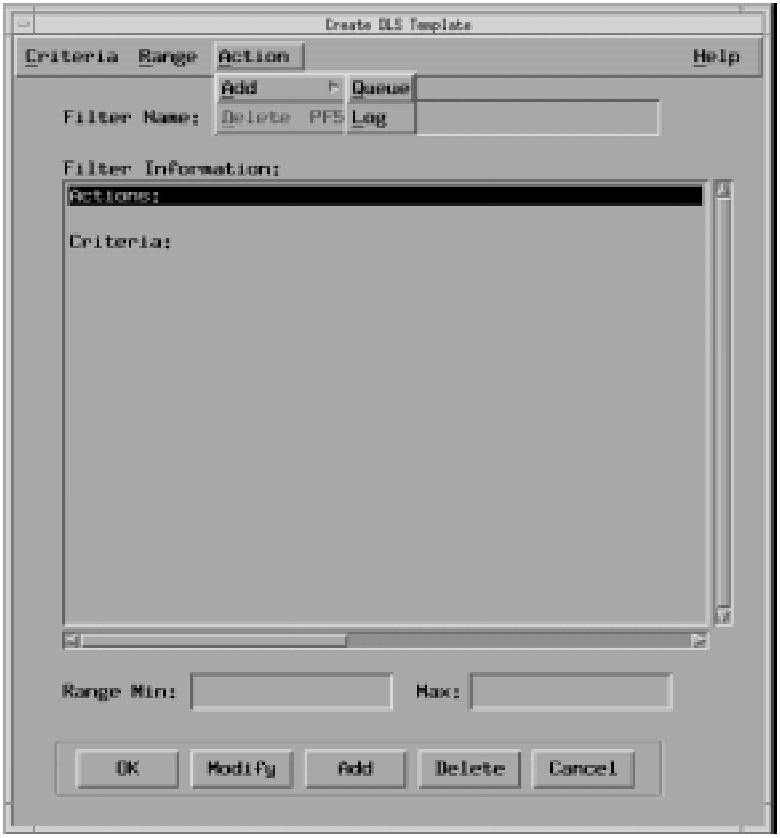
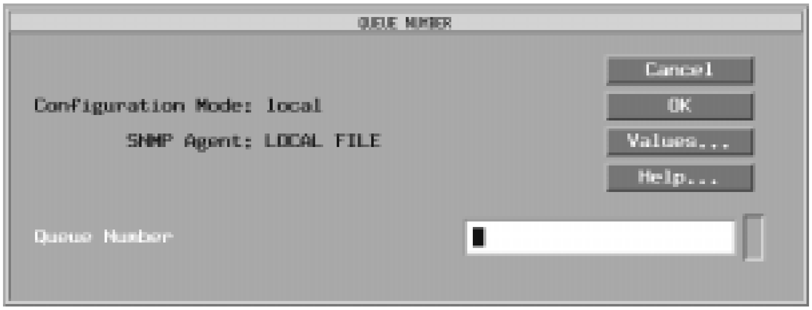


Figure 6-16. Selecting the DLSw Queue Action

The Queue Number window appears (Figure 6-17).



Configuration Mode: local

SNMP Agent: LOCAL FILE

Queue Number

Figure 6-17. Queue Number Window

8. **Enter the queue number.**

   DLSw will send traffic that meets this filter’s criteria and ranges to the queue number you specify.

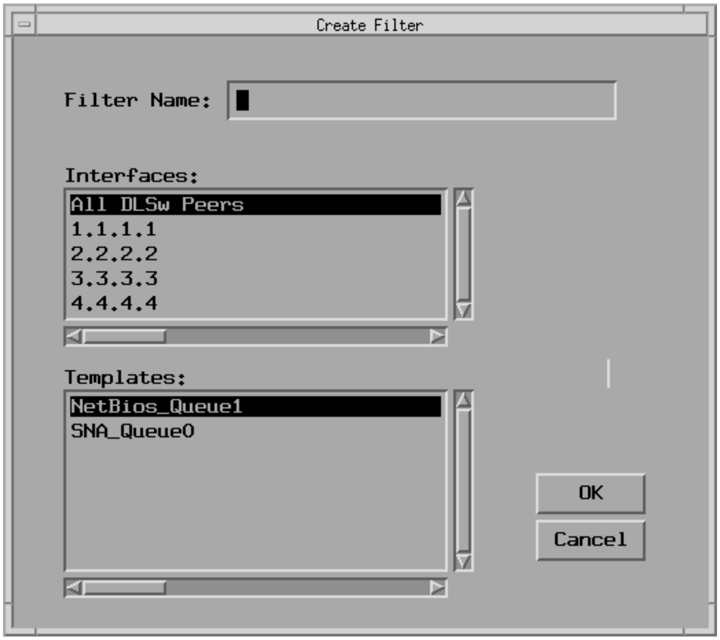
9. **Click on OK.**

   The Filter Template Management window reappears (refer to Figure 6-14).

10. **Click on Done to return to the DLS Priority/Outbound Filters window (refer to Figure 6-13).**

11. **To apply the template, click on Create.**

    The Create Filter window appears (Figure 6-18).



Create Filter

Filter Name:

Interfaces:

All DLSw Peers
1.1.1.1
2.2.2.2
3.3.3.3
4.4.4.4

Templates:

NetBios_Queue1
SNA_Queue0

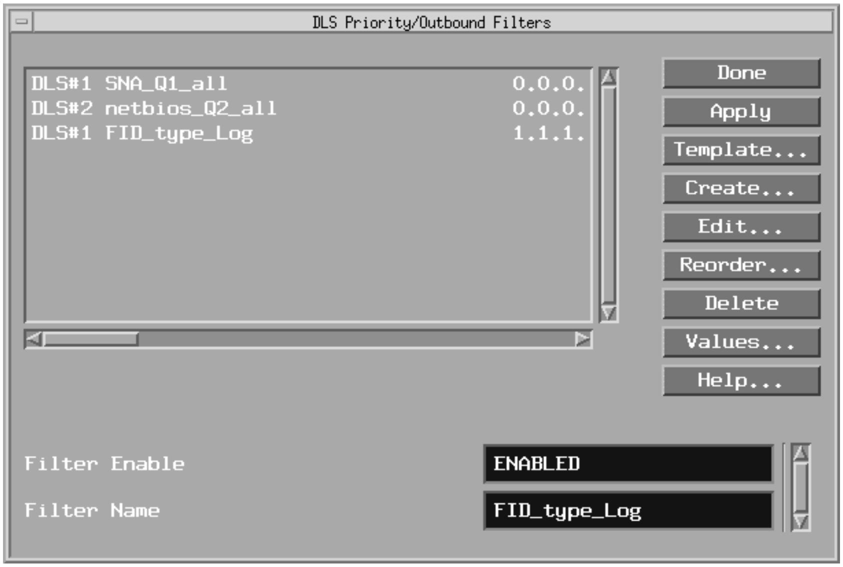
Figure 6-18. Create Filter Window

12. **Type a name for the filter in the Filter Name box.**
13. **Highlight All DLSw Peers to apply this template to all configured peers, or select an individual peer from the Interfaces scroll box.**
14. **Select the template that you want to apply from the Templates scroll box.**
15. **Click on OK.**

    The DLS Priority/Outbound Filters window reappears, with the new filter displayed in the scroll box (Figure 6-19).

16. **Repeat Steps 11 to 15 to apply other templates.**

    Each entry in the filter scroll box lists the filter number, filter name, and IP address of the affected DLSw peer. Filters that apply to all DLSw peers appear with IP address 0.0.0.0. Site Manager numbers the filters for each peer interface chronologically.



```
DLS#1 SNA_Q1_all                                0.0.0.
DLS#2 netbios_Q2_all                            0.0.0.
DLS#1 FID_type_Log                              1.1.1.
```

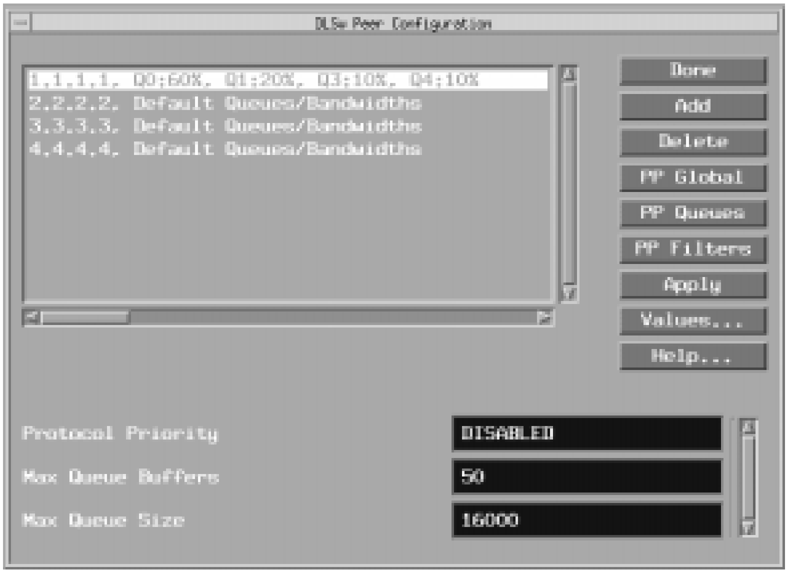
Filter Enable ENABLED

Filter Name FID_type_Log

Figure 6-19. DLS Priority/Outbound Filters Window with Configured FIlters

Using the DLSw Peer Configuration Window

In addition to using the menu selections shown in this section, you can access the DLSw Protocol Prioritization windows directly from the DLSw Peer Configuration window (Figure 6-20).



```
1.1.1.1. Q0:60%. Q1:20%. Q3:10%. Q4:10%
2.2.2.2. Default Queues/Bandwidths
3.3.3.3. Default Queues/Bandwidths
4.4.4.4. Default Queues/Bandwidths
```

Protocol Priority: DISABLED

Max Queue Buffers: 50

Max Queue Size: 16000

Figure 6-20. DLSw Peer Configuration Window

Table 6-1 lists the ways in which you access the DLSw Peer Configuration window.

Table 6-1. Accessing the DLSw Protocol Prioritization Windows

To Access This Window	Click on This Button in the DLSw Peer Configuration Window
Global DLSw PP Parameters/Defaults	PP Global
Peer Queue Configuration	PP Queues
DLS Priority/Outbound Filters	PP Filters

Sample Templates for DLSw Protocol Prioritization

In addition to using the Configuration Manager screens described in this guide to configure traffic filter templates, you can also edit or copy a traffic filter template using a text editor. The Configuration Manager stores all templates for all protocols in the file */usr/wf/template/template.flt*.

Included with the software is a *template.flt* file that contains two sample DLSw protocol prioritization templates that you can use for differentiating SNA and NetBIOS traffic. To use the sample templates, copy */usr/wf/template/template.flt* to the directory from which you start Site Manager (your Site Manager working directory). If that directory already contains a *template.flt* file, copy the contents of the latest file into your existing file.

The sample templates place SNA traffic in the default queue (Q0) and NetBIOS traffic in Q1. Using the default queue configuration, Q0 receives 60 percent of the bandwidth and NetBIOS receives 40 percent of the bandwidth. The section "Creating DLSw Priority Filters" earlier in this chapter lists the steps for creating filters from these, or similar, templates.

Appendix A
DLSw Default Settings

Tables A-1 to A-11 list the default settings for DLSw parameters. Use the Configuration Manager to edit the default settings.

Table A-1. DLSw Basic Global Parameters

Parameter	Default
DLSw Virtual Ring ID	None
Reject Unconfigured Peers	Accept
DLSw RFC Version	RFC 1434
DLSw NetBIOS Support	No
DLSw Peer IP Address (add only)	0.0.0.0 (none)

Table A-2. DLSw Basic Interface Parameters

Parameter	Default
SR Interface Ring ID	0x0
DLSw Slot IP Address	0.0.0.0 (none)

Table A-3. DLSw Advanced Global Parameters

Parameter	**Default**
Enable	Enable
TCP Window Size	8000 octets
IP Virtual Ring	None
Max Slot Sessions	200 sessions per slot
Virtual Ring MTU	1500
MAC Cache Age	300 s
NetBIOS Cache Age	300 s
Reject Unconfigured Peers	Accept
DLSw RFC Version	RFC 1434
Maximum Package Size	1532 bytes
Packaging Timeout	10 ms
Packaging Threshold	20% of TCP window size
Multislot Broadcasts	Enable
Initial Pacing Window	5
NetBIOS Session Alive Filter	Enable
KeepAlive Time	60 s
KeepAlive Retry Timer	60 s
KeepAlive Retries	4
SNA Fallback Attempts	5
NetBIOS Fallback Time	180 s
TCP Inact Time	300 s
TCP Inact Method	CIRCUITS

Table A-4. DLSw Advanced Interface Parameters

Parameter	**Default**
Enable	Enable
DLSw Mode	Primary

Table A-5. DLSw Peer IP Table Parameters

Parameter	**Default**
Peer IP Address	None
Transport Type	Unknown
Backup IP Address	0.0.0.0 (None)
Backup Max Up Time	0
Backup Peer Type	V20 (Unicast - Unknown)
Backup Hold Down Time	120
Backup Start Time	1
Backup End Time	1
Backup Delete	Create

Table A-6. DLSw Slot IP Table Parameters

Parameter	**Default**
IP Address for TCP Connection	None
Slot	None
IP Address	None

Table A-7. DLSw SAP Parameters

Parameter	Default
SAP Window	10 frames
SAP	0x004, 0x008, 0x00C

Table A-8. DLSw Default NetBIOS Peer IP Table Parameters

Parameter	Default
Default NetBIOS Peer IP Address	None
NetBIOS Name	None
NetBIOS Peer IP Address	None

Table A-9. DLSw Default MAC Peer IP Table Parameters

Parameter	Default
Default MAC Peer IP Address	None
MAC Address	None
MAC Peer IP Address	None

Table A-10. DLSw Local Devices Parameters

Parameter	Default
Disable	Enable
Link Station Address (hex)	None
DLSw Mode	Primary
PU Name	None
PU Type	None
IDBLOCK	None
IDNUM	None
XID Format	None
Source (Virtual) MAC (hex)	None
Source (Virtual) SAP (hex)	None
Destination MAC (hex)	None
Destination SAP (hex)	0x4
MAXOUT	7
MAXDATA	2057
Canureach Timer/Timer2	30 s
Canureach Retries/Retries2	4294967295
Link Station Timer	30 s
Link Station Retries	4294967295
SDLC Receive Credit	10
SDLC Transmit Credit	10
Enable XID Pass Thru	Disable
Device Activation Seq	Local Device First

Table A-11. DLSw Protocol Prioritization Parameters

Parameter	Default
Protocol Priority	Disabled
PP for Unconfigured Peers	Disabled
Max Queue Buffers for Unconfig Peers	50
Max Queue Size for Unconfig Peers	16000
Default Bandwidths	60,40, 0,0,0,0,0,0,0,0
Max Queue Buffers	50
Max Queue Size	16000
Queue Number	None
Queue Bandwidth Percent	0

Table A-12. DLSw Multicast Configuration Parameters

Parameter	Default
Multicast IP Address	0.0.0.0
Slot	00000
Multicast IP Slots	Depends on slot numbers selected for Slot parameter
Backup Config	No
Backup IP Address	0.0.0.0
Backup Peer Type	V20 (Unicast-Unknown)
Backup Max Up Time	0
Backup Hold Down Time	120
Backup Start Time	1
BAckup End Time	2400

Appendix B
Criteria for DLSw Prioritization

This appendix includes both the DLSw *predefined* criteria that the Configuration Manager provides and the supported DLSw reference points for *user-defined* criteria for DLSw prioritization, described in Chapter 6.

Predefined DLSw Criteria

You configure outbound filters for DLSw traffic based on the predefined criteria listed in Table B-1.

Table B-1. Predefined Outbound Filter Criteria Based on DLSw Header

Packet Type or Component	Predefined Criteria
Any	MAC Source Address[1] MAC Destination Address[1] DSAP[2] SSAP[2]
FID4	FID Type Network Priority Trans Priority Dest Subarea Address Origin Subarea Address Expedited Flow Indicator Destination Element Origin Element User-Defined
FID2	FID Type EFI (Expedited Flow Indicator) Destination Element DAF (Destination Address Field) OAF (Origin Address Field) User-Defined

[1] See the "Specifying MAC Address Ranges" section later in this appendix.

[2] See the "Specifying Source and Destination SAP Code Ranges" section, later in this appendix.

DLSw Reference Points

Tables B-2 and B-3 list the predefined DLSw reference points for outbound traffic filters based on the SNA transmission header.

Table B-2. DLSw Reference Points for FID2 Frames

Criteria (FID2)	Reference Point	Offset (bits)	Length (bits)
Format Identifier (FID)	SNA_START	0	4
Expedited Flow Indicator (EFI)	SNA_START	7	1
Destination Address Field (DAF)	SNA_START	16	8
Origin Address Field (OAF)	SNA_START	24	8

Table B-3. DLSw Reference Points for FID4 Frames

Criteria (FID4)	Reference Point	Offset (bits)	Length (bits)
Format Identifier (FID)	SNA_START	0	4
Network Priority	SNA_START	7	1
Transmission Priority Field (TPF)	SNA_START	30	2
Destination Subarea Address Field (DSAF)	SNA_START	64	32
Origin Subarea Address Field (OSAF)	SNA_START	96	32
Expedited Flow Indicator (EFI)	SNA_START	135	1
Destination Element Field (DEF)	SNA_START	144	16
Origin Element Field (OEF)	SNA_START	160	16

Specifying MAC Address Ranges

When you create a filter that includes a source or destination MAC Address criterion, you specify the MAC Address range in either most significant bit (MSB) or canonical format. Table B-4 lists the address formats to use.

Table B-4. Format for Specifying Source-Routing MAC Addresses

Address Type	Address Format
PPP	MSB
PPP	MSB
Bay Networks Standard Frame Relay	Canonical
Bay Networks Proprietary PPP	Canonical
Token Ring	MSB
Ethernet	Canonical

When defining outbound traffic filters you can specify a MAC address in either MSB or canonical format, but the default is canonical.

Source Routing Bridge Source MAC Addresses

When specifying source MAC source routing addresses, set the MSB to one.

For example, on Token Ring packets, the source MAC address to be filtered is 0x40000037450440. Then:

1. Add the first bit set MAC address 0x800000000000.
2. Enter the filter criteria range as 0xC00037450440.

Bit 0 (the 0x80 bit) of byte 0 (the leftmost byte) indicates the presence of the routing information field (RIF). This bit is set to 1 if the RIF field is present and 0 if there is no RIF field. Keep this in mind if you use a sniffer to analyze packets for their source MAC address. For example, a sniffer would decode LAA with the first byte of 40 as 0x400031740001. If the RIF bit is set, the hexadecimal value of the packet is 0xC00031740001.

Source Routing Bridge Functional MAC Addresses

Functional MAC addresses are destination MAC addresses that always conform to the following rules:

- Byte 0 = 0xC0
- Byte 1 = 0x00
- The first half of byte 2 = 0x0 to 0x7

Table B-5 lists some common functional MAC addresses.

Table B-5. Functional MAC Addresses

Function Name	MAC Address (MSB)	Identifying Bit	Ethernet Address
Active Monitor	0xC000 0000 0001	Byte 5, bit 7	0x030000000080
Ring Parameter Server	0xC000 0000 0002	Byte 5, bit 6	0x030000000040
Ring Error Monitor	0xC000 0000 0008	Byte 5, bit 4	0x030000000010
Configuration Report Server	0xC000 0000 0010	Byte 5, bit 3	0x030000000008
NetBIOS	0xC000 0000 0080	Byte 5, bit 0	0x030000000001
Bridge	0xC000 0000 0100	Byte 4, bit 7	0x030000008000
LAN Manager	0xC000 0000 2000	Byte 4, bit 2	0x030000000400
User-Defined	0xC000 0008 0000 to 0xC000 4000 0000	Byte 3, bits 0 - 4; Byte 2, bits 1 - 7	0x030000100000 to 0x030002000000

Specifying Source and Destination SAP Code Ranges

Table B-6 lists several SAP codes to use when specifying a range for source or destination SAP traffic filter criteria.

Table B-6. SAP Codes

Description	SAP Code
XID or TEST	00
Individual Sublayer Mgmt	02
Group Sublayer Mgmt	03
SNA	04, 08, 0C
IP	06
Proway Network Mgmt	0E
Novell and SDLC Link Servers	10
CLNP ISO OSI	20, 34
BPDU	42
X.25 over 802.2 LLC2	7E
XNS	80
Nestar	86
Active station list	8E
ARP	98
SNAP Subnet Access Protocol	AA
Banyan VIP	BC
Novell IPX	E0
CLNP ISO OSI	EC
IBM NetBIOS	F0
LAN Manager	F4, F5
Remote Program load	F8
UB	FA
IBM RPL	FC
ISO Network Layer	FE
LLC broadcast	FF

Appendix C
Troubleshooting DLSw

This appendix provides the following information about diagnosing and troubleshooting DLSw networks, specifically:

- Viewing the DLSw Log
- Enabling Extended Logging
- Using and Decoding the DLSw Log
- DLSw Session Setup
- Establishing DLSw/LLC Connections
- Establishing DLSw/SDLC Connections
- Disconnecting from the Network
- Troubleshooting DLSw
- Verifying the WAN Cabling

This appendix is for network administrators who understand SNA and DLSw. Because DLSw operation involves the complex interaction of multiple subsystems, administrators should also be familiar with SDLC, TCP, and LLC.

Viewing the DLSw Log

You view the log file containing Bay Networks event and debug messages using the Bay Networks network management software (Site Manager), the Bay Networks command line interface (Technician Interface), or any compatible third-party network management software.

For information about viewing events and messages using Site Manager or a compatible third-party network management software, see *Configuring and Managing Routers with Site Manager*. For a complete description of all warning, fault, trace, and informational messages, refer to *Event Messages for Routers*. For information on viewing events using the Technician Interface, see *Using Technician Interface Software*.

Enabling Extended Logging

Subsystems such as LLC and SDLC allow you to enable extended logging through the MIB. Extended logging provides additional messages and information that can help you identify and troubleshoot a DLSw network problem. However, using extended logging causes the router to use more log space and memory, and affects CPU performance. You enable extended logging using the Bay Networks Technician Interface.

Table C-1 lists each subsystem, the Technician Interface command that enables extended logging for that subsystem, and type(s) of messages or events that could appear in the log.

Table C-1. Extended Logging Commands for Subsystems

Subsystem	How to Enable	Items Logged
DLS	s wfDls.14.0 0xffffffff;commit* s wfDls.15.0 0x3;commit†	DLSw protocol and data link control events leading to connection state changes
LLC	s wfLlcInterfaceEntry.2.cct 0cfff1;commit	LLC inbound and outbound packets
SDLC	s wfSdlcPortAdminEntry.36.cct 0x1;commit	SDLC messages

* Enabled by default.

† DLS, LLC, and SDLC extended logging set by Technician Interface only.

With extended logging enabled, log messages describing the frame flows and state transitions appear during the critical phases of each connection being established.

Table C-2 shows more detailed information about the enabling bits shown in Table C-1.

Table C-2. Log Messages

Debug Flag Description	Enabling Bits	Enable Value (in Hex)
General Control and SSP Events	1 and 2	0x00000003
SDLC Events	3	0x00000004
1795 Peer and Capx/1434 Flow Control	4	0x00000008
SDLC Events	5	0x00000010
V2.0 Peer and Capx Events	6	0x00000020
Backup Peer Events	7	0x00000040
Test Table Lookup Results	29	0x10000000
SDLC and XID Information	31	0x40000000
SDLC LS Reference and DLS/TCP Protocol Priority	32	0x80000000

Using and Decoding the DLSw Log

This section provides general information about DLSw states and events, as described in RFC 1434 and RFC 1795. DLSw states and events appear as numbers within the text of logged messages.

If a message contains the text “old state = 3, new state = 1,” the numbers 3 and 1 point to specific conditions in the DLSw state table. Similarly, a message containing the text “event= 3,” points to a specific condition in the DLSw event table.

Table C-3 lists the DLSw state names and numbers. Table C-4 lists the DLSw events and numbers. Refer to these tables when decoding messages in the DLSw log.

Table C-3. DLSw State Table

State Name	State Number
CONNECTED	1
CONNECT PENDING	2
CONTACT PENDING	3
CIRCUIT ESTABLISHED	4
CIRCUIT PENDING	5
CIRCUIT RESTART	6
HALT PENDING	7
DISCONNECTED	11
DISCONNECT PENDING	12
RESTART PENDING	13
RESOLVE PENDING	14
CIRCUIT START	15
HALT PENDING NO ACK	16

Table C-4. DLSw Event Table

Event	Event Number (in decimal)
CANUREACH Received	3
ICANREACH Received	4
REACH_ACK Received	5
XIDFRAME Received	7
CONTACT Received	8

Table C-4. DLSw Event Table *(continued)*

Event	Event Number (in decimal)
CONTACTED Received	9
INFOFRAME Received	10
HALT_DL Received	14
DL_HALTED Received	15
RESTART_DL Received	16
DL_RESTARTED Received	17
NETBIOS_NQ/NETBIOS_NQ_ex/ NETBIOS_NQ_cs Received	18
NETBIOS_NR/NETBIOS_NR_ex/ NETBIOS_NR_cs Received	19
DATAFRAME Received	20
HALT_DL_NOACK Received	25
NETBIOS_ANQ Received	26
NETBIOS_ANR Received	27
KEEPALIVE Received	29
CAP_EXCHANGE Received	32
IFCM Received	33
TEST_CIRCUIT_REQ Received	122
TEST_CIRCUIT_RSP Received	123

Sample Log Entries

This section describes some common sample DLSw event entries that may appear in the log file. The event code in the Bay Networks log is an internal number that identifies the specific message. A description follows each message.

Event Code 16

```
#  15: 04/25/95 22:43:01 DEBUG     SLOT  1 DLS Event Code:  16
State change in connect_conf, conn = 30927f70, oldstate = 4, new
state = 3
```

This message describes major state changes:

connect_conf -- The routine processing the frame. It is probably a name corresponding to the type of event causing the state change.

conn = 30927f70 -- The unique connection identifier.

old state = 4, new state = 3-- The actual state transition occurring.

Event Code 17

```
#   4: 04/25/95 22:43:00 DEBUG     SLOT  1 DLS Event Code:  17
LLC test frame received
```

This message indicates that DLS received a specific frame type (test).

Event Code 36

```
 38: 04/25/95 22:43:17 DEBUG     SLOT  1 DLS Event Code:  36
Unexpected protocol action: state = 11, event = 10 conn = 30927f70
```

This messages shows that an illegal or unexpected event occurred. Although this does not always indicate a problem with the software, there could be a problem with the timer settings configured on each DLSw router. If the condition persists or causes improper operation, troubleshooting may be necessary.

state = 11 -- DISCONNECTED

event = 10 -- INFOFRAME Received

conn = 30927f70 -- The unique connection identifier

Event Code 45

```
#  10: 04/25/95 22:43:01 DEBUG     SLOT  1 DLS Event Code:  45
SSP XID frame rcvd in LLC, conn, state, flag: 30927f70, 4, 201
```

This message describes the receipt of an input frame from either TCP or the DLC:

SSP XID frame rcvd in LLC -- The type of frame received (XID) and where it was received (LLC, SDLC).

conn (30927f70) -- The unique connection identifier for this DLSw circuit. It will correspond to the correlator described in the DLSw RFCs state (4), CIRCUIT ESTABLISHED, as listed in the DLSw state table (refer to Table C-3).

flag (201) -- Bay Networks use only.

DLSw Session Setup

Before configuring DLSw, you should be familiar with how DLSw establishes sessions between network endpoints. To establish SNA or NetBIOS sessions between endpoints (devices), Bay Networks routers with DLSw enabled execute the following sequence of events.

- Upon receiving a TEST (POLL) or similar frame from an attached endstation, the receiving slot performs the following:
  - -- Converts the TEST (POLL) frame into an SSP CANUREACH command.
  - -- Searches the appropriate cache to determine if the remote location is known. If the remote location is already in the cache, the CANUREACH is forwarded only to this remote location. If the remote location is not in the cache, DLSw forwards the CANUREACH to all remote routers specified in the DLSw Peer IP Table, if this table exists.
  - -- Forwards the packet to all other slots defined in the DLSw Slot Table.
- Upon receiving a CANUREACH frame, a DLSw slot:
  - -- Forwards the frame to all other slots defined in this router’s DLSw Slot Table.
  - -- Converts the CANUREACH frame back to a TEST (POLL) frame.
  - -- Forwards the TEST (POLL) frame to all interfaces on this slot which have DLSw enabled.
- If the destination device resides on an attached LAN, then this device responds by broadcasting a TEST (RESPONSE) message. Upon receiving this response, the remote router:
  - -- Caches the MAC address (for SNA) or name (for NetBIOS) in the appropriate table on the router.

  - Converts the TEST (RESPONSE) packet into a DLSw ICANREACH frame.
  - Forwards the ICANREACH to the originating data link switch (router).
- Upon receiving the ICANREACH, the originating router:
  - Caches the MAC address or NetBIOS name and identity of the remote router in the appropriate table on the router.
  - Converts the ICANREACH back to a TEST (RESPONSE) frame.
  - Forwards the packet to the originating workstation.

At completion, all routers and endstations can forward SNA and NetBIOS packets appropriately, creating a logical session between endpoints.

Each slot on a Bay Networks router running DLSw functions as an independent data link switch. The network administrator controls the packets forwarded to DLSw by specifying the appropriate SAPs in the DLSw SAP Table.

Establishing DLSw/LLC Connections

Table C-1 illustrates a sample dual-switch DLSw network and the network packet exchanges (transactions) that occur when two DLSw routers connect to each other. Connections generate debug event messages in the log file. These messages provide critical information that can help you troubleshoot or report network connection problems.

Figure C-1 identifies each transaction with a message number. Use this number to point to the specific debug message that describes the network activity.

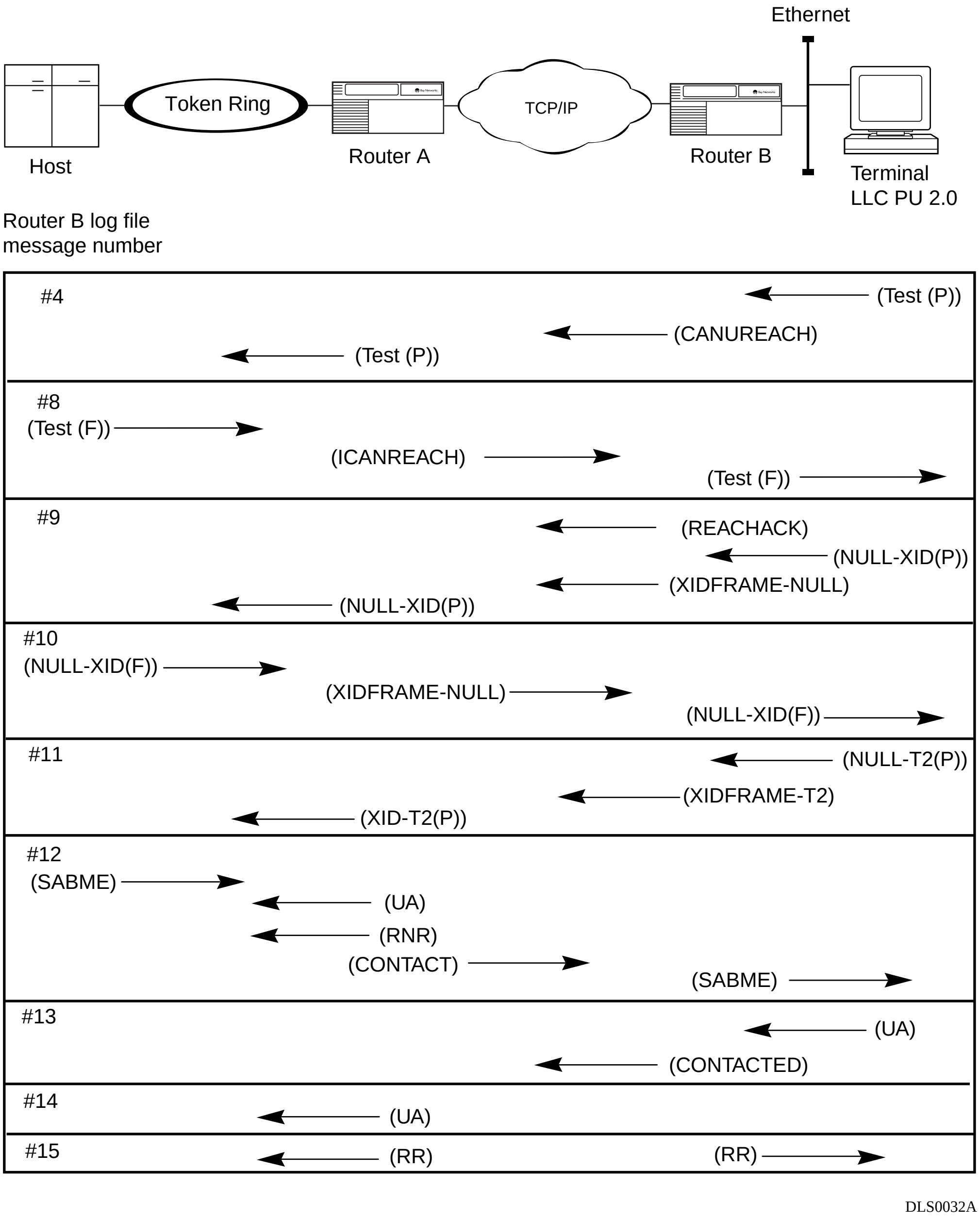


Figure C-1. Sample DLSw/LLC2 Network Connection Sequence (RFC 1434)

Reviewing the Network Log

This section describes the debug event messages that Router B logs when it establishes a connection with Router A (refer to Figure C-1). Each message begins with a number that you can use to reference the network activity shown in Figure C-1.

The initial connection sequence begins when the terminal sends a Test (P) packet to Router B. Router B sends a CANUREACH to Router A; Router A forwards a Test (P) frame to the host.

```
# 4: 04/25/95 22:43:00 DEBUG     SLOT  1 DLS Event Code:  17
LLC test frame received
```

The host computer returns a Test (F) frame, informing Router A that it is available. Router A then sends the ICANREACH frame to Router B. Router B sends a Test (F) frame to the terminal.

```
# 8: 04/25/95 22:43:00 DEBUG     SLOT  1 DLS Event Code:  18
SSP ICANREACH in LLC frame received connection = 30927f70
```

Router B returns a REACHACK acknowledgment frame to Router A. The terminal then sends a NULL-XID(P) frame to Router B. Router B forwards an LLC XIDFRAME-NULL to Router A. Router A sends a NULL-XID(P) to the host.

```
# 9: 04/25/95 22:43:01 DEBUG     SLOT  1 DLS Event Code:  17
LLC XID frame received
```

The host returns a NULL-XID (F) frame to Router A; Router A forwards an XIDFRAME-NULL packet to Router B. Router B sends a NULL-XID(F) to the terminal.

```
# 10: 04/25/95 22:43:01 DEBUG     SLOT  1 DLS Event Code:  45
SSP XID frame rcvd in LLC, conn, state, flag: 30927f70, 4, 201
```

The terminal sends a NULL-T2 (P) frame to Router B, and Router B generates and sends an XIDFRAME-T2 to Router A. Router A sends an XID-T2 (P) to the host.

```
#  11: 04/25/95 22:43:01 DEBUG     SLOT  1 DLS Event Code:  17
LLC XID frame received
```

The host computer generates an SABME frame and sends it to Router A. Router A returns UA and receiver not ready (RNR) frames back to the host. Router A then contacts Router B, and Router B sends the SABME contact frame to the terminal.

```
#  12: 04/25/95 22:43:01 DEBUG     SLOT  1 DLS Event Code:  45
SSP contact frame rcvd in LLC, conn, state, flag: 30927f70, 4, 201
```

The terminal returns an acknowledgment UA packet to Router B. Router B informs Router A that the contact is accepted. A state change occurs.

```
#  13: 04/25/95 22:43:01 DEBUG     SLOT  1 DLS Event Code:  16
State change in ssp_contact, conn = 30927f70, old state = 4, new
state = 3
```

Router A sends an acknowledgment UA packet to the host computer.

```
#  14: 04/25/95 22:43:01 DEBUG     SLOT  1 DLS Event Code:  17
LLC connect_conf frame received
```

The DLSw circuit reaches the CONNECTED state. Router A and Router B return receiver ready (RR) packets to their clients.

```
#  15: 04/25/95 22:43:01 DEBUG     SLOT  1 DLS Event Code:  16
State change in connect_conf, conn = 30927f70, old state = 3, new
state = 1
```

Establishing DLSw/SDLC Connections

Figure C-2 illustrates a sample dual-switch DLSw/SLDC network and the network packet exchanges that occur during SDLC connection establishment. Connection establishment generates debug event messages in the log file.

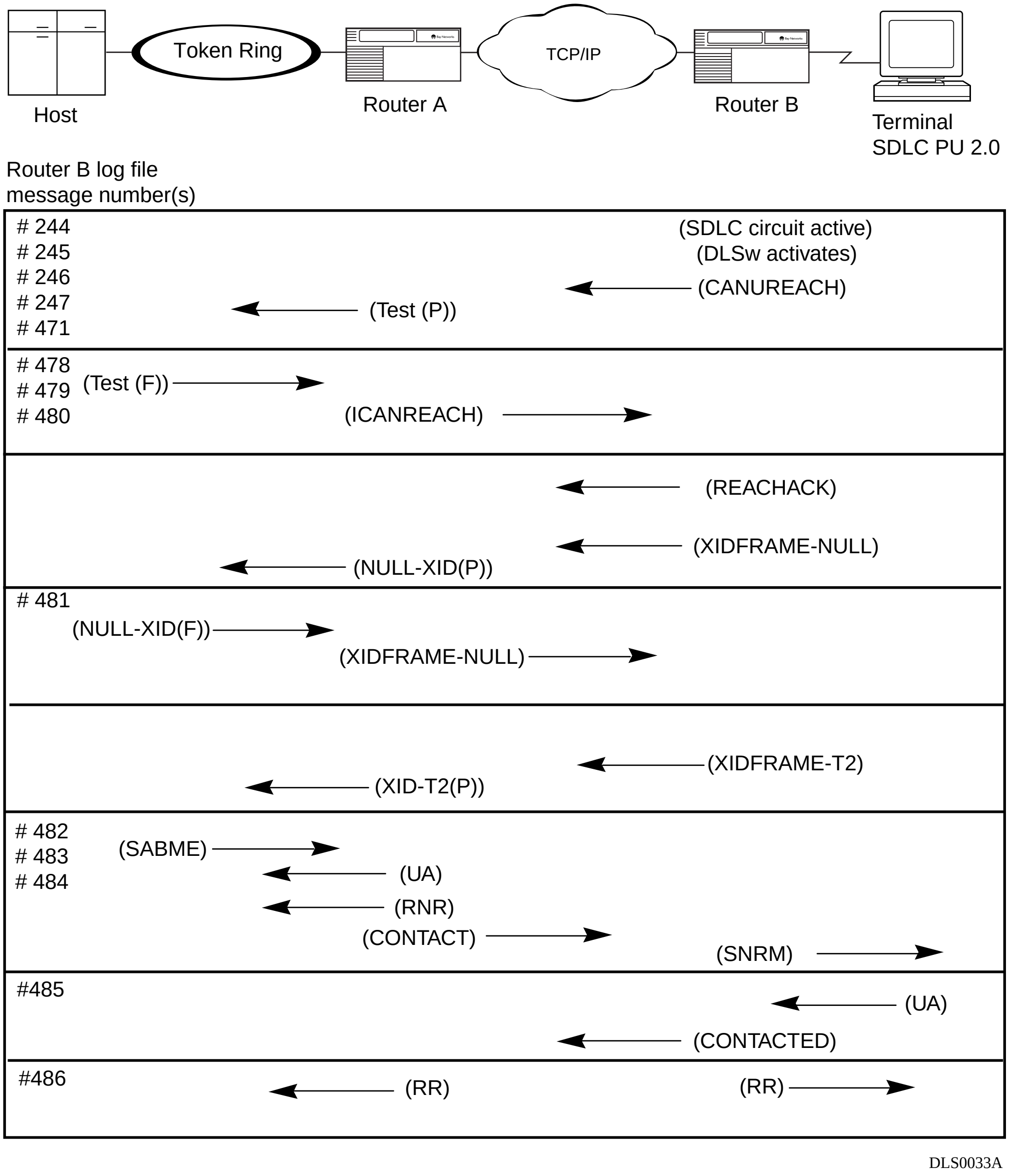


Figure C-2. Sample DLSw/SDLC Network Connection Sequence

Reviewing the Network Connection Sequence

This section describes the debug event messages that Router B (see Figure C-2) logs when it connects with Router A. Each message begins with a number that you can use to reference the network activity shown in Figure C-2.

SDLC becomes active on the circuit and DLSw notifies SDLC that it is configured on the circuit. SDLC processes the DLSw notification and sends a message indicating successful registration. DLSw attempts to contact the host with a CANUREACH frame. Router B sends the CANUREACH to Router A. Router A forwards Test (P) frame to the host.

```
# 244: 07/12/95 08:46:07 DEBUG     SLOT  1 SDLC Event Code:   8
sdlc_proto_gate_init
# 245: 07/12/95 08:46:08 DEBUG     SLOT  1 DLS Event Code:  86
received CO_ISAP registration response from SDLC, nwif = 3171ad50
# 246: 07/12/95 08:46:08 DEBUG     SLOT  1 SDLC Event Code:  11
DLC_IF_CONNECT_SEND_MSG
# 247: 07/12/95 08:46:08 DEBUG     SLOT  1 DLS Event Code:  60
received CONNECT response from SDLC port = 3171ad50, ls_ref =
3171e230
# 471: 07/12/95 08:48:08 DEBUG     SLOT  1 DLS Event Code:  18
SSP canureach frame received connection = 00000000
```

The host computer returns a Test (F) frame, informing Router A that it is available. Router A then sends the ICANREACH frame to Router B.

```
# 478: 07/12/95 08:48:08 DEBUG     SLOT  1 DLS Event Code:  18
SSP ICANREACH new connection frame received connection = 31619ea0
 479: 07/12/95 08:48:08 DEBUG     SLOT  1 DLS Event Code:  18
SSP ICANREACH connection frame received connection = 31619ea0
# 480: 07/12/95 08:48:08 DEBUG     SLOT  1 DLS Event Code:  18
SSP ICANREACH in SDLC frame received connection = 31619ea0
```

Router B returns a REACHACK acknowledgment frame to Router A. Router B forwards an XIDFRAME-NULL to Router A. Router A sends a NULL-XID(P) to the host.

The host returns a NULL-XID (F) frame to Router A, which forwards an XIDFRAME-NULL packet to Router B.

```
# 481: 07/12/95 08:48:08 DEBUG     SLOT  1 DLS Event Code:  45
SSP XID frame rcvd in SDLC, conn, state, flag: 31619ea0, 4, 1
```

Router B generates and sends an XIDFRAME-T2 to Router A. Router A sends an XID-T2 (P) to the host.

The host computer generates an SABME frame and sends it to Router A. Router A returns UA and RNR frames back to the Host. Router A then contacts Router B. Router B accepts the CONTACT frame, causing a state change. Router B sends the Set Mode indication SNRM frame to SDLC.

```
# 482: 07/12/95 08:48:08 DEBUG     SLOT  1 DLS Event Code:  45
SSP contact frame rcvd in SDLC, conn, state, flag: 31619ea0, 4, 1
# 483: 07/12/95 08:48:08 DEBUG     SLOT  1 DLS Event Code:  16
State change in ssp_contact, conn = 31619ea0, old state = 4, new
state = 3
# 484: 07/12/95 08:48:08 DEBUG     SLOT  1 SDLC Event Code:  11
DLC_IF_SET_MODE_SEND_MSG
```

SDLC acknowledges the Set Mode indication (UA).

```
# 485: 07/12/95 08:48:08 DEBUG     SLOT  1 DLS Event Code:  73
received SET_MODE response from SDLC
port = 3171ad50, ls_ref = 3171e230
```

The DLSw circuit reaches the CONNECTED state. Router A and Router B return receiver ready (RR) packets to their clients.

```
# 486: 07/12/95 08:48:08 DEBUG     SLOT  1 DLS Event Code:  16
State change in sdlc_connected, conn = 31619ea0, old state = 3, new
tate = 1
```

Disconnecting from the Network

This section provides some sample log messages that occur when you disconnect from a DLSw network. Included is a description of each event, followed by the actual log message(s).

A local endstation disconnects and generates a DISCONNECT frame. The DISCONNECT frame causes a state change to DISCONECTED. The local router sends the DISCONNECT frame to the remote router.

```
#  18: 04/25/95 22:43:09 DEBUG     SLOT  1 DLS Event Code:  17
LLC DISC frame received
#  19: 04/25/95 22:43:09 DEBUG     SLOT  1 DLS Event Code:  16
State change in llc_disc_ind, conn = 30927f70, old state = 1, new
state = 11
```

The remote router issues a DL_HALTED frame and sends it to the local router.

```
#  20: 04/25/95 22:43:09 DEBUG     SLOT  1 DLS Event Code:  45
SSP dl_halted frame rcvd in LLC, conn, state, flag: 30927f70, b, 0
```

The local endstation is DISCONNECTED end to end.

```
#  21: 04/25/95 22:43:09 DEBUG     SLOT  1 DLS Event Code:  16
State change in ssp_dlhalted, conn = 30927f70, old state = 11, new
state = 11
```

Troubleshooting DLSw

This section provides general information on troubleshooting DLSw and the basic DLSw component subsystems. It covers the following topics:

- Viewing Isolated Problems
- Common DLSw Problems and Nonproblems
- DLSw Troubleshooting Tables covering symptoms, possible causes, and actions specific for the following categories:
  - DLSw configurations
  - DLSw interfaces
  - TCP
  - SNA
  - LLC
  - SDLC

Viewing Isolated Problems

This section assumes that you have isolated a problem to DLSw. Troubleshoot DLSw as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for DLSw.**

   If you use the Technician Interface, enter

   log -fftwid -eDLS -s<*slot_no.*>

For example, f you are filtering events from Slots 3 and 4, enter

```
log -fftwid -eDLS -s3 -s4
```

2. **Make sure that the DLSw MTU size matches the synchronous line MTU size.**

   Unnecessary packet fragmentation can occur when these settings do not match.

3. **Use the Technician Interface or the Statistics Manager to inspect the global SRB settings, such as the internal LAN ID, the group LAN ID, and the bridge ID. If you are using the Technician Interface, enter**

   ```
   get wfBrSr.*.0
   ```

4. **Use the Technician Interface or the Statistics Manager to inspect the global DLSw settings, such as the configured TCP window size and the total number of established DLSw sessions. If you are using the Technician Interface, enter**

   ```
   get wfDls.*.0
   ```

   Make sure that the virtual ring ID for the IP cloud is unique and is consistent among all sites.

5. **Use the Technician Interface or the Statistics Manager to inspect the state of all of the DLSw interfaces currently configured, and the value of the instance field. If you are using the Technician Interface, enter**

   ```
   get wfDlsInterfaceEntry.3.*
   ```

6. **Use the Technician Interface or the Statistics Manager to inspect the state of all of the TCP connections. If you are using the Technician Interface, enter**

   ```
   get wfTcpConnEntry.2.*
   ```

   Make sure that all active TCP sessions are in an “established” state (represented by the value 5).

   If the sessions are in an established state, the local and remote DLSw TCP slot/peer configuration is probably correct.

If the sessions are not in an established state, do the following:

- Make sure all slots configured to run DLSw have a slot IP address assigned.
- Make sure that the slot IP address corresponds to the DLSw Peers setting at the remote site.

7. **Use the Technician Interface or the Statistics Manager to inspect the reception messages and connection state changes.**

Common DLSw Problems and Nonproblems

This section describes common problems and nonproblems associated with DLSw.

Common DLSw Problems

Table C-4 describes common problems with DLSw, LLC, and SDLC, and lists causes and actions.

Table C-5. Common DLSw Problems

Problem	**Possible Cause**	**Action/Solution**
DLSw/TCP connections do not come up.	Improper DLS Slot Table configuration; no IP address configured on slot	Each slot running DLSw requires a unique IP address assigned to each DLSw slot.
DLSw/TCP connections partially come up.	No peer configured	Add a peer and its IP address to the Peer Table.
DLSw connections do not come up.	DLS configured on wrong slot	Configure DLS on an LLC or SDLC interface.
Single- switch sessions do not establish.	Both interfaces not configured	Configure two interfaces for single-switch operation.

(continued)

Table C-5. Common DLSw Problems *(continued)*

Problem	**Possible Cause**	**Action/Solution**
Frame rejects cause session failures.	Endstation MAXIN parameter smaller than wfLlcInterfaceTw	Verify the configuration of the endstation and check the configured LLC window sizes.
	MTU received is too large for configuration	Increase the wfLlcInterfaceMaxMtu variable to larger than the possible data size.
	T1 timer too short for long WAN delays	Increase the wfLlcinterfaceTAckWait setting to avoid timeouts.
The router is sending RNRs.	Mismatch of SDLC link station interface MAXOUT parameter	Edit the MAXOUT parameter setting.
The DLS interface configured for SDLC does not come up.	Improper cabling	Install correct cable(s). Refer to the “Verifying the WAN Cabling” section later in this appendix.
An IBM AS/400 cannot connect to another AS/400.	Using SAP 0 for SSAP on test frames	Configure SAP 0 in the DLSw SAP configuration.

(continued)

Table C-5. Common DLSw Problems *(continued)*

Problem	Possible Cause	Action/Solution
File transfers with large packets are slow.	DLSw uses more CPU than SRB.	Edit DLSw packaging parameters; use protocol prioritization and prioritize SNA traffic over other protocols.
	The TCP window size is too small, causing RNRs at the source.	TCP flow control is limiting performance; increase the TCP Window Size parameter setting.
	The TCP window size is too large, causing latency problems.	Critical data is being buffered by TCP; decrease the TCP Window Size parameter setting and check performance.
	IP WAN frames are fragmented.	Set the Virtual Ring MTU parameter to less than the WAN maximum transfer unit.
	TCP is transmitting too many frames	Decrease the TCP Window Size parameter setting and check performance.
The Response time is slower than normal.	The TCP window size is too large.	Decrease the TCP Window Size parameter setting and check performance.

Common DLSw Nonproblems

The DLSw log often contains debug event messages that report conditions about proper network activity. These debug messages are not errors and should not be treated or reported for further action. The DLSw nonproblems include:

- Unexpected protocol action
- TCP open error 29
- DLSw peers not reachable due to lack of a route
- Traffic going over SRB instead of DLSw path
- Resetting dynamic window algorithm
- Expecting SNRM prior to DLSw connection to host

Unexpected protocol action

An unexpected protocol action occurred multiple times. This condition indicates that frames are being transmitted between two DLSw routers while an LLC Disconnect Pending frame is processing. This condition clears itself and the DLSw disconnect sequence finishes normally. The following sample log entries show this condition:

```
#  36: 04/25/95 22:43:17 DEBUG     SLOT  1 DLS Event Code:  16
State change in llc_disc_ind, conn = 30927f70, old state = 1,
new state = 11

#  38: 04/25/95 22:43:17 DEBUG     SLOT  1 DLS Event Code:  36
Unexpected protocol action: state = 11, event = 10 conn = 30927f70

#  39: 04/25/95 22:43:17 DEBUG     SLOT  1 DLS Event Code:   0
The previous event on slot 1 repeated 7 time(s).  [Code 36]

#  40: 04/25/95 22:43:17 DEBUG     SLOT  1 DLS Event Code:  45
SSP dl_halted frame rcvd in LLC, conn, state, flag: 30927f70, b,
0
```

TCP open error 29

The DLSw peer connections through TCP cannot be activated until the source (local) IP interface becomes active. For example, Token Ring networks that take longer to initialize may cause this error in the log. The TCP sessions establish when the IP interface activates. For example:

```
#  36: 04/25/95 22:43:17 INFO     SLOT  1 TCP Event Code:  7
TCP Error: 29 Opening 192.200.1.25,2065 - 192.200.4.40,2067 TCB:
0x3042cf0
```

DLSw peers not reachable due to lack of a route

IP needs to route the TCP connect request to the remote peer through the standard routing mechanisms. If IP cannot reach the destination address, the TCP peer connection cannot establish.

Traffic going over SRB instead of DLSw path

Performance is below normal and data traverses the network over SRB instead of the expected DLSw path. This could be caused by DLSw configured on the IP/WAN interface on the router instead of the destination port where the DLSw traffic is to terminate.

Resetting dynamic window algorithm

Proper LLC flow control operation is indicated by messages stating that the dynamic window algorithm is resetting.

Expecting SNRM prior to DLSw connection to host

Refer to *Configuring SDLC Services* and check the Pre-Activation Contact Frame parameter setting.

DLSw Troubleshooting Tables

Tables C-5 to C-11 provide the following troubleshooting information:

- DLSw configuration
- DLSw interface
- TCP
- SNA
- LLC
- SDLC

Table C-6. DLSw Configuration Troubleshooting

Problem	Possible Cause	Action/Solution
The log file contains no DLSw, SDLC, LLC, or TCP messages.	Specific router slot not active for DLSw configuration Image missing components	Check the hardware configuration to see if DLSw is configured on the slot. Make sure that the router software image contains DLS.exe, LLC.exe, NBASE.exe, and SDLC.exe.
Broadcasts are not seen on the desired LAN segments.	Peer not configured for destination router	Configure at least one peer that must receive broadcasts.

Table C-7. DLSw Interface Troubleshooting

Problem	Possible Cause	Action/Solution
The DLSw interface state is DOWN.	Physical interface not up	Check the connections; make sure that the physical interface is up.
	DLC interface not up	Check the DLC configuration and delete the interface, if necessary; notify Bay Networks.
The DLC interface is DOWN.	Physical interface not up	Check the connections; make sure that the physical interface is up.
The DLSw interface is DOWN; the LLC interface is UP.	DLSw interface configured on a different slot than physical interface	Check and correct the configuration to ensure that DLSw is configured on the same slot as the physical interface.
	DLSw interface different than corresponding LLC wfLlcInterfaceEntry.wfLlcInterfaceLlc2Cc	Correct the configuration; DLSw must be configured on the slot where DLC termination occurs.
	Potential LLC problem if not notifying DLSw that it is present	Delete the LLC interface; contact Bay Networks.
Ethernet interfaces drop sessions from Token Ring interfaces.	Frames sent to Ethernet are larger than 1500 bytes	Set the DLSw Virtual Ring MTU parameter to 1518 or less on any routers with Token Ring.
Ethernet sessions establish with difficulty.	Loops formed by dual router Ethernet connections	Two DLSw routers connected to an Ethernet segment must have filters to avoid loops.

Table C-8. TCP Troubleshooting

Problem	Possible Cause	Action/Solution
DLSw/TCP connections do not come up.	Improper DLS Slot Table configuration; no IP address configured on slot	Each slot running DLSw requires a unique IP address assigned to each DLSw slot.
DLSw/TCP connections partially come up.	No peer configured	Add a peer and its IP address to the Peer Table.
	Peer is not reachable	Check to see if IP routing is enabled and the peer is configured or known to DLSw.
TCP connections come up, but traffic is not passed.	DLSw Slot Table configuration does not match DLC interface location	Correct the configuration by creating a DLS slot entry for every slot that has a DLC interface.
TCP has excessive retransmissions.	TCP window is too large	Edit the TCP Window Size parameter and specify a smaller value.
	TCP is filling WAN buffers and causing dropped frames	Configure protocol prioritization and allocate adequate queue depth.
TCP sessions do not come down when the IP path is lost.	TCP Keepalive Time parameter set to 0	Edit the Keepalive Time parameter and specify a value in the range 0 to 2147483647 seconds. Refer to the Keepalive Time parameter in Chapter 5 for more information.

Table C-9. SNA Troubleshooting

Problem	Possible Cause	Action/Solution
SNA stations cannot connect over DLSw.	Host is unavailable or IP cannot reach it	Verify the status of the host and attempt to ping the target router.
	XID is incorrect	Obtain correct XID values.
	Destination MAC address incorrect; if LLC media is Ethernet, the address needs to be in non-canonical format	Verify that the destination MAC address is correct; if the LLC media is Ethernet, then flip the address format.
	First experience with new device	Obtain flows and traces and contact Bay Networks.
SNA stations fail in heavy network traffic.	Other traffic is taking too much time on the WAN	Use protocol prioritization to provide more bandwidth to SNA.
	DLC initiated termination of session	Depending on the configuration, refer to the LLC or the SDLC Troubleshooting table.

Table C-10. NetBIOS Troubleshooting

Problem	**Possible Cause**	**Action/Solution**
NetBIOS stations cannot connect over DLSw.	NetBIOS SAP not configured Excessive broadcast traffic on WAN	Configure SAP 0xF0 in the DLSw SAP TAble. Use traffic filters, caches, or network design to limit unnecessary NetBIOS traffic; use protocol prioritization to provide more DLSw bandwidth on the WAN.
NetBIOS stations cannot keep sessions alive during data transfer.	PC session level timeout short WAN connectivity is lost or not rerouting fast enough	Set the OS/2 *IBMLAN.INI* file parameter SRVHEURISTICS to 9. Use traffic filters, caches, or network design to limit unnecessary NetBIOS traffic; use protocol prioritization to provide more DLSw bandwidth on the WAN.

Table C-11. LLC Troubleshooting

Problem	**Possible Cause**	**Action/Solution**
Frame rejects cause session failures.	Endstation MAXIN parameter smaller than wfLlcInterfaceTw	Verify the configuration of the endstation and check the configured LLC window sizes.
	MTU received is too large for configuration	Increase the wfLlcInterfaceMaxMtu variable to larger than the possible data size.
	T1 timer too short for long WAN delays	Increase the wfLlcinterfaceTAckWait setting to avoid timeouts.

Table C-12. SDLC Troubleshooting

Problem	**Possible Cause**	**Action/Solution**
DLSw configured for SDLC does not come up.	Incorrect configuration	Check the configuration to ensure that SDLC is configured and connected.
	DLSw connection not establishing	Make sure that the router software image contains *DLS.exe*, *LLC.exe*, *NBASE.exe*, and *SDLC.exe*.
	Improper cabling	Verify that you are using the correct cables; refer to “Verifying the WAN Cabling” section in this appendix.

(continued)

Table C-12. SDLC Troubleshooting *(continued)*

Problem	Possible Cause	Action/Solution
SDLC does not connect to the host computer.	SDLC interface not active	Check the configuration to ensure that there is an SDLC connection.
	SDLC local devices not configured properly	Check the DLSw local device configuration.
	Source or destination MAC address incorrect; if LLC media is Ethernet, the address needs to be in non-canonical format	Verify that the MAC address is correct; if the LLC media is Ethernet, then flip the address format.
	XID is incorrect	Obtain correct XID values.
	SDLC device configured for NRZI	Check the SDLC device and set the Sync Line Coding parameter.
The SDLC connection is up and down.	Idle timeout too short for some configurations	Increase the SDLC Idle Line Timer parameter (wfSdlcPortAdminIdleTimer).
	SDLC device configured for half/full duplex	For a half-duplex physical line, set the RTS Enable parameter to Enable or set wfSyncRtsEnable to 1; for a full-duplex data link, set the Primary Full Duplex parameter to Falsefull duplex or set wfSdlcPortAdminPriFdplx to 2.

Verifying the WAN Cabling

Tables C-12 to C-15 list the specific WAN cables that ensure reliable DLSw connectivity over an SLDC connection. The table includes:

- The Bay Networks cable part number
- Pin description and connector type
- Supported routers
- Modem or no modem configuration

Table C-13. BLN® and BCN® Synchronous Interface Cables

Cable	Description	Modem/No Modem
7215	15-pin to male V.35	Modem
7255	15-pin to male RS-232	Modem
7221	15-pin to male X.21	Modem
7941	15-pin to female RS-232	No modem
7942	15-pin to female V.35	No modem
AA0018003	44-pin to male X.21	No modem

Table C-14. AN®, ARN, ASN™, and EASF Synchronous Interface Cables

Cable	Description	Modem/No modem
7220	44-pin to male V.35	Modem
7224	44-pin to male X.21	Modem
7826	44-pin to male RS-232	Modem
7943	44-pin to female RS-232	No modem
7944	44-pin to female V.35	No modem
AA0018004	15-pin to female X.21	No modem

Table C-15. Octal Sync Interface Cables

Cable	Description	Modem/No modem
7932	50-pin to male V.35	Modem
7934	50-pin to male RS-232	Modem
7936	50-pin to male X.21	Modem
7945	50-pin to female RS-232	No modem
7946	50-pin to female V.35	No modem
AA0018005	50-pin to female X.21	No modem

Table C-16. Male No-Modem Cables

Cable	Description	Router
7218	15-pin to male RS-232	BLN/BCN
7219	15-pin to male V.35	BLN/BCN
7833	44-pin to male RS-232	AN/ASN
7834	44-pin to male V.35	AN/ASN

Index